Ministry of Justice

Cyber Security Guidance

Technical User Edition

Contents

Cyber and Technical Security Guidance

Summary

This site lists the https://www.gov.uk/government/organisations/ministry-of-justice Information Security policies. It contains important guidance on how to keep information safe and secure.

Policies shown here are listed for technical users and non-technical users (referred to as all users).

Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

The Technical Guidance covers technical decisions in the more widely.

Note: This guidance is dated: 8 November 2023.

Change log

A 'change log' is available. It details the most recent changes to this information.

The changes are also available as RSS or Atom feeds.

Searching this content

The security guidance is searchable in two ways:

1. By searching for the word or phrase on your preferred search engine, and specifying this site:

   ```
   site:https://security-guidance.service.justice.gov.uk/
   ```

   For example, to search for information about passwords, you might use the following search expression:

   ```
   password site:https://security-guidance.service.justice.gov.uk/
   ```
2. By downloading one of the offline versions and using the inbuilt search capability of your offline reader.

Offline content

This offline version of the guidance is available as a PDF file for convenience. However, it is time-limited: it is not valid after 8 December 2023. For the latest, current version of the guidance, refer to the security guidance site.

Security culture

In addition to the obvious security resources such as policies, controls, and software and hardware tools, all organisations need employees, suppliers and other colleagues to behave in a way that helps ensure good security at all times. A simple example is where someone will act in a way that maintains good security, even if they don't know exactly what the formal process is. The extent to which an organisation has good security in indicated by its security culture.

Security culture refers to the set of values, shared by everyone in an organisation, that determines how people are expected to think about and approach security. Getting security culture right helps develop a security conscious workforce, and promotes the desired security behaviours expected from everyone working in or for the organisation.

The is creating a portfolio of security culture resources to help supplement the formal policy and guidance material. Initial security culture material is available for preview.

Information structure

policy documents are listed beneath the following headings:

- Information security policies
- Mobile devices and teleworking
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Compliance
- Risk Assessment

The documents have been developed and defined within this taxonomy, and are listed in the next section, together with their suggested target audiences.

Information security policies

Management direction for information security

These are the policies for all users:

- Avoiding too much security
- IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- IT Security All Users Policy
- IT Security Policy (Overview)
- Line Manager approval

These are the policies for technical users:

- IT Security Technical Users Policy
- Shared Responsibility Models
- Technical Controls Policy

Mobile devices and teleworking

Mobile device policy

These policies are for all users:

- Mobile Device and Remote Working Policy
- Remote Working

Teleworking

This policy is for all users:

- Personal Devices

Human resource security

Prior to employment

This policy is for all users:

- Minimum User Clearance Levels Guide

During employment

This policy is for all users:

- Training and Education

Termination and change of employment

This policy is for all users:

- End or change of employment

Asset management

Responsibility for assets

These policies are for all users:

- Acceptable use
- Acceptable use policy
- Guidance on IT Accounts and Assets for Long Term Leave
- Protect Yourself Online
- Web browsing security

Information classification

These policies are for all users:

- Government Classification Scheme
- Information Classification and Handling Guide
- Information Classification and Handling Policy

These policies are for technical users:

- Data Handling and Information Sharing Guide
- Secrets management

Media handling

These policies are for all users:

- Removable media
- Secure disposal of IT equipment
- Secure disposal of IT - physical and on-premise
- Working securely with paper documents and files

This policy is for technical users:

- Secure disposal of IT - public and private cloud

Access control

Business requirements of access control

These policies are for technical users:

- Access Control Guide
- Access Control Policy
- Enterprise Access Control Policy
- Privileged Account Management Guide

User access management

These policies are for technical users:

- Authentication
- Management access
- Managing User Access Guide
- Multi-Factor Authentication
- Privileged User Backups, Removable Media and Incident Management Guide
- Privileged User Configuration, Patching and Change Management Guide
- Privileged User Guide
- Privileged User Logging and Protective Monitoring Guide

User responsibilities

This policy is for all users:

- Protecting Social Media Accounts

System and application access control

These policies are for all users:

- Password Managers
- Passwords
- Using 1Password

These policies are for technical users:

- Account management
- Authorisation
- Multi-user accounts and Public-Facing Service Accounts Guide
- Password Creation and Authentication Guide
- Password Management Guide
- Password Storage and Management Guide
- Policies for Google Apps administrators
- Policies for MacBook Administrators
- System User and Application Administrators

Cryptography

Cryptographic controls

These policies are for technical users:

- Automated certificate renewal
- Cryptography
- HMG Cryptography Business Continuity Management Standard
- Public Key Infrastructure Policy

- Use of HMG Cryptography Policy

Physical and environmental security

Equipment

These policies are for all users:

- Clear Screen and Desk Policy
- Equipment Reassignment Guide
- Laptops
- Locking and shutdown
- Policies for MacBook Users

This policy is for technical users:

- System Lockdown and Hardening Standard

Operations security

Operational procedures and responsibilities

These policies are for technical users:

- Active Cyber Defence: Mail Check
- Active Cyber Defence: Public Sector DNS
- Active Cyber Defence: Web Check
- Offshoring Guide

Protection from malware

This policy is for all users:

- Ransomware

These policies are for technical users:

- Malware Protection Guide (Overview)
- Malware Protection Guide: Defensive Layer 1
- Malware Protection Guide: Defensive Layer 2
- Malware Protection Guide: Defensive Layer 3

Backup

These policies are for technical users:

- System backup guidance
- System backup policy
- System backup standard

Logging and monitoring

These policies are for technical users:

- Accounting
- Commercial off-the-shelf applications
- Custom Applications
- Logging and monitoring
- Online identifiers in security logging and monitoring
- Protective Monitoring
- Security Log Collection

- Security Log Collection: Enterprise IT - Infrastructure
- Security Log Collection: Enterprise IT - Mobile Devices
- Security Log Collection: Hosting Platforms
- Security Log Collection: Log entry metadata
- Security Log Collection: Maturity Tiers

Control of operational software

This policy is for all users:

- Guidance for using Open Internet Tools

Technical vulnerability management

These policies are for technical users:

- Patch management guide
- Vulnerability Disclosure
- Vulnerability Disclosure: Implementing `security.txt`
- Vulnerability scanning and patch management guide
- Vulnerability scanning guide

Communications security

Network security management

These policies are for technical users:

- Code of Connection Standard
- Defensive domain registrations
- Domain names and Domain Name System (DNS) security policy
- Internet v. PSN
- IP DNS Diagram Handling
- Multiple Back-to-back Consecutive Firewalls
- Networks are just bearers

Information transfer

These policies are for all users:

- Bluetooth
- Email
- General Apps Guidance
- Phishing Guide
- Protecting WhatsApp accounts
- Secure Data Transfer Guide
- Sending information securely
- Web browsing security policy profiles
- Wifi security policy

These policies are for technical users:

- Criminal Justice Secure Mail (CJSM)
- Data Sovereignty
- Email Authentication Guide
- Email Blocklist Policy
- Email Blocklist Process
- Email Security Guide

- Secure Email Transfer Guide
- Spam and Phishing Guide

System acquisition, development and maintenance

Security requirements of information systems

These policies are for technical users:

- Technical Security Controls Guide
- Technical Security Controls Guide: Defensive Layer 1
- Technical Security Controls Guide: Defensive Layer 2

Security in development and support processes

These policies are for technical users:

- Maintained by Default
- Secure by Default
- Service Owners Responsibilities
- Source Code Publishing
- System Test Standard

Test data

This policy is for technical users:

- Using Live Data for Testing purposes

Supplier relationships

Information security in supplier relationships

These policies are for technical users:

- Suppliers to : Assessing Suppliers
- Suppliers to : Contracts
- Suppliers to : Security Aspect Letters
- Suppliers to : Supplier Corporate IT

Supplier service delivery management

These policies are for technical users:

- Azure Account Baseline Templates
- Baseline for Amazon Web Services accounts
- Baseline for Azure Subscriptions

Information security incident management

Management of information security incidents

These policies are for all users:

- IT Security Incident Management Policy
- IT Security Incident Response Plan and Process Guide
- Lost devices or other IT security incidents
- Reporting an incident

These policies are for technical users:

- IT Investigations - Planning and Operations Policy

- IT Disaster Recovery Plan and Process Guide
- IT Disaster Recovery Policy

Compliance

Compliance with legal and contractual requirements

This policy is for all users:

- Data Security and Privacy

These policies are for technical users:

- Data Destruction
- Data Destruction: Contract Clauses - Definitions
- Data Destruction: Contract Clauses - Long Format
- Data Destruction: Contract Clauses - Long Format (Appendix)
- Data Destruction: Contract Clauses - Short Format
- Data Destruction: Instruction and Confirmation Letter
- Data Security & Privacy Lifecycle Expectations
- Data Security & Privacy Triage Standards

Information security reviews

This policy is for technical users:

- Standards Assurance Tables

Risk Assessment

Risk Management

These policies are for technical users:

- Infrastructure and system accreditation
- IT Health Checks

Risk Assessment Process

This policy is for all users:

- Risk reviews

Other Guidance

The provides the base material for all security guidance in the .

Glossary

A glossary of some terms used in this guidance is available here.

Acronyms

Technical Guidance

The Technical Guidance should be read together with this security-focused guidance.

Change log for Security Guidance

This document summarises what changes were made, and when, to Security policy and guidance. The most recent changes appear at the beginning of the list.

2023-09-11 17:45 BST Update ITHC details	Updates to information about IT Health Checks.
2023-08-30 17:45 BST Clearance requirements	Added details about minimum user clearance requirements.
2023-08-09 17:35 BST Build tooling updates	Updates to build tooling for security and performance improvements.
2023-07-13 17:00 BST Accessing MoJ IT systems from overseas	Removed topic on accessing MoJ IT systems from overseas.
2023-07-07 16:45 BST Taking equipment overseas	Removed general advice topic on taking equipment overseas.
2023-06-22 17:35 BST Formatting and terminology updates	Minor improvements to formatting, and updates to terminology.
2023-06-05 18:13 BST Updates to incident management policy	Refresh and add extra detail about managing security incidents.
2023-04-29 13:54 BST Add 1Password guidance	Add information about using the 1Password tool.
2023-04-18 17:10 BST Revise content	Updates to personnel and related information.
2023-03-21 17:35 GMT Restructure landing page, and added service owners responsibilities guidance	New material on service owner responsibilities.
2023-02-28 17:35 GMT Corrected policy reference number	Policy number POL.ITAUP.022 in the Acceptable Use Policy was incorrectly listed as number 021.
2023-02-16 17:35 GMT Corrected typo in template	Fixed minor typo in Asset template.
2023-02-08 17:35 GMT Updated remote working guidance	Clarification on using hotel or other public wifi spots.
2023-01-22 17:41 GMT Updated authorisation information	More details on implementing defensive depth and dealing with external IP addresses.
2023-01-10 18:04 GMT Updated contact details for secure disposal	When seeking help for secure disposal, contact IT Service Desk in the first instance.
2022-10-19 14:34 BST Updated project README	An update to the README and refresh of the content.
2022-08-31 09:50 BST Overseas travel	Clarification regarding transit or destination locations.
2022-08-30 10:43 BST Added guidance on protecting WhatsApp accounts	Extra information on how WhatsApp accounts might be attacked, and how to protect your accounts.
2022-08-09 12:17 BST Remove links to download leaflets	Remove links to leaflet downloads, ready for later updates.
2022-08-05 12:08 BST Add guidance on video conferencing hardware	Provide more details on the use of dedicated hardware for video and conference calls.
2022-08-04 16:22 BST Add connected vehicle reference in bluetooth guidance	Connected vehicles are discussed in personal devices, but the information also applies in the bluetooth guidance.

2022-07-22 13:14 BST Use of personal devices to receive MFA codes	Added clarification that personal devices may be used to receive MFA authentication codes if an MoJ-issued device is not available.
2022-07-21 13:45 BST Guidance on use of personal devices	Added clarification and emphasis that personal devices must not be used for work purposes. This includes accessing MoJ Slack channels using personal devices.
2022-07-04 14:23 BST Correct broken links	Internal links on a page were broken; now fixed.
2022-06-23 12:02 BST Accessibility updates	Improved the content tagging following guidance on accessibility improvements. Affects all pages, the link in this notification is to an example page.
2022-06-01 13:36 BST Reporting phishing	Clarified process for reporting phishing attempts.
2022-05-27 16:09 BST Add IASME certification information and templates.	Added material to assist suppliers in seeking security certification, particularly regarding the IASME Governance standard.
2022-05-20 15:37 BST Updates to overseas travel information.	More information about applying with sufficient advance notice, and a reminder about passport validity dates.
2022-05-06 12:30 BST Minor restructure to Phishing information.	The section on Out Of Band Checks has been slightly reordered, to improve readability.
2022-05-06 12:18 BST Added link to Password Poster.	An information poster about how to make strong passwords is now available for download.
2022-04-19 17:45 BST Update links for contacting security team.	Standardise on security@justice.gov.uk email address for contacting security team.
2022-04-08 10:09 BST Add guidance on secure disposal of cloud materials.	New guidance to ensure the confidentiality of MoJ data remains when a cloud service is decommissioned.
2022-04-06 15:53 BST Update security.txt link.	Corrected link to the standard security.txt file.
2022-04-04 10:50 BST Add password manager guidance.	Added extra information on the use of password manager apps in the MoJ.
2022-03-21 10:35 GMT Add guidance on sharing information.	Added extra information on sharing information internally and externally.
2022-03-21 10:22 GMT Add guidance on QR codes.	Added information on QR codes; currently considered low risk.
2022-03-11 15:31 GMT Updates to ransomware information leaflet.	Updates to correct typos and improve style.
2022-03-10 17:01 GMT Updates to LastPass guidance.	More information about when and how LastPass may be used.
2022-03-10 13:09 GMT Various minor corrections.	Fixing broken links and updating references to standards.
2022-03-04 09:16 GMT Updated email security guide.	Clarification that phishing or spoofing of MoJ colleagues, by MoJ colleagues, is not permitted other than with formal approval in advance, justified by a good business case.
2022-02-18 18:35 GMT Added phishing guide.	New topic, providing advice on dealing with phishing threats.
2022-02-16 11:19 GMT Updated security.txt file.	Provided new expiry date for security.txt file.
2022-02-15 12:18 GMT Various minor corrections.	Corrected contact details, fixed an incorrect link, and updated secure disposal information.

2022-02-07 15:49 GMT Updated glossary.	Expanded list of glossary definitions, and explanation of out-of-band-checks.
2022-02-01 11:51 GMT Update to passwords guidance.	A reminder not to share passwords or other account details.
2022-01-25 10:37 GMT Publication of ransomware information leaflet.	Useful leaflet explaining what Ransomware is, and tips on protecting your work and your systems.
2022-01-18 17:06 GMT Updated guidance for hosting platforms.	Updated baseline guidance for AWS and Azure platforms.
2022-01-07 14:36 GMT Contact details for AWS	Updated contact details for Baseline AWS accounts.
2022-01-06 09:36 GMT System lockdown and hardening	Guidance added to prevent outbound connections to random internet systems, unless this is a core part of their design. Firewall rules and other network configuration must prevent this.
2022-01-04 16:27 GMT IT Health Check	Updated guidance with a new section on Cloud platforms.
2022-01-04 16:10 GMT Update Slack channel for privacy team	Provide revised channel details for contact privacy team through Slack IM.
2021-12-23 13:50 GMT Update overseas travel guidance	Updates to information on overseas travel and accessing MoJ IT systems from overseas.
2021-12-21 13:18 GMT Provide seasonal SMS scam advice	Material to help improve awareness and best practices for security.
2021-12-15 15:09 GMT Use DuckDuckGo search engine	Default to using DDG for content search.
2021-12-13 11:44 GMT Security threat level guidance	New security threat Level guidance, and associated procedures.
2021-12-13 11:27 GMT Debrief on return from travel	Added description of a security debrief that is mandatory after some travel or where other security conditions apply.
2021-12-13 11:24 GMT Accessing MoJ systems from overseas	Added link to supplementary information on the MoJ Intranet.
2021-12-08 09:15 GMT Email access	Added clarification regarding when access is permitted to a user's business email account.
2021-12-07 15:18 GMT Email Authentication	Added guidance requiring the use of MTA-SLS and TLS-RPT in MoJ email systems.
2021-11-30 13:54 GMT Personal Devices	Clarified guidance on connecting personal devices using Bluetooth, and added new section on connected vehicles.
2021-11-22 16:23 GMT MFA	Clarified guidance on sending one-time MFA codes only to individual devices or accounts, not to shared devices or accounts.
2021-11-22 14:14 GMT Government Classification Scheme	Updated and consolidated guidance on classification of Government information.
2021-11-19 15:22 GMT Other guidance and security.txt	Improved structure for other guidance information, and added security.txt file.
2021-11-19 10:09 GMT Sending information securely	Guidance on working securely with paper documents and files.

2021-11-17 17:07 GMT Personal devices	Updated guidance about using a personal device to connect to a business Teams meeting as a Guest.
2021-11-09 15:37 GMT Acceptable use policy	Provide more detail on monitoring of systems and information, and to clarify the situation regarding Data Protection and the storage or processing of information outside the UK.
2021-11-08 17:30 GMT System backup policy	Corrected broken links within the content, also some structural changes for easier cross-referencing with related topics.
2021-11-04 09:05 GMT Working securely with paper documents and files	This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office.
2021-11-03 17:12 GMT Email blocking	The policy and processes for blocking emails, and deleting emails through administrative processes, across email services across the MoJ.
2021-11-03 17:00 GMT Domain names	An overview of domain name registration and monitoring principles and responsibilities within the MoJ.
2021-10-29 11:52 BST Logging retention	Information about keeping logging information.
2021-10-19 13:06 BST Remote working	Simplified the guidance regarding remote working.
2021-10-15 16:27 BST Email best practices	Added guidance regarding attachments and the use of 'cc' and 'bcc' fields in emails.
2021-10-14 13:47 BST Azure subscription baselines	Added guidance on baselines and templates for Azure subscriptions.
2021-10-13 15:50 BST IT Health Checks	Added guidance on requesting and managing IT Health Checks.
2021-10-08 09:56 BST Wifi policy	Added policy information about wifi.
2021-10-05 14:28 BST Client certificates	Added notes about obtaining client certificates.
2021-10-01 15:24 BST Connection to public wifi	Clarification about connecting to public wifi spots, such as hotels or coffee shops, or home broadband. Also extra details for remote working securely.
2021-10-01 15:07 BST Personal device attachment	Clarifying the connection of personal peripherals, and the charging of personal devices from USB ports.
2021-09-13 17:21 BST Government Security Standard 007 V2	Updates following the release of V2 of the Gov007 security standard.
2021-09-02 15:16:00 BST Extra guidance on remote working.	Additional best practices for keeping safe and secure when working away from the office.
2021-08-20 14:14:00 BST Update to general apps guidance.	Add Trello guidance, and clarification over Official and Official Sensitive material in apps.
2021-08-18 15:17:00 BST Add change log page.	Created a change log page, and associated RSS and Atom feeds, to describe new or changed content.
2021-08-16 17:04:00 BST Clarification for accessing MoJ IT systems overseas.	Additional information describing the process.
2021-08-16 17:03:00 BST Data Movement Form updated.	Data Movement Form updated.

Getting in contact

Reporting an incident

colleagues should visit https://intranet.justice.gov.uk/guidance/security/report-a-security-incident/ on the Intranet.

Suppliers to the should refer to provided methods/documentation and contact your usual points of contact.

Security Team: asking for help

Overview

This document tells you about the Security Team. It explains how to ask for help, outlines how we handle your requests, and describes what happens next.

To ask for help from a security consultant, send an email to: .

About the team

The Security Team is part of Security & Privacy. The Chief Information Security Officer leads the team.

The team provides help and guidance around cyber security matters, such as:

- Understanding the risks facing your systems and services.
- Designing and implementing effective mitigations for these risks.
- Developing services using security best practices.
- Checking that you or your third party suppliers have enough, and appropriate, cyber security measures in place.
- Applying IT Security policy to specific scenarios.

Asking for help

If you need help dealing with a cyber security task or problem, send an email to:

Some requests are better handled by other teams. For urgent matters such as incidents, or to get help about physical or personnel security, contact . For help with data protection, contact .

The security team keep an eye open for email requests. Normally, you'll get an acknowledgement or more detailed reply within two working days.

To help us help you, please answer these questions in your email request, as best you can:

1. Who is the work for?
2. Why is it important?
3. What happens if the work is not done (or not done on time)?
4. What is your need (old-style accreditation on an existing contract, guidance or advice, review of proposed approach,...)?
5. What skills or experience does the work need (known or predicted)?
6. When is the next project milestone that needs cyber consultancy input or involvement?

How the team handle requests for help

Each working day, we review all new requests.

We aim to get a reply to you within two working days of us receiving the request. Some large or complex requests might need more information and discussion. These requests take extra time for us to work out the best way to support you.

Some requests might not be appropriate for the team. In such cases, we send a prompt reply, explaining why it would be better to talk with a different team. We'll usually recommend a more appropriate team, and provide contact details for them.

What happens next

If your request is not appropriate for the team, we'll tell you immediately after the initial assessment.

If your request is appropriate for the team, the assigned consultant contacts you directly. They will engage with you to start providing the help you need.

If things go wrong...

If you disagree with our decision about your request, or there is some other problem, contact us again: .

If you'd prefer a different escalation route, contact ciso@digital.justice.gov.uk.

Security culture

Security culture

This section includes material created or provided by the to help improve awareness and best practices for security within the organisation.

Note: The advice in this material cannot guarantee to protect you from problems. The range of security threats is huge, and increasing all the time.

Who is this for?

This material is for anyone who implements, administers, supports, uses or delivers services.

Christmas SMS delivery scams

Seasonal celebrations are fun, but can also suffer from scams. A common scam involves sending fake parcel delivery text messages. The messages contain fake links. The links capture personal information and bank account details. Bad actors then use these details to steal money from individuals.

Some SMS messages get people to install malware. An example is Flubot, which steals personal and banking details. Flubot also uses your contact lists to send more fake texts.

The best way to avoid SMS scams is to contact parcel delivery companies directly. Go to their website and tracking your parcel there. Never click on a link in a text message.

Information security policies

Management direction for information security

Avoiding too much security

This guidance applies to developers and system administrators who work for the .

Is it possible to have too much security? Yes. Providing too much security for things or information that do not need protection is a waste of resources. It undermines the value of the security for things that do need it.

Security by obscurity is one of the weakest approaches for protecting something. It's far better to have a technical control in place to protect the system.

Not all domain names or IP addresses in Government systems are sensitive items

An example is a domain name or IP address. These values do not need to be secret for all systems. Only those that need it. It might be tempting to say that 'all IP addresses are . This is then used as a reason for an (in)action, such as "I can't email you that network diagram because it contains IP addresses." But the statement has wider consequences. It imposes a set of security requirements for everyone. It imposes them irrespective of the actual secrecy required.

is not a different classification to . It doesn't need special technical controls or procedures. Rather, it's a reminder to look after a piece of information. It's not a controls checklist. Using labels too casually conflicts with the idea of thinking about information and what we're doing with it, and using that to decide how best to secure the information.

Of course, you might need to keep the access details for some systems secure. An example might be where you cannot maintain or patch a legacy system. But these should be exceptional or 'edge' cases.

There are only a small number of situations where you need to protect IP addresses or domain names. It's usually where the context makes the information sensitive in some way. IP addresses can be personally-identifiable information. For example, a system log file might hold the IP address of a client accessing the system. This might reveal a link between an individual and their use of services. But the IP address of a public sector server or a router should not be personal data.

Remember also that within the , system almost always have RFC1918 addresses. These are normally not routable from the Internet. If you can access the system from the Internet, then you have other problems to resolve. Address them by appropriate security measures rather than hoping that secrecy is enough.

In other words, avoid saying that 'all IP addresses and domain names must be secure'. Instead, think about and justify the handling protections around each piece of information. Ask what data or capability is actually in need of protection, and from what risks.

It's not only about domain names or IP addresses

The need to keep some aspect of a system secret might be evidence that the technical security measures around the system are not complete, adequate, or appropriate to the risks. A well-designed system won't depend on secrecy alone for security.

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The is required to adhere (but prefers to exceed) to the Minimum Cyber Security Standard (MCSS).

The Standard

The UK HMG Security Policy Framework mandates protective security outcomes that the must achieve (and suppliers to , where they process data/information).

More information is available from https://www.gov.uk/government/publications/the-minimum-cyber-security-standard.

IDENTIFY

IDENTIFY is a prerequisite standard that requires:

- appropriate information security governance processes;
- identification and cataloguing of information held/processed; and
- identification and cataloguing of key operational services provided.

PROTECT

PROTECT is the core standard to provide fundamentally defences to information and requires:

- access to systems and information to be limited to identified, authenticated and authorised systems/users;
- systems to be proportionally protected against exploitation of known vulnerabilities; and
- highly privileged accounts (such as administrative level) to be protected from common attacks.

DETECT

DETECT is the core standard to detect when attacks are taking, or have taken, place and requires:

- capture event information (and apply common threat intelligence sources, such as CiSP);
- based on PROTECT, define and direct monitoring tactics to detect when defence measures seem to have failed;
- detection of common attack techniques (such as commonly known applications or tooling); and
- implementation of transaction monitoring solutions where systems could be vulnerable to fraud attempts.

RESPOND

RESPOND is the core standard to define the minimum of how organisations should respond to attacks and requires:

- development and maintenance of an incident response & management plan (including reporting, roles and responsibilities);
- development and maintenance of communication plans, particularly to relevant supervisory bodies, law enforcement and responsible organisations such as the NCSC;
- regular testing of the incident response & management plan;
- assessment and implementation of mitigating measures on discovery of an incident (successful attack); and
- post-incident reviews to ensure feedback into the iteration of the incident response & management plan.

RECOVER

RECOVER is the core standard to define the minimum of how organisations should recover from an attack once it has been considered closed, and requires:

- identification and testing of contingency mechanisms to ensure the continuance of critical service delivery;
- timely restoration of the service to normal operation (a plan to do so, and testing of that plan);
- from DETECT & RESPOND, immediately implementing controls to ensure the same issue cannot arise in the same way again, ensuring systematic vulnerabilities are proportional remediated.

IT Security Policy (Overview)

This policy gives an overview of information security principles and responsibilities within the and provides a summary of the 's related security policies and guides.

Related information

Technical Controls Policy on page 30

Audience

This policy is aimed at three audiences:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the .
General users	All other staff working for the .

Within this policy, "all users" refers to General users, Technical users, and Service Providers as defined previously.

Associated documentation

For further guidance on IT Security, refer to the following policies.

- IT Security All Users Policy: which provides further details of the responsibilities of all users at the .
- IT Security Technical Users Policy: which provides the details of where users can find more technical and service provider related information on IT Security within the .

Principles

All users :

- Comply with the 's wherever they work.
- Report all security incidents promptly and in line with 's .
- Make themselves aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other guidance.
- Be aware of the need for Information Security as an integral part of the day to day business.
- Protect information assets under the control of the organisation.

Further information can be found in the IT Security All Users Policy.

Technical users

Technical users follow the guidance set out for all users in IT Security All Users Policy **AND** also comply with the IT Security Technical Users Policy.

Service Providers

Service Providers follow the guidance set out for all users in IT Security All Users Policy **AND** also comply with the IT Security Technical Users Policy.

Enforcement

- This policy is enforced by lower level policies, standards, procedures and guidance.
- Non-conformance with this policy could result in disciplinary action taken in accordance with the 's Disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the always co-operates with the relevant authorities, and provides appropriate evidence.

IT Security All Users Policy
Introduction

This policy provides more information on the actions expected of all users when using equipment and infrastructure. It is a sub-page to the IT Security Policy Overview.

Note: In this document, the terms "data" and "information" are used interchangeably.

Audience

This policy is aimed at three audiences:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the .

General users	All other staff working for the .

Within this policy, "all users" refers to General users, Technical users, and Service Providers as defined previously.

Approach

The ensures that IT security controls are designed and implemented to protect data, IT Assets, and reputation, based around the following requirements:

Confidentiality	Knowing and ensuring that data can only be accessed by those authorised to do so.
Integrity	Knowing and ensuring the accuracy and completeness of data, and that it has not been deliberately or inadvertently modified from a previous version.
Availability	Knowing and ensuring that IT systems and data can always be accessed when required and authorised.

Assets

This policy applies to all premises, physical equipment, software and data owned or managed by the . This includes IT systems, whether developed by the or managed by IT service providers. It covers the use of IT equipment and the data processed on those IT systems, irrespective of location. It provides direction and support to preserve the confidentiality, integrity, and availability of resources.

Security classification

All Staff are responsible for ensuring data is:

- Classified correctly as detailed in the
- Distributed only in accordance with the statements of this policy and related guides.
- Protected by the appropriate security controls to ensure its confidentiality, integrity and availability.

Access to classified information shall be controlled in accordance with the requirements set out within the .

Physical and personnel security

The Physical Security Policy defines how physical access to assets must be controlled within the to prevent unauthorised access, use, modification, loss, or damage. All users must understand that:

- All IT systems and services must be assessed against environmental risks, for example flood or fire, to maintain the asset's confidentiality, integrity, and availability.
- The 's IT Teams are not directly responsible for the physical security and environment of the sites.
- Physical security controls and the environment in which the IT systems operate form part of a system's overall risk landscape. All users ensure they adhere to the security controls and requirements set out in this policy.
- Unless otherwise formally agreed by the , all users, including agency staff and contractors who have access to data, require Baseline Personnel Security Standard (BPSS) assessment, as a minimum.
- National Security Vetting should only be applied for where it is necessary, proportionate, and adds real value.
- The does not have a standing requirement for system administrators or application developers to maintain Security Check (SC) clearance.

Further information on physical and personnel security is available from and CPNI Guidance.

Identity and access control

The ensures that information and IT assets can be accessed only by authorised personnel, and that each individual is accountable for their actions.

The guide outlines the controls and processes designed to limit access based on a "need to know" basis, and according to defined roles and responsibilities.

The addresses access control principles such as identification, authentication, authorisation, and accounting.

Password management

The sets out the requirements for strong password implementation and management, to help prevent unauthorised access to systems. Examples include password creation, authentication, storage and management.

Email security

The tells you about safe and secure use of email within the .

The more detailed specifies the controls and processes required to protect the 's email systems from unauthorised access or misuse, that may compromise the confidentiality, integrity or availability of the data stored and shared within them.

The guide outlines the various security levels required to transfer information from the 's email servers to organisations outside the and other government departments. It covers topics such as the threats to email security (phishing) and secure email transfer.

Remote working and portable devices

The has in place guidance that sets out the requirements for safely accessing and using the 's systems and applications when working remotely, for example from home, another government office, or while travelling.

Mobile computing is the use of portable equipment such as mobile phone, laptop or tablet, and which supports remote working. Mobile computing equipment provided by the must be used in line with the .

Any request to take IT equipment overseas must follow the guidance provided in the and the information on accessing IT systems from overseas.

Malware protection

The specifies the controls and processes that be used to protect all systems against malware. Malware might enter the by employee email, through the internet, mobile computers, or removable media devices.

The addresses the following relevant domains:

- Implementation controls to stop malware entering devices and systems.
- Preventing malicious code from executing on devices and systems.
- Mitigating the impact of malware when entering devices and systems.

Roles and responsibilities

All users are responsible for ensuring the confidentiality, integrity, and availability of data within the . This includes all data and assets. These responsibilities extend to all assets referenced in this policy.

All users comply with the roles and responsibilities outlined in the Information Assurance Framework Process.

Specific roles and responsibilities are described within each sub-page. All users comply with these roles and responsibilities, and understand these as being a part of their ultimate responsibility for information security within the .

For the purpose of this Information Security Policy, the following roles are described. They have specific responsibilities in the implementation and monitoring of different provisions of the policy.

Role	Responsibility	Which includes...
Senior Information Risk Owners (SIROs)	The SIRO is responsible for the overall information risk policy and guidance, and ensures that the policy and guidance material continues to provide appropriate risk appetite and a suitable risk framework.	Implementing and managing information risk management in their respective business groups.
		Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.

Role	Responsibility	Which includes...
		Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.
Delegated Agency SIROs	The delegated agency SIRO is responsible for the information risk policy and guidance as it applies to their systems and personnel, and ensures the agency adheres to the 's risk appetite and risk framework.	In line with the SIRO, but for Agency systems and personnel.
Information Asset Owners (IAO)	IAOs, also known as IA Leads, must be satisfied that all required technical, personnel, physical and procedural security controls are in place and followed. IAOs are responsible for ensuring the management and security of their information asset over the whole asset lifecycle.	Logging and monitoring.
		Reviewing access permissions.
		Understanding and addressing risks associated to their information assets.
		Ensuring secure disposal of information when it is no longer required.
System Owners	System Owners are responsible for managing access control rules for their particular system.	Verifying access rights in order to assist a scheduled review audit of User accounts and permissions.
Contract Owners	Contract Owners are responsible for ensuring contractors adhere to the IT Security Policy set out here and in associated documentation.	Verify that contracts are written to reflect the 's IT Security Policy.
		Ensure contractors comply with the requirements set out by this policy and associated documentation.
		Being responsible for escalating the risk of non-compliance by a supplier, and seeking guidance on suspected non-compliance with security requirements in a contract.
		Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the , is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.

IT Security Technical Users Policy
Introduction

This policy provides more information on the actions expected of Technical and Service Provider users when using equipment and infrastructure. It is a sub-page to the IT Security Policy Overview.

Audience

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the .

Vulnerability scanning and patch management

The outlines the requirements for maintaining up to date systems and equipment to protect them from security vulnerabilities.

The guide includes patching schedules for the different systems and equipment according to their risk levels. It sets out the vulnerability ratings used to understand the criticality of a system security vulnerability. The guide addresses the following areas:

- Patching schedules and technical guides.
- Scanning requirements for different systems.

Technical controls

The ensures protection from unauthorised access or misuse of the IT systems, applications, and data stored within them.

The policy outlines the control design requirements that are needed to secure the network and IT assets in accordance with the three layers of defence. The policy addresses the following areas:

- Enforcing access controls in support of the .
- Building adequate security for the network and network boundaries.
- Creating secure software development and software configuration processes and designs.
- Monitoring the network against malicious code and anomalous behaviour.

Cryptography

Cryptography is a method of securing information and communication channels to allow only authorised recipients and personnel to view the information. The 's IT systems use cryptographic technologies to provide secure connections to third party systems or to protect information "at rest" on user devices, including laptops and mobile devices.

However, where staff have procured key material or hardware through the United Kingdom Key Production Authority (UKKPA) or any other cryptographic items where National Cyber Security Centre (NCSC) dictate that national cryptographic policy applies, the NCSC dictate the policy. In this case, the (previously HMG IA Standard No. 4, Protective Security Controls for the Handling and Management of Cryptographic Items, IS4) applies.

Note: IS4 can be accessed by joining the Cyber Security Information Sharing Partnership (CISP) and joining the UKKPA-Crpy Key Policy and Incident Management Group.

The 's Staff who use cryptography ensure they have the appropriate level of security clearance. This requires secret (SC) level clearance for managing cryptography.

The Chief Information Security Officer (CISO) is accountable to the Senior Information Risk Owner (SIRO) and Senior Security Advisor (SSA) for ensuring the 's compliance with the minimum cryptography requirements.

Software development

The ensures that all in house development, including development performed by third parties, is performed according to industry best practices and standards, as laid out in the Software Development Lifecycle Guide (SDLC).

All developers ensure they are aware of the importance of security when developing software and applications for use. The SDLC addresses the required methodology to be used in code development, and the security concerns that be accounted for during the development lifecycle.

Security incident management

The 's covers the end-to-end incident lifecycle, and provides the guidance for the to respond effectively in the event of an IT Security Incident, which includes security incidents. Examples of topics covered are preparation for incidents, escalation and incident response, and recovery activities, including containment, resolution, and recovery.

The IT Security Incident Response Plan and Process Guide provides additional detail to the policy, but also further guidance around Incident Response Team assembly and communication channels.

Suppliers and procurement

IT Security

For the Information Assurance Framework Process to be effective, it must extend to organisations working on behalf of the or handling assets, such as contractors, offshore or nearshore managed service providers, and suppliers of IT systems. Within the Framework, the Contract owner is responsible for ensuring that:

- The supplier service delivery be regularly monitored, reviewed, and audited.
- When the buys IT goods, services, systems, or equipment, IT security implications be considered.
- All IT suppliers who handle and store information on behalf of the be assessed annually against the (previously HMG Security Policy Framework) and the 's IT Security Policy. Additional self-assessment requirements may be stipulated in the contract between the IT supplier and the . The 's IT suppliers are responsible for carrying out these self-assessments, and for submitting those assessments to the . The is responsible for approving the assessments submitted by the supplier.
- The appropriate measures be put in place for any supplier not meeting compliance requirements, and the relevant teams be notified and consulted.
- All suppliers and contractors adhere to the GDPR and the Data Protection Act 2018.

Further advice can be found in the .

Physical and personnel Security

The Contract owner include appropriate clauses in a contract with any supplier which will define the classified matter that is furnished, or which is to be developed, under said contract. This will include any relevant personnel security controls such as security clearance. Not all contracts will require such clauses, but where they are required, and failing the inclusion of this information in the contract, a separate is issued to the contractor along with the contract document.

Privileged users

The 's Privileged User Guide sets out the key responsibilities for administrator roles within the in order to protect systems, assets and applications from unauthorised access, use, modification, or damage.

The guide sets out the security controls and processes required for the secure handling of assets and data stored and processed within them, such as the management of administrator accounts and secure configuration and change management.

Risk management

Technical risk assessment and information assurance

The risk assessment and information assurance is defined in the Information Assurance Framework Process, which requires that all IT systems that manage or are connected to government information be assessed to identify technical risks.

Audit

A security audit is a systematic evaluation of the 's IT security management system. It is performed to maintain effective security policies and practices. These checks are subject to self or peer audit by operational line management, contract managers or HQ managers, as judged to be appropriate by the managers with responsibility for delivery. For instance, checks on Information Asset Registers and Information Risk Registers be carried out quarterly, but other information assurance checks might be carried out less frequently, or triggered by events such as contract renewals.

Third party audits will be carried out by the Government Internal Audit Agency (GIAA) to provide an external evaluation of policies and practices. For more information, contact the Government Internal Audit Agency:

When conducting an audit:

- Documentary evidence be made available to auditors upon request.
- Details provided include the implementation of any technical security control in an IT system. Documentary evidence of changes be reviewed.
- The evaluation cover all types of changes, including configuration changes, to IT systems, and the IT security implications of those changes. This includes the case where no significant IT security impacts are identified.
- Evidence of operating effectiveness for technical controls be provided, and the desired risk mitigation as documented in the Information Assurance Framework Process.
- Activities involving verification of operational systems be carefully planned and agreed to minimise disruptions to business processes.

Line Manager approval

This guidance applies to all staff and contractors who work for the .

Some IT Policy documents need you to get a review or approval from a Line Manager or other senior person. Do this before taking an action or working in a particular way.

An example is:

- Personal Devices.

This guidance describes what you should do. The guidance contains steps to follow for Line Managers, and their Direct Reports.

Steps to follow (Line Managers)

Note: If at any time you need help about this process, or the applicable IT Policies, just ask: .

1. Check that your direct report (DR) has said what they want in their request. The request should identify which IT Policies apply.
2. Check that the request is valid from a business perspective. If not, deny the request (step 7).
3. Check that Acceptable Use is in the list of applicable policies.
4. Review the requirements or obligations within the IT Policies that apply to the request.
5. Check that the DR understands and will follow the requirements or obligations. For example, have a discussion with them, or ask them for more information or evidence.
6. If they are able to follow the applicable IT Policies, send a formal approval to the DR. An email is enough for this.
7. If you don't think they can follow the Policies, or there's a weak business case for the request, refuse it.
8. Keep a copy of your formal reply, in accord with Data Retention requirements.
9. Some IT Policies need a copy of formal approval for other parties. For example, before your DR travels to some countries on business, send a copy of your approval to .

Steps to follow (Direct Reports)

Note: If at any time you need help about this process, or the applicable IT Policies, just ask: .

1. Check that your business need is valid.
2. Check which IT Policies apply to your request. Include Acceptable Use in the list of applicable policies.
3. Check that you understand the requirements or obligations within those IT Policies.
4. Prepare evidence to show that you will follow all the requirements or obligations. Check that you have all the required information.
5. Send a formal approval request to the authorities required by the IT Policies. Ensure that you include:
   - Your request.
   - The business case.
   - The list of applicable IT Policies.
   - Evidence that you understand and can follow the requirements or obligations.
6. Be ready to have a more detailed discussion about your request, or to supply more information.
7. If you get formal approval, keep a copy, in accord with Data Retention requirements.
8. If your request is denied, check that you understand the reasons. Use this understanding to tackle your business task again, if appropriate.

Shared Responsibility Models

The by default will leverage shared responsibility models, particularly in commodity environments, in order to achieve efficiencies such as time, risk and cost.

The believes that it should focus on elements which are unique to its requirements rather than attempting to solve commodity requirements in a unique way.

h/t https://aws.amazon.com/compliance/shared-responsibility-model/

Assessments

The conducts assessments (including risk assessments) where appropriate to ensure it understands the shared responsibility model, its obligations under the same and measure how third-parties are meeting their obligations.

Inherited

The inherits controls which are fully controlled and managed by a third-party, such as physical and environmental controls in a data centre.

Shared

has shared controls which is jointly responsible for with the third-party, for example:

- Patch Management - AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management - AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

specific

The is responsible for appropriate use within its partnership or 'tenancy' of a third-party supplier or product.

For example, in AWS, must correctly leverage native AWS functionality (such as Security Groups) to protect systems/data, and only the can implement these.

Technical Controls Policy

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.TCP.xxx**, where **xxx** is a unique ID number.

Related information

System Backup Policy on page 182
Acceptable Use Policy on page 52
Access Control Policy on page 89
Code of connection standard on page 233
Information Classification and Handling Policy on page 75
IT Security Incident Management Policy on page 334
IT Security Policy (Overview) on page 22
Malware Protection Guide - Overview on page 174
Offshoring Guide on page 155
Passwords on page 116
Patch Management Guide on page 230
Protective Monitoring Guide on page 194
Secure disposal of IT equipment on page 77
Secure disposal of IT - physical and on-premise on page 78
Secure disposal of IT - public and private cloud on page 80
System Backup Policy on page 182
System Lockdown and Hardening Standard on page 151
System Test Standard on page 311
Use of HMG Cryptography Policy on page 143

Approach to technical controls

The relies heavily upon IT systems to support service delivery in all business groups. This policy covers the technical security controls required for all IT systems.

This document outlines the minimum baseline standard for the application of technical security controls which applies to all IT systems. Each IT system is different and it is intended that IT systems will be assessed and a judgement made on the applicability of the technical controls outlined in this policy.

POL.TCP.001: All IT equipment and systems comply with this policy, which outlines the minimum baseline standard, when considering technical security controls. This includes where appropriate, the standards, guides and procedures which support this policy.

POL.TCP.002: All IT systems provide evidence that this policy has been considered and the appropriate technical controls selected.

POL.TCP.003: All IT systems have their security architecture documented. This can be within an existing system architecture document or where appropriate within the relevant section of risk management documentation.

Overarching objectives

The objectives of this policy are:

- To facilitate the consistent application of technical security controls across the where similar controls and configurations are applied in a similar manner to a common standard.
- To support business continuity by promoting standard configuration which will make it easier to re-provision or re-build systems.
- By providing a minimum baseline technical security requirement for all IT systems, the appropriateness of those controls can be reviewed centrally against future security developments and Information Assurance strategy.
- Reduce the cost of implementing IT systems by ensuring security considerations are considered at the start of the development process shaping the requirements and providing input into system design.

Technical controls lifecycle

The development and operation of an IT system follows a project lifecycle from initial design through to disposal where Information Security needs to be including and considered at every stage.

POL.TCP.004: The selection of technical security controls be based on a technical risk assessment. For systems covered under the accreditation process, this is an assessment conducted following HMG Information Assurance Standard No. 1 and 2.

POL.TCP.005: All IT systems have all selected technical security controls operationally active before use in a live environment. Any exceptions are at the discretion of the system Accreditor, IAO or SIRO.

POL.TCP.006: All IT systems be tested in a Non-Live Environment (NLE) prior to going into live operation. This includes the testing of any security controls and features.

POL.TCP.007: All IT systems use live data in system testing. Any exceptions are at the discretion of the system Accreditor and approved by the business group SIRO.

POL.TCP.008: All IT systems use live personal data in system testing. Any exceptions must be approved by the IAO or SIRO, this approval process is managed by the Data Access and Compliance Unit (DACU).

POL.TCP.009: All IT systems enforce separation between test environments and live operational environments.

POL.TCP.010: All IT systems be tested in line with the System Test Standard, this includes conducting a secure code review.

Protection of system test data

IT System test environments generally do not implement all the security controls and operating procedures present in a live operational environment. As such it is important to consider what security controls are required to protect both the system source information (for example source files and configuration data) and any test data utilised.

POL.TCP.011: Where an IT system uses live test data or test data which attracts a HMG protective marking, the system test environment or NLE be accredited to process data at that protective marking.

Assurance and Compliance

The IT Security Policy describes how the manages information security risk and the information assurance arrangements in place to ensure that any information security controls adopted are adequate and operating correctly.

Compliance to HMG Information Assurance Standards

For IT systems operating in an HMG environment, general security standards are provided centrally from the to ensure that across HMG, a consistent approach is applied.

POL.TCP.012: All IT systems ensure that they comply with HMG Information Assurance standards. This includes the assessment of technical risk, selection of controls and their implementation. The primary reference is .

Technical review of operational changes

POL.TCP.013: All IT systems have all operational changes reviewed and approved by IT IA prior to any system change. This is to ensure the risk profile of a system is not significantly altered by the change and that any required technical security controls have been considered.

Note: An Accreditor may decide that a particular system change requires a revision to that system's accreditation. This could involve updating the risk management documentation where appropriate.

Physical Security of IT Assets Policy

The physical environment in which an IT system is used often influences the design decisions taken regarding which technical security controls are required to attain the desired risk mitigation.

POL.TCP.014: The physical location and environment an IT system will operate in be considered when selecting technical security controls. This includes any IT equipment used in a remote working environment.

POL.TCP.015: Where an IT system is provided under contract, that contract specify the responsibilities for equipment and IT Security at any service provider, , or other third party sites used.

POL.TCP.016: Where IT equipment for IT systems are located at a third party site, the security of these assets be documented and agreed with IT IA.

Physical security is the responsibility of Corporate security and business continuity branch where further information can be found at.

POL.TCP.016.001: Buildings and premises used to store and process HMG protectively marked information need to meet a specified HMG standard, this includes supplier premises. Corporate security and business continuity branch be consulted and can provide further advice.

An example of where IT Security controls are influenced by the physical environment is where a desktop terminal (with access to sensitive information) is located in an area where it can be overlooked by members of the public. Supplementary technical and procedural controls are required to balance the additional risk posed.

Cabling security

All IT systems have some form of cabling, whether it is for power, network connectivity or connections to peripheral devices.

Cabling itself needs to be protected against potential threats such as the compromise of confidentiality due to physical access (such as unattended network ports in a public area) or loss of availability due to power cabling running through an area which is liable to flood.

POL.TCP.017: Any technical risk assessment examine the risks associated with cabling within an IT system.

POL.TCP.018: All IT systems consider the need to separate cable trunking where justified by the Business Impact Assessment (BIA) and risk assessment. Further advice can be sought from Corporate security and business continuity branch.

Network cabling in particular is prone to electronic interference or interception.

Equipment maintenance

Maintenance of IT equipment can support Information Security by ensuring systems continue to meet their integrity and availability requirements but it can also introduce new security risks.

POL.TCP.019: Equipment be appropriately maintained to ensure continued availability and integrity.

POL.TCP.020: All IT systems provide documented evidence of a maintenance regime or support arrangements. This could be within risk management documentation or referenced support agreements or contracts.

POL.TCP.021: Any piece of IT equipment taken offsite for maintenance or repair which may contain protectively marked data or personal information be approved via an operational change request by IT IA. Pieces of IT equipment which fall into this category include (but are not limited to):

- Magnetic Storage Media
- Solid State Drives
- Optical Media
- Digital printers, copiers, and, multi-function devices
- Networking Equipment
- Personal Electronic Devices

POL.TCP.022: Any piece of IT equipment which has been taken offsite for maintenance or repair be assessed and tested before integration or installation back into a IT system. This activity must be approved via an operational change request by IT IA.

Note: One change request can be used to cover both the removal to an offsite location and its return.

POL.TCP.023: Where sanitisation of a piece of IT equipment is required prior to any maintenance or repair, this be completed according to HMG Information Assurance Standard No. 5.

POL.TCP.024: All IT systems maintain a log of maintenance activity noting any IT IA approvals where appropriate.

On some occasions, IT equipment may be decommissioned rather than repaired.

TEMPEST

IT systems which process or handle protectively marked information can produce unintended emanations which can compromise the information being processed or be used as a covert channel to compromise the system as a whole. This activity, its investigation, testing and suppression, is collectively known as TEMPEST within HMG.

POL.TCP.025: Where a technical risk assessment has indicated that TEMPEST threats pose a risk to an IT system, TEMPEST controls must be considered. The application controls follow CESG Good Practice Guide No. 14.

Identity and Access Management Policy
Access Control

Access to IT systems must be controlled on the basis of business need and security requirements. Access control rules and rights for each user or group of users must be clearly stated in an access control statement (within risk management documentation or other referenced security documentation) and assessed through a Business Impact Assessment (BIA).

For end Users, this is presented through an IT system's Security Operating Procedures (SyOPs). Further details are provided in the Acceptable Use Policy.

POL.TCP.026: All IT systems provide a secure access control mechanism which can be configured to restrict access to both system functionality and information assets processed or stored.

POL.TCP.027: All IT systems use the appropriate access control mechanism based on the method of access and risk assessment (for example, remote access where two factor authentication is assessed to be appropriate).

POL.TCP.028: Access to an IT system (and functionality provided) be provided on a 'need-to-know' (least privilege) basis. Any additional privileges only be granted through a valid business case signed-off by the business system owner or a senior manager.

POL.TCP.029: Any access control solution take into consideration the Information Classification and Handling Policy.

POL.TCP.030: All IT systems define and maintain an access control schema which aligns to the IT Security Policy.

POL.TCP.031: All IT systems follow the Access Control Policy.

User Identity Management

Management of user identities on IT systems is important to ensure access to services and information is on a 'need-to-know' basis and end users actions can be monitored and correctly attributed.

POL.TCP.032: All IT systems have a process for managing User identities covering the full lifecycle (from creation to removal), this includes where a User changes role or business group. This must be in line with the Access Control Policy.

Note: The lifecycle for User identities needs to be mapped onto the HR processes for new joiners and leavers. Refer to the Intranet for more information.

User Registration

POL.TCP.033: All IT systems have or use a formal user registration and deregistration procedure to control the allocation and removal of access rights.

POL.TCP.034: Each User on an IT system have a unique User IDs which can be used to record their actions on that system. The use of group IDs will only be considered on a case by case basis by the system Accreditor (for example, legacy systems which may not provide the functionality for unique User IDs).

POL.TCP.035: A check be made to ensure a User is authorised to access an IT system before being granted their access credentials (for example, from a system owner or senior manager). This includes ensuring only the appropriate access required by that User is granted.

POL.TCP.036: Users be made aware of their access rights to an IT system.

POL.TCP.037: All IT systems maintain a formal record of all Users registered on that system.

POL.TCP.038: All IT systems have a process for periodically checking and removing redundant User IDs and accounts.

POL.TCP.039: All IT systems ensure that a redundant User ID is not recycled and issued to other User.

Privilege Management

Most IT systems provide access to a number of services and information assets. In general, a particular User does not need access to every service or information asset. As such, privileges and privilege management provides a mechanism to restrict user access and enforce principles such as 'need-to-know'.

POL.TCP.040: The privileges associated with each component of an IT system (e.g. operating system, database and applications) be categorised and grouped together into appropriate roles which can be assigned to individual Users.

POL.TCP.041: Privileges be allocated on a 'need-to-know' (least privilege) basis.

POL.TCP.042: Where appropriate, any allocation of privileges which allows a User to perform system administrative functions be assigned to a different User ID from the User ID used by that User for normal business functions.

POL.TCP.043: Segregation of duties be considered in the allocation of privileges.

User Password Management

POL.TCP.044: The requirement for an IT system to be protected by a password be derived from a technical risk assessment (using HMG Information Assurance Standard No. 1 and 2 for systems undergoing the accreditation process) and a Business Impact Assessment (BIA).

POL.TCP.045: The standard on password generation, composition and management is contained within the Password guidance. All IT systems which use passwords for access control follow this standard.

POL.TCP.046: All supplier or vendor supplied passwords be changed before live operation.

POL.TCP.047: All IT systems have a process to change any passwords which have been compromised.

Though passwords are the primary method of User authentication, other technologies for User identification and authentication, such as biometrics and hardware tokens should be considered where appropriate.

Review of user rights

To maintain effective control over who has access to which information assets and services, access rights and privileges need to be regularly reviewed.

POL.TCP.048: All IT systems have and follow a process to review user access rights and privileges on a regular basis and the capability to change those rights, as required, in a timely manner.

POL.TCP.049: All IT systems have the capability to provide a report on all user access rights upon request.

Network Security Policy

Network security is a combination of security controls, the architecture in which those controls are deployed and, the processes and procedures which direct their operation.

POL.TCP.050: The risk assessment for an IT system include an assessment of the threats and vulnerabilities to or from any IT network supported by or utilised by that system.

POL.TCP.051: All IT systems implement controls to ensure the Confidentiality, Integrity, Availability and Accountability of data in transit across any networks utilised. This includes ensuring correct network routing.

POL.TCP.052: All IT systems implement controls to protect any exposed services (i.e. those made available for use across a network) from unauthorised access. This includes remote access services.

POL.TCP.053: Based on a Business Impact Assessment (BIA) and technical risk assessment, where appropriate as directed by the Accreditor, an IT Heath Check be conducted on all IT systems. The type of check conducted must be inline with the segmentation model detailed in HMG Information Assurance Standard No. 1 and 2.

POL.TCP.054: All IT system follow the Enterprise Security Architecture Framework. This framework provides details on architectural patterns for secure system design and guidance on network segregation.

Network access control

Much like User access control, network access controls seeks to control access to network services and systems. networks are generally shared networks, with some extending across organisational boundaries and outside of the itself.

POL.TCP.055: All IT systems implement appropriate authentication mechanisms for access to network devices (e.g. servers, printers, network storage and routers). This includes access to devices from an internal network.

POL.TCP.056: Where an IT system connects to an external network, network security controls be implemented to enforce separation between the two networks and restrict data flow and access between the two networks.

POL.TCP.057: The selection and application of network access controls follow the Enterprise Security Architecture Framework.

Application Security Policy

The strategy for the comprehensive application of Information Security is often described as 'Defence in Depth'. This is to say, security controls should be appropriately considered at all levels of an IT system. It is therefore important to assess what security controls need to be applied at the application level.

POL.TCP.058: The risk assessment for an IT system include an assessment of the threats and vulnerabilities to any application supported by or utilised by that system.

POL.TCP.059: All software applications which form an IT system be patchable and supported.

POL.TCP.060: Commercial Off The Shelf (COTS) supplied software be maintainable with appropriate support arrangement/agreements in place based on an IT system's risk assessment.

POL.TCP.061: Where an application is developed for the (i.e. is not COTS products), a defined process for identifying and rectifying security issues be established.

POL.TCP.062: Where applicable, an application be within the scope of an IT system's IT Health Check (ITHC).

POL.TCP.063: All IT systems follow the Enterprise Security Architecture Framework. This framework provides details on standard security features and secure development practices which must be considered.

Protective Monitoring Policy

All IT systems are monitored to detect non-conformance to policy and record auditable events providing evidence to help diagnose and investigate security incidents.

POL.TCP.064: All IT systems provide the capability to audit events whether initiated by a User or system process.

POL.TCP.065: All IT systems implement a set of audit points which are in accordance with the Protective Monitoring Guide.

POL.TCP.066: All IT systems be included in a protective monitoring solution. The level of monitoring required must be determined using HMG Information Assurance Standard No. 1 and 2, and CESG Good Practice Guide No. 13.

POL.TCP.067: All audit logs be securely stored to protect the confidentiality of the data contained.

POL.TCP.068: All IT systems implement controls to protect the integrity of audit and accounting logs.

POL.TCP.069: All IT systems synchronise all IT devices with a consistent time source.

POL.TCP.070: All audit and accounting logs be retained in accordance with stated data retention period as expressed by Information Asset Owner (IAO) and recorded in the system risk management documentation (refer to the logging and monitoring information).

POL.TCP.071: All IT systems follow the Protective Monitoring Guide, where further guidance is provided.

Interface with Security

The is responsible for managing security incidents involving IT systems and information assets. As such, they are the primary consumer of any protective monitoring solution as it is a key feed of information and mechanism for raising security incidents.

POL.TCP.072: All protective monitoring solutions provide the capability to report security incident (or the audit and log data which can be used to generate security incidents) to the .

POL.TCP.073: All IT systems provide their audit logs to the upon request.

Further information on IT incident management is available in IT Security Incident Management Policy.

Connection with 3rd Party Systems Policy

Working with other Government departments and establishing partnerships with other organisations is common practice at the .

In the context of this policy, the definition of a 3rd party system is any system which is not a internal network. Therefore, a 3rd party connection is a connection between a internal network or system and an external network or system for system-to-system data transfers. This includes other Government department using the GSi.

Where there is a business need for such third party access, a risk assessment needs to be carried out to determine the security implications and control requirements. Security controls must be agreed and defined in an agreement or contract with the third party before a connection is provided.

POL.TCP.074: All IT systems which connect to a 3rd party system or share information with any 3rd party include the following in the technical risk assessment:

- Access to information assets by 3rd parties;
- Compliance to applicable legal or regulatory requirements;
- Security of network connection;
- Business continuity.

POL.TCP.075: All IT systems which connect to or share information with a 3rd party system ensure a Code of Connection is drawn up, understood and signed by each connected parties Information Asset Owner (IAO). An Information Sharing Agreement is also required.

POL.TCP.076: Where 3rd party access involves other participants, for example subcontractors, this be brought to the attention of the system Accreditor for approval where any agreements made with the 3rd party will also be considered applicable to any further participants.

POL.TCP.077: Where an IT system is connected to a 3rd party for the purposes of offshoring, it comply with Offshoring Guide.

POL.TCP.078: Any Codes of Connection comply with Code of connection standard.

Security of 3rd party access

When connecting to a 3rd party system, the security controls deployed on either side of the connection need to be considered and assessed.

POL.TCP.079: A process be defined for controlling and notifying transmission, despatch and receipt of data to/from a 3rd party.

POL.TCP.080: An agreed protective marking system be used for all data transfers. By default, this is the HMG protective marking system.

POL.TCP.081: All IT systems which connect to or share information with a 3rd party system ensure that adequate security controls are in place to:

- Protect against virus or malware infiltration and malicious attack;
- Provide adherence to Acceptable Use Policy and Information Classification and Handling Policy where applicable.

POL.TCP.082: All connections meet the minimum technical standard detailed in the Code of Connection Standard. Where HMG cryptographic material is required, additional policy requirements are detailed in the Use of HMG Cryptography Policy.

Secure storage and processing of Information Assets

The HMG protective marking system defines how information needs be labelled and handled. Further information on the marking system can be found in Information Classification and Handling Policy.

POL.TCP.083: All IT systems which handle HMG protectively marked or personal data be accredited to the assessed Business Impact Level (BIL) as captured in a Business Impact Assessment (BIA). Any exceptions are at the discretion of the system Accreditor.

POL.TCP.084: All Users of an IT system be aware of the protective marking which the system is operating at. Where it is not feasible to label each screen viewed by a user which contains protectively marked information, a message be displayed on successful log-on advising the user of the protective marking of the information held on that system.

POL.TCP.085: All electronic outputs from an IT system containing protectively marked information carry the appropriate protective marking. This includes MS Word documents, e-mails and system-to-system data transfers.

Aggregation policy

POL.TCP.086: The risk assessment of an IT system consider the business impact should the aggregated sum of data held on system be compromised (in terms of Confidentiality, Integrity and Availability). This assessment must be made with reference to HMG Information Assurance Standard No. 6 and CESG Good Practice Guide No. 9.

Personal Data

HMG outlines specific requirements on the protection of personal data as documented in HMG Information Assurance Standard No. 6. All Government departments need to follow these requirements to ensure personal data is correctly stored, processed and handled on IT systems.

POL.TCP.087: The definition of personal data is derived from HMG Information Assurance Standard No. 6. Any information assets in an IT system assessed as personal be labelled, as a minimum, .

Note: Further details on the application of an HMG protective marking is provided in the Information Classification and Handling Policy.

Use of Cryptographic Controls

HMG cryptographic material is used within IT systems mainly to secure communications with IT assets which are not directly connected to a network, for example remote access laptop. HMG maintains strict requirements and controls over the deployment and use of HMG cryptographic material which the has to follow.

POL.TCP.088: Any IT system which utilises HMG cryptographic material in any technical security controls (e.g. VPN solution) conform to the Use of HMG Cryptography Policy.

Secure System Build and Configuration Policy

Capacity planning

IT system managers need to monitor their system and network usage so that they are able to provide an early warning of any potential capacity shortages, bottlenecks, or overcapacity.

POL.TCP.089: All IT systems consider capacity planning during system design and operation to ensure continued availability.

POL.TCP.090: Capacity planning take account of the need for current and future audit and logging requirements.

POL.TCP.091: All IT systems monitor system and network usage and provide the capability to detect potential capacity issues or bottlenecks.

POL.TCP.092: All IT systems report any potential capacity issues to Service Management preferably in advance of any immediate issues.

Patching policy

Patches and Service Packs, in general, are updates to software or firmware to fix a bug or provide additional functionality. A security patch is a change typically applied to a software asset to correct a vulnerability which if exploited could compromise that asset and others on an IT system or wider network.

It is important to ensure IT systems are kept up to date with the latest security patches as any known vulnerability is highly likely to be exploited by a threat source.

POL.TCP.093: All IT systems, including operating systems and applications, be subject to a security vulnerability patching regime consistent with the level of criticality of the IT system to the business in accordance with the Patch Management Guide.

POL.TCP.094: Security patches be applied in a timely manner according to their categorisation in accordance with the Patch Management Guide.

POL.TCP.095: All IT systems have a Patch Management Plan. This plan must include a process for managing, testing and deploying security patches. Further details are available in the Patch Management Guide.

The Patch Management Guide provides the baseline standard and template patch management plan. This standard provides details of patch categorisation (based on the severity of the vulnerability and criticality of update) and the expected timescales for applying a particular patch based on its categorisation.

Lockdown policy

POL.TCP.096: All unnecessary or unused applications, services (including system services) and functionality be removed or disabled from all IT systems.

POL.TCP.097: Where applicable, Government Assurance Pack (GAP) be considered for MS Windows based systems.

POL.TCP.098: All IT desktop and server hardware be locked down to remove, prevent or limit access to non-business critical communication ports (e.g. USB port), removable media drives (e.g. CD Drive) and network communication interfaces (e.g. infrared or Bluetooth).

POL.TCP.099: All IT desktop and server hardware be built using a standard build, where possible, where the security of the build has been assessed and approved by IT IA.

POL.TCP.100: All IT systems be locked down in accordance with System Lockdown and Hardening Standard. This standard describes general lockdown procedures supplemented by system specific procedures. For example, a set of specific procedures for MS Windows based application servers.

Protection from malicious code

Preventative measures are required to detect and defend against the introduction of malicious code, and to protect against mobile code threats (for example JavaScript or ActiveX code executing malicious code in a web browser).

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses and logic bombs.

POL.TCP.101: All IT systems have an anti-virus client installed on each desktop and/or server configured to conduct regular anti-virus scans with real-time scanning activated.

POL.TCP.102: All anti-virus clients be updated with the latest virus definitions to a schedule outlined in the Malware Protection Guide. The default limit is within 4 hours of release by the anti-virus client vendor.

POL.TCP.103: All imports and exports to an IT system received from an external network or via removable media must be scanned for viruses and malware prior to being loaded on that system. This includes e-mails as well as system-to-system transfers.

POL.TCP.104: All IT systems have a procedure to report any virus or malware instances. As standard, this must be an alert to the User and to the .

POL.TCP.105: All IT systems refer to the Malware Protection Guide when selecting security controls to protect against malicious code and threats from mobile code.

Note: All malicious code instances must be recorded as an IT Security incident. Further details are provided in IT Security Incident Management Policy.

Covert channels and Trojan code

A covert channel is where information can be exposed by an indirect or obscure method. Trojan code is designed to change the way an application or system operates in a way that it appears to be operating normally however it contains code which can perform unauthorised actions.

POL.TCP.106: All IT systems be analysed for potential covert channels which are either present in the system design or exposed through any of the applications hosted.

POL.TCP.107: Where a risk assessment indicates that Trojan code is a threat, all applications hosted by an IT system be tested for potential Trojan code.

Further details and guidance on the prevention of covert channels and Trojan code in application can be found in the Enterprise Security Architecture Framework.

Data Backup

Data back-up arrangements for IT systems support the overall business continuity plans of the .

POL.TCP.108: All IT systems have back-up procedures to maintain the integrity and availability of all Information Assets held. This must align to the Recovery Point Objective which may be expressed in the Business Impact Assessment (BIA).

POL.TCP.109: All IT systems maintain a log of all back-ups taken.

POL.TCP.110: Back-up data be stored and handled in a manner appropriate to the protective marking of the Information Assets stored.

POL.TCP.111: All IT systems check all historic back-ups regularly to ensure that they can be relied upon. This includes the testing of back-up media such as tape or hard disks.

POL.TCP.112: All IT systems have a back-up restoration procedure which is tested regularly. Ideally, the testing takes place automatically.

POL.TCP.113: The retention period for historic back-ups align to the retention period of the Information Assets held.

POL.TCP.114: All IT systems conform to the System Backup Policy.

Electronic Messaging Policy
Electronic mail (E-Mail)

E-mail presents a number of security challenges as it provides a channel for malware proliferation and for the exfiltration of sensitive information assets out of the either accidentally or maliciously.

Note: The following policy statements are applicable to IT systems which are either, an e-mail system, or, make use of e-mail services provides by another system.

POL.TCP.115: All e-mails sent or received external to an IT network be examined for potential viruses (or malware) and its content inspected for adherence to the Acceptable Use Policy and Information Classification and Handling Policy where applicable.

POL.TCP.116: All IT systems which process e-mails must make provision to detect incorrect addressing or misdirection.

POL.TCP.117: All e-mail group distribution lists (e.g. ZZ distribution lists) be configured with a local address for internal distribution only. The use of an external address must be supported by a valid business case and is subject to approval by the ITSO.

Further details on the secure operating procedures applicable to the use of email are provided in the Acceptable Use Policy.

Configuration Management Policy

Configuration management is important to maintaining the operational security of live IT systems and ensuring any changes or disposal of assets is conducted in a secure manner.

POL.TCP.118: All IT system configurations be fully documented and version controlled.

POL.TCP.119: All IT systems maintain an asset inventory covering all hardware and software assets.

POL.TCP.120: All IT operational changes, system changes or upgrades be approved by IT IA prior to any change or upgrade taking place.

IT Asset disposal policy

IT assets at their end of life can contain data, system design or configuration details can be used to compromise IT systems in addition to potentially compromising the Confidentiality of information assets held.

POL.TCP.121: All IT systems have an asset decommissioning and disposal procedure.

POL.TCP.122: All IT system seek approval from IT IA before any disposal or decommissioning activity takes place.

POL.TCP.123: Disposal of IT assets be in conformance to Secure disposal of IT equipment guide.

Compliance with Legal Requirement

A number of pieces of legislation are relevant to Information Assurance (IA). To avoid breaches of any criminal and civil law all relevant statutory, regulatory and contractual requirements need to be considered when applying any technical security controls.

POL.TCP.124: All IT systems consider applicable legal and regulatory requirement when selecting, designing and operating any security controls. This consideration must be documented. This consideration must be document (for example in a system design document and/or RMADS).

Applicable pieces of legislation may include (but is not limited to):

- The Computer Misuse Act, 1990
- The Copyright, Designs and Patents Act 1988
- The Data Protection Act 1998
- The Official Secrets Act 1989
- The Public Records Acts 1958 and 1967
- Freedom of Information Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Civil Evidence Act 1968 and Police and Criminal Evidence Act
- Wireless Telegraphy Act 1949
- The Communication Act 2003

Mobile devices and teleworking

Mobile device policy

Mobile Device and Remote Working Policy

Introduction

This policy gives an overview of mobile devices and remote working security principles and responsibilities within the . It provides a summary of the 's related policies and guides in relation to mobile devices and remote working.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.MOB.xxx**, where **xxx** is a unique ID number.

Audience

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Any other business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services, including processing, transmitting,and storing data for, or on behalf of, the .
General users	All other staff working for the

“All users” refers to General users, Technical users, and Service Providers, as defined previously.

Mobile devices

POL.MOB.001: When using mobile devices, special care be taken to ensure that business information is not compromised. When issuing or using mobile devices, the following points be adhered to:

- **POL.MOB.002:** Mobile devices be registered as an asset.
- **POL.MOB.003:** Software installation be available for general users, except when using an approved process or tool, such as an self-service app store.
- **POL.MOB.004:** There be an ability for remote disabling, erasure or lockout.
- **POL.MOB.005:** approved web services and web apps be used.

Use in public places

POL.MOB.006: Care be taken when using mobile devices in public places, meeting rooms, and other unprotected areas. Protection be in place to avoid the unauthorised access to, or disclosure of, the information stored and processed by these devices.

The Cryptography guide offers techniques and information used in the to support stronger security when using mobile devices.

The Access Control Guide explains how the manages access to its IT systems so that users have access to the material they need, in a secure manner.

Theft or loss

POL.MOB.007: Mobile devices be physically protected against theft, especially when left unattended. Examples include leaving devices unattended in cars and other forms of transport, hotel rooms, conference centres, and meeting places.

Note: Sometimes, it might feel difficult to determine a sensible level of protection. For example, leaving a laptop unattended but in plain sight on the seat of car in a public car park is not very secure. But if the car is parked in an car park, then the vehicle - and therefore its contents - are probably more secure. The answer is that you should always apply the best possible protection for the assets you are responsible for, at all times. Don't rely on other security mechanisms to provide protection that you neglected to apply.

POL.MOB.008: The have, and follow, a clear procedure covering legal, insurance, and security requirements for cases of loss or theft of mobile devices.

Use of private equipment

POL.MOB.009: You use personal devices for work purposes.

Exceptions are possible on a case-by-case basis, for example to accommodate Accessibility requirements. To discuss whether you have a case for exemption, contact the Security team in the first instance, *before* using a personal device for work purposes. If an exception is permitted, use of the personal device be in compliance with personal device guidance.

Remote working

Remote working refers to all forms of business activity that takes place outside of the office. Remote working is sometimes described as “Working From Anywhere”. Remote working locations include non-traditional work environments or contexts, such as:

- Coffee shops.
- Commuter hubs.
- Co-working spaces.
- Flexible workplace.
- Home offices or workspaces.
- Telecommuting.
- Virtual Work Environments.

POL.MOB.010: The allows remote working, but the following points be considered, confirmed, and documented as acceptable during the approval process:

- The existing physical security of the remote working site, taking into account the physical security of the building and the local environment.
- The communications security requirements, taking into account the need for remote access to the 's internal systems, the sensitivity of the information that will be accessed and passed over the communication link, and the sensitivity of the internal systems being accessed.
- Any threat of unauthorised access to information or resources from other persons using the remote working location, for example family or friends.
- The implementation of home networks, and requirements or restrictions on the configuration of wireless network services (wifi).
- Malware protection and firewall requirements.

POL.MOB.011: The guidelines and arrangements for remote working be considered, including:

- The provision of suitable equipment and storage furniture for the remote working activities.
- A definition of the work permitted, the hours of work, the classification of information that may be held, and the internal systems and services that the remote worker is authorised to access.
- The provision of hardware and software support and maintenance.
- The provision of insurance.
- The procedures for information and asset backup, and for ensuring business continuity.
- Audit and security monitoring.
- Limitation or revocation of authority and access rights, and the return of equipment when the remote working activities are terminated.

Current supporting documentation:

- Remote Working
- Security Guidance for Using a Personal Device

Enforcement

This policy is enforced by lower level policies, standards, procedures, and guidance.

Non-conformance with this policy could result in disciplinary action taken in accordance with the 's Disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence,

they might also be prosecuted. In such cases, the department always cooperates with the relevant authorities, and provides appropriate evidence.

Remote Working
Key points

- Be professional, and help keep information and resources safe and secure at all times.
- Think about where you are working, for example - can other people or family access what you are working on? Be thoughtful about information privacy.
- Keep accounts and password information secure.
- Take care of your equipment. Devices are more likely to be stolen or lost when working away from the office or home.
- Get in touch quickly to report problems or security questions.
- Use the VPN if you are handling sensitive information, or connecting to systems from a remote location.
- Send work material to personal email accounts.
- Use personal devices or accounts for work purposes - the exception is that a home wifi connection may be used to connect equipment.
- Leave equipment unattended.

Overview

The Remote Working Guide gives you advice and guidance on the main security issues that are likely to affect you as a remote worker or a user of mobile computing facilities, (e.g. desktop/laptop computer, smart phones, etc), within the , including its Agencies and Associated Offices.

It also sets out your individual responsibilities for IT security when working remotely.

Audience

This guide applies to all staff in the , its Agencies, Associated Offices and Arm's Length Bodies (ALBs), including contractors, agency and casual staff and service providers, who use computing equipment provided by the Department for remote working or mobile computing, or process any departmental information while working remotely or while using mobile computing equipment.

What is remote working?

Remote working means you are working away from the office. This could be from home, at another or government office, whilst travelling, at a conference, or in a hotel.

Protecting your workspace and equipment

Remote working is when you work from any non- location, for example, working at home. It's important to think about confidentiality, integrity and availability aspects as you work. This means protecting equipment, and the area where you work.

- Keep equipment and information safe and secure.
- Protect information from accidental access by unauthorised people.
- Lock or log off your device when leaving it unattended. For long periods of non-use, shut down your device.
- Ensure that your devices are powered off when you first enter a country when travelling outside the UK.
- Keep your workspace clear and tidy. Follow a 'clear desk policy' for information, including paperwork, to ensure information isn't seen by unauthorised people.
- Use IT equipment for business purposes in preference to your own equipment such as laptops or printers.
- Be wary of anyone overlooking or eavesdropping what you are doing. Consider whether you, or the information, might be Overseen, Overheard, or Overshared.
- Protect chargers and other computer accessories, especially equipment, when travelling. This is to prevent them from being tampered with. Keep them secure and out of sight as much as possible, for example in your hand luggage or on your person.
- Ensure that a laptop BitLocker PIN or similar access control is enabled.
- Use an -issued VPN when connecting to Hotel or other public wifi spots.

- Let family or other unauthorised people use equipment.
- Leave equipment unattended.
- Work on sensitive information in public spaces, or where your equipment can be seen by others.
- Advertise the fact that you work with materials. However, pre-installed materials such as backgrounds provided as standard with equipment are acceptable.
- Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
- Send your work material to your personal devices or your personal email address.
- Redirect print jobs from printers to a personal printer.
- Use public 'charging stations' provided at airports, conference venues, hotels, or similar public locations. They might be used to upload malicious software onto your device.
- Connect equipment to vehicles, using either USB or Bluetooth. These connections can download information from the device or upload malicious software.

Working securely

It's important to consider the security of how you work remotely.

- **Work locations** - as with home working discussed previously, you need to be equally, if not more, vigilant when working in public spaces.
- **Confidentiality** - be aware of others eavesdropping or shoulder surfing, both what you are working on and what you are saying, for example during conference and video calls.
- Keep **equipment and information**, including printouts and documents, safe and secure.

Even when working remotely, you must still follow the security policies and operating procedures for systems you access and work with.

Using public wifi or internet, and home broadband

Some locations, such as hotels, coffee shops, or public transport, offer 'public' wifi or internet access.

The public services are usually offered for free. They only need you to agree to some terms of service.

While apparently convenient, these services can have some serious problems:

- They have no security appropriate for protecting information.
- There is no guarantee about keeping information transmitted through them private or confidential.
- Public services are usually shared. This means that performance can often be very slow and unreliable.

If you need network access, but cannot connect to an network or home broadband service:

- Use an hotspot. This is usually provided on your -issued mobile device.

If you need to use a public wifi or internet service, or home broadband, with your equipment, because you do not have an hotspot, then:

- Connect using an -issued VPN. Before doing any work, check that the -issued VPN is working correctly.

Using your own equipment

The main guidance is available here.

- Use official equipment for business purposes.
- Send your work material to your personal devices or your email accounts.

If you are working remotely, or do not have access to equipment, it might be tempting to use your own equipment, especially printers. Avoid doing this.

Printing

The advice is to avoid printing anything when working remotely, and in particular not to use personal printers.

However, if you really must print information:

- Connect directly to the printer using USB, not wifi.
- Consult the information asset owner or line manager before printing the information.

- Store any and all printed materials safely and securely until you return to premises, when they must be disposed of or filed appropriately.
- Print out personal information relating to others.
- Redirect print jobs from an printer to a personal printer.
- Dispose of unshredded information in your home rubbish or recycling. Use a cross-cut shredder to destroy printed materials securely, before disposal at non- locations.

Basically, think before you print.

Privacy

It is important to protect privacy: yours and that of the . Events like the Covid-19 (Coronavirus) pandemic are often exploited by people wanting to get access to sensitive or valuable information. This often results in an increase in attempts to get access to personal information or accounts, using phishing and email scams. Be extra vigilant whenever you get an unexpected communication.

Be aware of your working environment when you work with information. If anyone might access the data, or hear you talk about it as you use it, that could cause privacy problems. Be aware of SMART devices around your remote location, and ensure they are switched off if conducting video or voice communications.

Guidance and suggestions for improving Privacy appear throughout this guide, but it's worthwhile highlighting these points:

- Lock your computer, even when unattended for short periods.
- Think about whether an unauthorised person, such as a family member, might access the information you are working with.
- Write down passwords. Use a password manager.

Contacts for getting help

In practice, all sorts of things can go wrong from time-to-time. Don't be afraid to report incidents and issues; you will be creating a better and safer work environment.

Related information

NCSC Home working: preparing your organisation and staff CPNI Home Working Advice

To access the following link, you'll need to be connected to the HMPPS Intranet.

HMPPS Advice

Teleworking

Personal devices

This guidance applies to all staff and contractors who work for the . It provides advice about using personal devices for work purposes.

Related information

Bluetooth on page 258

Overview

A personal device is any desktop, laptop, tablet, phone, external drive, or similar device that the does not own.

Note: 'Personal devices' include all personally-owned devices with processing ability or Internet connectivity. This includes all types of assistance, organisational or Internet of Things (IoT) devices. Connected vehicles are a special case discussed in this guidance. In case of any doubt, ask for help about specific examples.

Not everyone has access to an device for remote use. If you need equipment, you can request it. It can be provided quickly. Contact your Line Manager for details. A request can then be raised through the .

In unusual circumstances, it might not be possible to organise provision of equipment. In such cases, you request access to an virtual environment.

Except when connecting to an virtual environment, or with documented approval in exceptional circumstances as described in this guidance, you use a personal device for work purposes.

Avoid connecting peripherals to devices, unless those peripherals are supplied or approved by the . Examples of peripheral devices include USB, wireless, or Bluetooth keyboards or mice.

Note: Exemptions are possible for connecting peripherals where accessibility support is required. Contact your Line Manager for documented approval before connecting a peripheral device.

Personal devices be charged from the USB ports of an device.

Note: Specifically: a personal mobile phone be charged from the USB ports of an device.

Guidance

- If you have an -issued device or virtual environment, you use that.
- You use a personal device to access tools such as Gmail, Docs, Slides, Sheets, Drive, Meet, or Hangouts for work purposes.
- You use a personal device to access Office 365 tools such as Outlook email or calendar, Word, Excel, or PowerPoint for work purposes.
    - Wherever possible, an work device be used to join business Teams calls, either via video or dial in.
    - In cases where staff have not been provided with a work phone or laptop or any other work device which allows them to join or dial into Teams, staff join from their personal devices as a Guest. The chair of the meeting confirm the identity of each and every person joining their call as a Guest.
- This guidance applies to all tools accessed through a web browser or installed client applications.
- You send information to your personal email account.
- You use personal accounts for work purposes.
- You store work files or information on a personal device such as a desktop, laptop, tablet or phone.
- You store work files or information on a personal storage device or memory stick, such as an external drive, thumb drive, or USB stick.
- Some teams within the have permission to use personal devices for some tasks. This permission continues, but is being reviewed on an on-going basis. Ensure that you have documented approval recording your permission. Ensure that the permission is no more than 12 months old. To request or refresh permission, ask your Line Manager to seek approval by checking with the .

Note: You are not asked or required to use your own devices for work purposes. Statement **POL.MOB.009** of the mobile device and remote working policy makes clear that you use personal devices for work purposes. If you have access to devices for work purposes, you use them by default. A special case is that if you do not have an -issued mobile phone, you use a personal device to receive Multi-factor authentication (MFA) codes or messages which authorise access by devices to systems.

Using tools on personal devices

In accordance with other policy on the use of personal devices, and the use of mobile devices specifically, you use personal devices to access tools, such as Slack workspaces.

Note: The rest of this section refers to Slack workspaces, but applies equally to other tools, such as Teams, Trello, Jira, and so on.

You could of course use personal devices to access other (non-) Slack communities.

The point is that you use personal devices for work purposes. Slack workspaces are official workspaces and only be accessed using devices.

Personal devices are not allowed to access services or content containing data. Work devices be used to access services such as Slack communities. If you do not have a work mobile device, and need to access services such as Slack on a mobile device, you request one using Service Now.

Virtual environment

The provides access to a Virtual Environment to help with exceptional circumstances. This is where suitable provision of a physical device is not possible.

Request a virtual environment through the `Creation of WVD instances` product offering within the Service Catalogue in Service Now.

Note: A virtual environment does not offer the same capabilities or performance as a physical -issued device. Using an -issued device is always preferable.

Connected vehicles

Connected vehicles are effectively Bluetooth-connected storage devices. They are considered personal devices for the purposes of this guidance, regardless of whether they are owned, leased or rented.

Automatic transfer of contact information and calendar events might happen during the pairing process. The resulting transferred data is accessible to any third party who subsequently pairs their mobile device to the vehicle.

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, devices be paired with Bluetooth-enabled vehicles.

Human resource security

Prior to employment

Minimum User Clearance Requirements Guide

This Minimum User Clearance Requirements Guide outlines the level of security clearance required for staff in order to access specific account types. This is a sub-page to the .

Related information

Access Control guide on page 87

Security clearance levels

The uses the national security vetting clearance levels:

- Baseline Personnel Security Standard (BPSS)
- Counter Terrorist Check (CTC)
- Security Check (SC)
- Developed Vetting (DV)

Where appropriate, Enhanced checks apply, for example Enhanced Security Check (eSC).

Minimum user clearance requirements

Most of the IT systems are able to process information. Therefore all roles in the require staff to attain BPSS clearance as a minimum to be granted access rights to view information. Some roles require staff to have higher clearance.

For an individual to perform any of the following tasks, clearance higher than BPSS is required:

- Has long term, regular, unsupervised access to data centres or communications rooms.
- Has regular privileged unsupervised and unconstrained access to systems which contain data for multiple systems, for example backups, or console access to multiple cloud services.
- Has cryptography responsibilities and handling, under advice from the Crypto Custodian.

- Has access to multiple system security testing outcomes which reveal vulnerabilities in live services.
- Has a role such as system support or IT investigation role, such that without further authority or authorisation, an individual might:
  - Act as another user.
  - Obtain credentials for another user.
  - Directly access other users' data.

If an individual does not need to perform any of the previous tasks, then BPSS, DBS or Enhanced Check is sufficient.

The HQ and Executive Agencies might have additional, specific requirements for DV/DV STRAP clearance for individual systems. These requirements should be followed where applicable.

Please contact the for further information.

During employment

Training and Education

Overview

This information applies to anyone and everyone working for, or with, the .

The 's Information Security awareness programme plays an essential part in maintaining security. It informs all staff of:

- Their duties with regard to security.
- Their responsibilities to protect the assets (information, equipment, people and buildings) they have access to and use.
- The importance of reporting any actual or suspected security incidents.

Requirements

All staff starting or returning to work within the receive mandatory security training.

The objective is to ensure that all new and current staff members are aware of their security responsibilities whilst working at the .

Full details of the mandatory training are provided in the Joiner, Mover, and Leaver pages on the Intranet.

In summary, as a minimum everyone :

- Have taken and completed an Security induction.
- Have completed the Civil Service Learning course on "Responsible for Information (RfI)", or an approved equivalent.

Normally, this training be completed successfully before accessing information, resources, or assets.

Termination and change of employment

End or change of employment

Managers must ensure that all employees, contractors and third-party users return all assets within their possession and that all access rights (including building passes, access to buildings, IT systems, applications and directories) are removed at the point of termination or change of employment.

If the leaver has security clearance, managers should contact the to advise that the person has resigned and tell them their leaving date or the date on which they will be moving to a different department.

Leavers should read the HR guidance at End or change employment.

Managers must also complete a leaver's checklist as a record of actions.

Downloads

Leavers checklist

A downloadable version of the "End or change of employment" document is available here.

Asset management

Responsibility for assets

Acceptable use of Information Technology at work

This guidance applies to all staff and contractors who work for the .

Everyone working at the has access to Information Technology (IT) resources. You must use them in an acceptable way. This guidance explains what that means. The definitive list of Acceptable Use Policy statements is here.

Related information

Email blocking policy on page 271

Summary

Be sensible when using IT resources:

- The resources are for you to do work.
- Protect the resources at all times, to help prevent unacceptable use.
- If the use would cause problems, upset, offence, or embarrassment, it's probably not acceptable.
- Context is important. Security risks can increase when working outside your normal workplace.
- Be aware that your use of resources is monitored. During an investigation into a security incident, IT forensic techniques capture evidence.
- If you're not sure if something is acceptable, ask for help first.
- Above all, if you think there is a problem, report it or ask for help.

The way you use IT is important, because it indicates your approach to work, and can be taken into account when assessing your behaviour and performance.

What is meant by IT?

IT means the devices or services you use for creating, storing, or sharing information. This includes everything from devices (such as laptops, 'phones, mobile Wi-Fi hotspots (MiFi), iPads, tablets, printers, USB "memory sticks") through to online services (citizen-facing online services, staff tools, corporate email).

Acceptable use of IT

Acceptable use of IT is when you use it to do your work.

IT helps you complete your tasks as efficiently and effectively as possible. Sometimes, you might need account details such as passwords to use the IT. Acceptable use means protecting this kind of information, too.

Acceptable use can also vary according to context. For example, checking sensitive personal details might be perfectly normal within a secured office, but is not acceptable in a public space where anyone else might access those details.

Unacceptable use of IT

Unacceptable use of IT prevents you or your colleagues from doing work, or is unlawful or illegal, or does not take the context into account.

There are many unacceptable uses of IT, making it impossible to provide a complete list. Examples of things to avoid include:

- Deliberately or accidentally sharing resources or information, such as passwords, with people who are not supposed to have them.
- Using resources without permission.
- Storing sensitive information where it could easily be lost or stolen.
- Using unapproved tools or processes to store sensitive information, such as passwords or credit card details.
- Using your work email address for personal tasks.
- Using your personal devices or your personal email address for work tasks.
- Excessive private use during working time.
- Installing unlicensed or unauthorised software.
- Redirecting print jobs from printers to a personal printer.
- Sending your work material to your personal devices or your personal email accounts. (It is of course acceptable and necessary from time-to-time to send work material to someone else's email address when they are directly involved with that work, for example someone in the Office of the Public Guardian (OPG) emailing someone regarding Lasting Power of Attorney (LPA).)

Why unacceptable use is a problem

Unacceptable use of IT might affect the in several ways, such as:

- Bad publicity or embarrassment.
- Increased or unexpected costs or delays.
- Civil or legal action.
- Reduced efficiency and effectiveness.

Unacceptable use might also affect you, too:

- Suspension of access, so that you cannot do your work.
- Disciplinary proceedings, up to and including dismissal.
- Termination of contract for contractors and agency staff.

Keeping control

You are responsible for protecting your IT resources. This includes keeping your usernames and passwords safe and secure.

It also means looking after equipment, especially when working away from locations. You are responsible for protecting equipment issued to you. Any theft of equipment, or deliberate or wilful damage to equipment, should normally be reported to the Police and to the .

Note: You should normally report instances of theft or damage to authorities as indicated. However, there might be additional circumstances which mean a sensitive handling of the situation is appropriate. It is acceptable to consider the context of the situation when making a report. Ensure you can justify your actions. In cases of uncertainty, don't hesitate to ask your line manager, or other responsible authority for advice.

While you might be careful about acceptable use of IT, there are still risks from malware, ransomware, or phishing attacks.

If you get an email from anyone or anywhere that you are not sure about, remember:

- Don't open any attachments.
- Don't click on any links in the email.

If there is any doubt, or you are worried that the email might be malicious or inappropriate, report it immediately as an IT security incident.

Personal use of IT

Limited personal use of IT is acceptable as long as it does not cause a problem with your work or that of your colleagues. Context is important. For example, doing personal internet banking during your lunch break might be acceptable, but doing the same thing during a work meeting would not.

Personal use of mobile phones

You might be allocated a mobile phone for use as part of your work. The mobile phone enables you to:

- Make or receive calls.
- Send or receive SMS texts.
- Use Internet services.

This usage must always be for work purposes.

Examples of unacceptable mobile phone use include:

- Making charitable donations from the mobile phone account.
- Signing up for premium rate text services.
- Calling premium rate telephone services.
- Voting in "reality TV" popularity contests - these usually involve premium rate services.
- Downloading, uploading, or streaming media files that are not work-related, such as music or movies.
- "Tethering" another device to the mobile phone, and then using the other device for any of the previously mentioned activities.

... as well as any other activities that are not obviously work-related.

All use of IT resources is monitored and logged. This includes mobile phone usage listed in account bills. It is possible to find out if you used a work-issued mobile phone for unacceptable activities. Unacceptable use is reported to your Line Manager for further appropriate action. Assessing your behaviour and performance takes this kind of activity into account.

Using IT outside your usual workplace

Some IT resources might be usable away from your usual workplace, such as a laptop. Even outside the office, you must continue to ensure acceptable use of the IT resources.

You should also ask before taking IT equipment outside the UK.

Avoid using removable media

Removable media like memory sticks are portable and easy-to-use. Unfortunately, this makes them a security risk, so avoid using them. If however they are essential to your work, follow the Use of Removable Media guidance.

Personalisation of equipment

A popular trend is to adorn laptops with stickers. This is acceptable as long as the material does not cause problems such as upset, offence, or embarrassment. The same applies if you customise the desktop environment of your equipment, for example by changing the desktop image.

Acceptable Use Policy

This document is the Acceptable Use Policy. It provides the core set of security principles and expectations on the acceptable use of IT systems.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.ITAUP.xxx**, where **xxx** is a unique ID number.

Related information

Technical Controls Policy on page 30

Introduction

IT systems and services are first and foremost provided to support the delivery of the 's business services. To achieve this, most users are provided with an appropriate general purpose computer environment, and access to services and communication tools such as email and the Internet.

This policy outlines the acceptable use of IT systems and services, and the expectations that the has on its staff when accessing or using those systems or services.

Scope

This policy covers all Users (including contractors and agency staff) who use IT systems or services.

Failure to adhere to this policy result in:

- Suspension of access to IT systems and services.
- For employees, disciplinary proceedings up to and including dismissal.
- For others with access to IT systems and services, including specifically contractors and agency staff, termination of contract.

POL.ITAUP.001: All Users be made aware of the Acceptable Use Policy (this document), and provided with security awareness training which covers this policy.

POL.ITAUP.002: All Users undergo refresher security awareness training covering this policy, every 12 months.

Protection of assets

It is paramount that all Users protect the confidentiality of information held on, processed, and transmitted by IT systems. All Users have a role in protecting the information assets which are under their control, or that they have access to.

IT systems have been designed to protect the confidentiality of the data held on them. However, maintaining this requires the application of, and adherence to, a clear set of operating procedures by all Users. These are collectively known as Security Operating Procedures (SyOPs).

It is important that all Users of an IT system, including support and system administrative Users, are familiar with these SyOPs, and are provided with the appropriate training.

POL.ITAUP.003: All IT systems have, and maintain, a set of Security Operating Procedures (SyOPs). For systems undergoing an assurance process, these SyOPs be included as part of the assurance.

POL.ITAUP.004: All Users of an IT system, including support and system administrative staff, read the applicable SyOPs, and acknowledge that they have both read and understood the SyOPs before being granted access. A record be kept of a User being granted access, and made available for review during assurance, or upon authorised request.

POL.ITAUP.005: All Users be made aware that non-conformance to the system SyOPs constitutes a breach of the IT Security Policy, and result in disciplinary action.

POL.ITAUP.006: Any change to an IT system's SyOPs be approved through an assured change control process, before the change is made.

POL.ITAUP.007: Any request to perform an action on an IT system which contravenes its SyOPs be approved by the before the action is taken.

For most Users, access to IT systems and information held on them is through a desktop device, a laptop, or a mobile or remote device. These devices have the capacity to store large amounts of potentially sensitive information assets. It is important that Users follow Information Management processes and handling guidelines to ensure information is stored and accessed appropriately. Further information on information handling is provided in the Information Classification and Handling Policy.

General Security Operating Procedures (SyOPs)

The policy refers to a key set of general SyOPs, as follows:

- Privileged User Guide.
- System Users and Application Administrators.

- Remote Working.

To minimise the number of SyOPs in circulation and standardise procedures, the SyOPs listed previously act as the primary set, which individual IT systems are expected to conform to, in terms of their own SyOPs. Any deviations or additions are dependent upon approval through the assurance process.

POL.ITAUP.008: All IT systems have documented SyOPs which comply with the general SyOPs listed in this policy. Any deviations or additions be recorded in separate SyOPs which form an addendum to one of the SyOPs listed.

Note: An IT system make use of, in their entirety, one or more of the SyOPs listed in this policy if the procedures of that IT system do not deviate from those described in the general SyOPs.

Removable Media

Removable storage media include devices such as USB memory sticks, writeable CDs or DVDs, and external drives. These devices contain large amounts of protectively marked data, and so pose a significant risk to the confidentiality of the data they hold. As such, the controls the use of removable media through SyOPs, technical security controls, and by requiring movements of bulk data to be authorised by using a Data Movement Form.

POL.ITAUP.009: Any removable media device be approved by security, where that device is used to store protectively marked data. The type of device and associated SyOPs be approved by security before operational use.

POL.ITAUP.010: All Users ensure that all data stored on or transported by removable media is in accordance with the applicable system SyOPs.

POL.ITAUP.011: All Users seek approval from the prior to any bulk transfer of protectively marked data using removable media. security advises on any technical and procedural requirements, such as data encryption and handling arrangements.

Passwords

A username and password combination is the primary access credential used for authenticating a User to systems, and authorising User access to information assets and services provided by that system. It is therefore important that Users keep their access credentials safe and secure.

POL.ITAUP.012: All Users share or disclose any passwords with any other person.

POL.ITAUP.013: All Users :

- Attempt to gain unauthorised access to another User's IT account.
- Attempt to use another Users access credentials to gain access to an system.
- Attempt to access information for which they do not have a 'need-to-know'.
- Use the same password on more than one system.

Legal and regulatory requirements

There are a number of legal and regulatory requirements that the must comply with. These obligations are in addition to HMG security policy, as expressed in the HMG Security Policy Framework.

POL.ITAUP.014: All Users be made aware of legal and regulatory requirements that they adhere to when accessing systems. These requirements be included as part of the SyOPs.

Corporate Image

Communications sent from systems, or products developed using them, such as branded documents or presentations, damage the public image of the if they are for purposes not in the interest of the , or they are abusive, offensive, defamatory, obscene, or indecent, or of such a nature as to bring the or any its employees into disrepute.

POL.ITAUP.015: All Users ensure that systems are not used in an abusive, offensive, defamatory, obscene, or indecent way, or are of such a nature as to bring the or any its employees into disrepute.

Potential to cause offence and harm

The has a duty of care to all staff, and to provide a positive working environment. Part of this duty involves ensuring all staff maintain a high standard of behaviour and conduct.

POL.ITAUP.016: systems be used for any activity that causes offence to employees, customers, suppliers, partners, or visitors, or used in a way that violates the Code of Conduct.

Personal use

The permits limited personal use of its IT systems, provided this use does not conflict or interfere with normal business activities. The monitors the use of its IT systems. Any personal use is subject to monitoring and auditing, and also be retained in backup format, even after deletion from live systems.

The reserves the right to restrict personal use of its IT systems. The main methods employed are:

- Filtering of Internet and email traffic. All Internet and email traffic is filtered and analysed. Further details are available.
- Policy and procedures. This policy and associated SyOPs set out the restrictions placed on the use of systems.

POL.ITAUP.017: Users ensure that any personal use of systems does not conflict or interfere with normal business activities. Any conflict be reported to the User's line manager.

POL.ITAUP.018: Users ensure that any personal use of systems is consistent with any applicable SyOPs, and with this acceptable use policy.

POL.ITAUP.019: Users be aware that any personal use of systems which contravenes any applicable SyOPs, or this acceptable use policy, constitutes a breach of the IT Security Policy and result in disciplinary action.

Maintaining system and data integrity

Users comply with all applicable operating procedures, and ensure that they do not circumvent any security controls in place. Changes to the configuration of an IT system which affect either the integrity of that system or the integrity of shared data be undertaken or supervised by an authorised User or system Administrator.

POL.ITAUP.020: All Users request any changes to systems or equipment through the . Further details are provided in the System Users and Application Administrators guidance.

Electronic messaging and use of the Internet

Due to the risks associated with electronic communications such as email and the Internet, the controls and monitors usage of systems in accordance with applicable legal and regulatory requirements.

IT systems are designed to protect the from Internet-borne attacks, to reduce the risk of information being leaked or compromised, and to support the in providing a safe working environment. This is mainly achieved through the filtering and monitoring of all Internet and email traffic.

Also, the use of any high bandwidth services, such as video streaming websites, create network capacity issues, causing poor performance affecting important services. Therefore, the restricts access to the Internet, based on job role. Amendments can be made on the submissions of a business case for approval by the .

The regards as a disciplinary offence any usage of electric communications, such as email and other methods including instant messaging and the Internet, which breaks the law, contravenes HR policies, or involves unauthorised access to or handling of material that is deemed to be inappropriate, abusive, offensive, defamatory, obscene, or indecent.

External email and the Internet are, in general, insecure services where it is possible for external entities to intercept, monitor, change, 'spoof', or otherwise interfere with legitimate content. The deploys a number of security controls to protect its Users from Internet- and email-borne attacks. However, these controls are reliant on Users remaining vigilant, following any applicable SyOPs, and reporting any suspicious behaviour.

POL.ITAUP.021: All Users use the Internet, email, and other electronic communication systems only in accordance with this acceptable use policy document.

Managing email use

Users are responsible for ensuring that all information is handled in line with the protective marking of that information, in accordance with the Information Classification and Handling Policy.

The is connected to the Government network, which provides a secure environment for sending or receiving emails between Government departments. This allows Users with an email account (normally with the suffix '`@justice.gov.uk`') to send emails with handling caveats such as to another or government User, where their email suffix ends in '`gov.uk`'.

POL.ITAUP.022: All Users ensure that information contained within or attached to an email is handled in accordance with the Information Classification and Handling Policy.

Email is a major source of malware, and a route into the for criminal organisations. It be used to defraud staff, or to exfiltrate information. All Users exercise care when handling emails, and report any suspicious activity as an IT security incident.

POL.ITAUP.023: All Users ensure that they do not:

- Open any attachments to an email where the source is untrusted, unknown, or unsolicited.
- Click on any links within an email, where the source is untrusted, unknown, or unsolicited.

POL.ITAUP.024: Where a User suspects that an email received is from an untrusted, unknown, or unsolicited source, they report it as an IT security incident.

Connectivity and remote access

Remote access is provided to systems and services, allowing Users access from offsite and home locations to connect in. The main methods of access are either via a laptop or other mobile device. Normally, remote access is to a protected IT system. Users be aware of the security controls and procedures of the devices and systems being used, as well as any applicable general physical security considerations. This includes any restriction on the carriage of such devices, as they contain HMG protectively marked data, or HMG cryptographic material.

security maintains a list of countries where carriage and use of remote access devices is permitted.

Further details can be found in the Remote Working guidance.

POL.ITAUP.025: All Users be aware of the Remote Working guidance, and confirm that they have read and understood it before being provided with any remote access devices or equipment, such as an encryption or access control token.

POL.ITAUP.026: Any User wishing to take a remote access device out of the UK consult the Remote Working guidance before doing so, and the applicable device IT Security Operating Procedures document.

Monitoring of communications

Communications be monitored without notice, and on a continual basis, for a number of reasons. These include compliance with legal obligations, effective maintenance of IT systems, preventing or detecting unauthorised use or criminal activities such as cyber-intrusion, monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

The monitors telephone usage, network, email, and Internet traffic data, including sender, receiver, subject, attachments to an email, numbers called, duration of calls, the domain names of websites visited, the duration of visits, and files uploaded or downloaded from the Internet, at a network level.

The , so far as possible and appropriate, respects User privacy and autonomy whilst they are working, but in accordance with the personal use information, any personal use of systems is also subject to monitoring. By carrying out personal activities using systems, Users are consenting to the processing any sensitive personal data which be revealed by such monitoring, such as regular visits to a set of websites.

For the purposes of business continuity, it be necessary for the to access business communications, including within email mailboxes, while a User is absent from work, including for a holiday and because of illness. Access is only granted through submission of a formal request to the , where approval is required from the relevant line manager. The and HR are normally consulted as well, before access is granted.

POL.ITAUP.027: All Users be aware that their electronic communications are being monitored in accordance with this acceptable use policy.

POL.ITAUP.028: All Users be aware that business communication such as email mailboxes be accessed if they are absent from work. This access is normally requested through, and authorised by, the User's line manager. The and HR are normally consulted as well, before access is granted.

Data protection considerations

Acceptable use considerations apply to the storage of personal data. This storage includes data hosting in 'cloud' environments, or within services or databases hosted or administered outside:

- The UK.
- The European Economic Area (EEA).
- Countries with an Adequacy Decision (an 'Adequacy Decision Country' or ADC).

POL.ITAUP.029: The default position is that personal data be transferred to or through, or stored, in the US or elsewhere outside the UK, EEA, or an ADC, other than in exceptional circumstances.

This position also applies where a supplier uses cloud storage facilities in the UK, EEA, or an ADC, but their employees outside the UK, EEA, or the ADC are able to view the information for activities such as maintenance or trouble-shooting. The effect of this access is equivalent to the personal data being held outside the UK, EEA, or an ADC.

The reason for this position is that even with additional contractual clauses, the cannot ensure protection of its personal data stored outside the UK, EEA, or an ADC, due to some government surveillance laws.

POL.ITAUP.030: A supplier based in the UK, EEA, or an ADC, and which stores client data in the UK, EEA, or an ADC, be considered first and preferred where possible.

POL.ITAUP.031: If an alternative supplier cannot be sourced, then a Standard Contractual Clause (SCC) and a Transfer Impact Assessment (TIA) be completed.

These documents are reviewed by the , after which the transfer be approved. A template for these documents can be requested from

POL.ITAUP.032: If the outcome of the assessment does not support the transfer and storage of information outside the UK, EEA, or an ADC, the Information Security and Risk (ISR) Board review the case, and if appropriate, accept the risks in order for the supplier to be used.

POL.ITAUP.033: This acceptable use policy for personal data apply to:

- An existing supplier changing the location of its servers, storage, or services outside the UK, EEA, or an ADC.
- New suppliers.

Data protection acceptable use protocols and standard operating procedures

The has produced a number of Acceptable Use protocol documents, providing specific data protection guidance.

The documents are available on the Intranet, or by contacting the .

The documents are as follows:

- Acceptable Use Protocol Commercial and Contract Management
- Acceptable Use Protocol Subject Access Requests
- Acceptable Use Protocol Storage of Personal Data
- Acceptable Use Protocol Data Subjects' Rights
- Acceptable Use Protocol Processing of People Data
- Acceptable Use Protocol Analytical Platform
- Acceptable Use Protocol Recording

There are also a number of Standard Operating Procedures (SOP)s, including:

- Personal Data Risk Management

- Data protection impact assessment guidance
- Data sharing agreement assessment

For more information on these protocols and procedures, contact the .

Guidance on IT Accounts and Assets for Long Term Leave

Audience and Document Purpose

This document is intended for line managers who have a staff member going on any type of long-term secondment, loan, or leave. It provides guidance on how to handle the IT accounts and IT assets (such as desktops, laptops, or mobile phones) of the staff member while they are on leave.

Long term means longer than 2 months.

Types of secondment, loan, or leave where this might apply include:

- Adoption Leave.
- Career Break.
- Loan.
- Maternity Leave.
- Secondment.
- Shared Parental Leave.

For the purpose of this guidance, all of these are examples of "long-term leave".

Guidance Statement
Retaining assets, and access during leave

This guidance applies to assets, defined as being laptops, desktops, or mobile phones.

- A staff member going on any long-term leave may keep their assets while they remain contractually employed by the , **AND** where the leave is not longer than 12 months in duration.
- Remind your staff member that the Acceptable Usage Policy applies at all times during their leave. The policy can be found here.
- Preparation or return from any type of leave may be accompanied by changes in working patterns. The Remote Working guidance provides useful advice for anyone who may be working remotely for the first time. The policy can be found here.

Note: Devices that are not used for 3 months or more go in to a technical "quarantine", intentionally to render them unusable. Staff members should log in to their devices once per month during leave, to ensure that technical quarantine is not activated. Logging in also helps ensure that system updates are downloaded and applied.

Reviewing access to data and information systems

Before the staff member goes on leave, review their access to data and information systems, to ensure that this meets an ongoing need. This means that:

- If the staff member's role is planned to change on their return to the , consider removing access now to data and information systems which they will no longer need. If their role is not planned to change on their return, you might consider leaving access "as-is" currently.
- Consider removing access to data or information systems which are . This is in line with the necessity rigorously to apply the "need to know" principle for information. Refer to the guidance on classifying information for more detail https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/

When to remove access and return assets

In a number of circumstances assets should be returned and access should be removed. This is where:

- The leave is longer in duration, and there is no business need or individual need for the user to keep assets and access. This should be considered for any leave more than 12 months in duration. This is likely to be for Career Breaks or Loans.

- The staff member has no means of securely storing the asset, for example locking it securely in their home.
- Staff members going on leave for less than 12 months may return their assets and have access removed if they choose to do so.
- Line managers are empowered to determine whether the staff member should keep assets and access, as long as there is appropriate business justification, and staff members are appropriately supported. For example, a communication mechanism for keeping in touch is agreed.
- If, during their leave, the staff member decides to end their employment (resign), their line manager is responsible for following the appropriate leaver's process with them. Refer to the Resignation section of the HR guidance and forms, with particular reference to the Leavers Checklist for Managers. This can be found at: https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/resignation/

How to remove access and return assets

- Access to systems and return of assets can be organised through the appropriate items in the Technology Portal. Please refer to the Knowledge Base article on "Returning your laptop, accessories and mobile phones" for details. Removal of access to local systems should be arranged with local IT teams.

Note: When a Dom1 account is deactivated, its data is recoverable for up to 12 months. Refer to the Knowledge Base article on "How to Re-instate a Deactivated Email Account or Mailbox".

Protect yourself online

There are five simple things we can all do to protect ourselves online:

1. Use a strong password to protect your laptop, computer and mobile devices. To choose a good password, follow NCSC guidance.
2. Think before clicking on links or attachments within emails. By hovering your cursor over the link you can find the actual URL. If you are unsure if an email is genuine, contact your IT or security team.
3. Do not use your work email address to register for accounts on websites for personal use. For example, a shopping website does not need your work email address. Using the wrong address could open up your work email account to spam and fraudulent emails. This in turn could harm your department's IT system.
4. Protect your online identity. Do not share sensitive information about your work on social media or online professional networks.
5. Do not disclose your level of vetting. If you share this information, you advertise what resources you have access to. This could make you a target for malicious individuals.

For more information, refer to the Acceptable Use guidance.

Information classification

Data Handling and Information Sharing Guide

This guide is designed to help protect information held on IT systems, by providing guidance on how it should be handled and shared in a safe and secure manner.

Related information

Email blocking policy on page 271

Overview
Introduction

The identifies mandatory requirements about the value and classification of information assets. To comply with these requirements, the needs to ensure that:

> Where information is shared for business purposes, departments and agencies ensure the receiving party understands the obligations and protects the assets appropriately.

and

All staff handling sensitive government assets are briefed about how legislation (particularly regarding Freedom of Information and Data Protection) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies. Appropriate management structures be in place to ensure the proper handling, control and (if appropriate) managed disclosure of sensitive assets.

The policy on data handling and information sharing is covered in the Information Classification and Handling Policy, whilst this document sets out the guidance sharing information within the and externally with other Government departments and 3rd parties.

Note: Other guidance might refer to information classified as being `IL3 REST*`. This is an older classification standard. In general, `IL3 REST*` is approximately equivalent to with the handling caveat, often written as. While this approximate alignment might be helpful, you should always review classification where older terms are used, to ensure that the correct current classification is used.

Scope

This document provides guidance on handling or sharing information stored on IT systems, or exchanged electronically within the , or with external parties.

The can help you with more guidance on the handling of protectively marked data.

This guide is split into three sections:

- Handling data on IT systems.
- Information sharing.
- Reporting data loss.

Note: This document provides guidance for handling and sharing of information and data up to and including and , or the older Impact Level (IL) 3. Where information attracts a high protective marking or IL, advice be sought from the and the .

Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. Safeguarding data is captured as a basic requirement in Level 1 and the will need to demonstrate compliance against this requirement.

Handling data on IT systems

This section covers how data be handled on IT systems, this includes both:

- Data in transit.
- Data at rest.

For the purposes of this guide, the term "sensitive" data or information refers to data or information which attracts a handling caveat of . Refer to the Information Classification and Handling Policy for further details.

Ownership of information

All information is assigned an individual who has overall responsibility for the various handling aspects including:

- Registration.
- Labelling.
- Storage.
- Any transfers.
- Setting a retention period.
- Deleting, destroying or returning data and media.
- Ensuring that any applicable legal, regulatory or contractual obligations are adhered to.

This individual is the Information Asset Owner (IAO). The IAO ensure that information for which they are responsible for is appropriately handled, and where there is a business requirement to share it with a 3rd party, that it is shared in a safe and secure manner.

Electronic data transfer and storage

Data be stored only on managed accredited networks, with transfers onto remote access laptops or other mobile devices or media minimised. No sensitive data should be stored solely on non-networked devices or media unless specifically approved by the IAO.

Data in transit

The term "data in transit" covers all electronic moves or transfers of data from one IT system to another, where either the sender or the recipient system is an IT system. This includes the electronic movement of data using either a system-to-system connection such as CJSE, or removable media such as a USB mass storage device.

Secure network (system-to-system electronic transfer)

The preference for transferring data is to use a secure accredited government network whether that is a owner network (e.g. DISC, ONMI, Quantum or MINT) or the Government Secure Intranet (GSi).

As these networks can support data up to and including , a base level of assurance is provided. However, consideration will need to be given to the following factors to ascertain if any additional security controls are required:

- The amount of data being transferred.
- Frequency.
- Any "need-to-know" considerations. Refer to the Access Control Guide for further information.

Any additional controls be captured on the DMF (refer to the Data Movement Form). Advice should be obtained from the when required.

USB mass storage device

If using a secure network is not feasible, the next preferred option is to use an encrypted removable media, such as an approved USB mass storage device.

For more information, refer to the Removable Media guidance.

The type of device selected is normally dependant on the sensitivity of the data and the amount of data being transferred. Advice be sought from the on the best option to use when completing the DMF (refer to the Data Movement Form).

Optical media

The use of optical media (i.e. CD/DVD) is not recommended for data transfer.

Data at rest on -issued laptops

"Data at rest" is a term used to refer to all data in computer storage. This excludes data that is traversing a network, or temporarily residing in computer memory to be read or updated. The protection of data at rest is achieved by encrypting the hard disk. -issued laptops use an approved whole disk encryption product. This allows data to be safely stored.

Disposal and decommissioning

Sensitive data be kept for longer than is needed. The IAO check for compliance, including any mandatory retention period.

Physical media containing sensitive data be disposed of securely, even if that data is encrypted. The reason is that an attacker could potentially make unlimited attempts to crack the encryption used if the media comes into their possession.

Further information on disposal and decommissioning can be found in the Secure Disposal of IT Equipment guidance.

Information sharing
General principles

Where there is a business need to transfer sensitive data, it be appropriately secured or encrypted using an approved mechanism prior to electronic transmission or export to removable media devices.

Transferring sensitive data with the appropriate security controls may be achieved by:

- Transmission over a secure network that is accredited to carry such data, either in clear (where this has been formally approved by Information Assurance and the IAO), or encrypted.
- Transmission over an unprotected network, employing encryption of sufficient strength to mitigate any communication security risks identified.
- Physical transportation of storage media using encryption of sufficient strength to mitigate the security risks associated with the information being transferred in addition to the physical and procedural measures required to protect the media itself.

Note: Only the minimum amount of sensitive data necessary to meet the business requirement should be transferred and not the entire data set.

The sender ensure that any data shared can be adequately secured by the recipient. The sensitivity of data never be downgraded in order to send it over inadequately protected channels, or to send it to a recipient who does not have an appropriate facility to protect it after it arrives.

Sharing sensitive information

staff, including contractors and agency staff, make sure they observe the following measures when sharing sensitive information:

- Check that all recipients are authorised and cleared to receive sensitive information before sending it to them.
- Ensure that the confidentiality of the sensitive information is protected during transit, for example by encrypting the data.
- Ensure copies of sensitive information are not kept beyond when they are actually required, for example by keeping information "just in case" it might be needed in the future.

All staff avoid exposing sensitive data to unnecessary risks, in particular by observing all aspects of Acceptable Use Policy .

Authorisation be sought from the IAO before sensitive information can be moved or shared with a 3rd party. The authorisation itself is captured within the Data Movement Form. the following sub-sections provide guidance on particular types of information sharing common across the , and to help you complete a DMF.

Internally within the

Information marked up to and including can be transferred in bulk within an IT system or domain such as DOM1, without additional controls required to preserve the confidentiality of that information.

Where information is transferred between IT systems or domains, additional controls might be required to:

- Ensure the information is routed correctly to preserve its confidentiality.
- Maintain the integrity of the data in transit to guard against inadvertent, accidental or deliberate modification.
- Ensure the exchange cannot be repudiated by either party, for example, be enabling proof of sending or proof of receipt.

Information transferred between two IT systems requires a completed and authorised Data Movement Form using one of the data in transit options.

Information sharing with another HMG department

Information shared with another government department be transferred to an assured system. This means the system be assured to the same level as the data being transferred. The transfer take place using one of the data in transit options. The preference is for information to be transferred using a secure network. However, for low frequency bulk transfers of data, approved removable media might be more suitable. A completed and authorised Data Movement Form is required.

Information sharing with external 3rd parties

Any transfer of sensitive data to a 3rd party, including sub-contractors or service providers, be authorised by the relevant IAO. An appropriate contract, Data Movement Form, and Non-disclosure Agreement (NDA) be in place prior to the transfer.

It might also be appropriate to establish a Security Aspects Letter (SAL) and Codes of Connection (CoCo) agreement.

Where the information is , it be transferred to an assured system, assured to the same level as the data being transferred, provided by the external 3rd party, using one of the data in transit options.

Any transfer to a 3rd party be undertaken with appropriate security controls in place, using the guidance from this document, and seeking advice from the as required.

Sharing across an unsecured network

Sensitive data be encrypted prior to being transmitted over an unsecured network such as the Internet. The encrypted data may then be sent via file transfer or as an email attachment.

Ideally, both sender and recipient should check the integrity of data before and after transmission. This includes checking for malicious content, and for evidence of tampering during transit.

Using commercial encryption products for low sensitivity information

Where there is a business requirement to do so, sensitive information may be shared with a 3rd party using a commercial grade encryption product such as SecureZip. Further information on the use of SecureZip can be found in Using SecureZIP.

Note: File encryption does not protect the name of the file. This could reveal clues as to the nature and importance of the encrypted data. Encrypted files should be given innocuous names for transmission. If the data is contained in numerous small files, these should be collected together into a single archive ("zip") file. This archive should then be encrypted. Each file or archive should be sent separately, rather than attaching multiple encrypted files to a single email.

Sharing information higher than

Where there is a business requirement to share information classified higher than , advice be sought from the prior to completing a Data Movement Form.

Data Movement Form (DMF)

The Data Movement Form (DMF) is available here.

The purpose of the DMF is to ensure that the movement of information assets is secure, and in compliance with the .

Failure to fulfil or comply with the controls and measures identified within the DMF will lead to unnecessary risk or exposure for the , or the relevant Information Asset Owner (IAO), or the Senior Information Risk Owner (SIRO).

A DMF be completed, and approval received from the , for the following scenarios:

- Data is being moved or shared by using a physical storage device to transfer the information. An example is where you use a "memory stick", a USB drive, a storage array, or some other removable media. The DMF in this scenario focuses on the data being moved or shared.
- Data is being moved or shared by electronic (network) communication, where the movement is from an IT system to an external party. An example is using secure file transfer or approved email to transfer the information. The DMF in this scenario focuses on the data being moved or shared.
- An asset (a "data bearing asset") is being moved to, or transported by, an external party. This might be as a result of an office move, or because the asset is being decommissioned. The asset might contain or process information. Examples of data bearing assets include laptops, servers, multi-functional devices, and any other data bearing peripherals. The DMF in this scenario focuses on the asset being moved or transported, rather than the information that the asset might contain or process.

A DMF be submitted to the for information purposes, in the following scenarios:

- Data is being moved or shared by electronic (network) communication, where the movement is entirely within or between IT systems.
- Data is being moved in full compliance with the already-approved service design and operation specification and procedures.
- An asset (a "data bearing asset") is being moved but remains within the or its supplier-provided and -approved facilities at all times.

Note: In the informational scenarios, a DMF is only expected the first time a data movement or sharing takes place. Subsequent, repeat instances of the movement or sharing, do not require a re-submission of the DMF. For example, when setting up a backup process as part of an approved service design, a DMF is created and submitted to the for information purposes, but does not need to be re-created or re-submitted for each backup occurrence. If the implementation or process for the data movement or sharing changes, for example a new new backup technology or process is deployed, then a fresh informational DMF is required.

In any case of doubt, it is always advisable to complete a DMF and await approval or other feedback from the .

Using SecureZIP

SecureZip is a compression and encryption product which can be used to encrypt sensitive data for use in removable media and email based information transfers.

Note: SecureZip can produce "self-extracting" encrypted files that are executable programs which are likely to be blocked by network firewalls or email content checkers.

The general rules for transmitting a password to a recipient are:

- Never transfer the password with the encrypted file, or even over the same communication channel. Use an alternative method, for example if an encrypted file is sent by email, communicate the password or key via SMS text message, letter, fax or phone call.
- Transfer the encrypted data file first. Only send the password or key after the recipient has confirmed receipt of the file.
- Avoid detailing the purpose of a password when it is sent.
- Avoid re-using passwords and demonstrate good security discipline to 3rd parties by creating a completely new password or phrase for each transmission.

More guidance on password best practices is available.

Government Classification Scheme

The Government Security Classification (GSC) system has three levels: , , and .

The GSC was issued by the Cabinet Office in 2018: https://www.gov.uk/government/publications/government-security-classifications

This is the majority of information that is created or processed by the public sector.

> Includes routine business operations and services, some of which could have damaging consequences if lost, stolen, or published in the media, but which are not subject to a heightened threat profile.

This classification applies to the vast majority of government information including general administration, public safety, criminal justice, and law enforcement, and reflects the fact that reasonable measures need to be taken to look after it and to comply with relevant legislation such as the Data Protection Act, Freedom of Information Act, and Public Records Acts.

A limited amount of information is particularly sensitive, but still comes within if it is not subject to the threat sources for which is designed, even if its loss or compromise could have severely damaging consequences. The need to know principle be rigorously enforced for this information, particularly where it might be shared outside of a routine or well understood business process. There are very few activities where all related information or cases require the marking, though this might apply to assets previously marked as `CONFIDENTIAL`. Across a range of information assets which were previously normally marked as `PROTECT` or `RESTRICTED`, there might be individual cases/instances which are more sensitive (some of which might be marked `CONFIDENTIAL` on an individual basis). This more sensitive information is identified by adding ", and must therefore be marked ". This marking alerts users to the enhanced level of risk and that additional controls are required.

Very sensitive information that justifies heightened protective measures to defend against determined or highly capability threats.

> Where compromise might seriously damage military capabilities, international relations or the investigation of serious organised crime.

Use of only be used where there is a high impact and a sophisticated or determined threat (elements of serious and organised crime, and some state actors):

- Classified material received from Other Government Departments (OGDs) or agencies relating to national security and counter-terrorism.
- Intelligence and investigations relating to individuals of interests to security agencies.
- Information that might seriously damage security and intelligence operations.
- Information affecting the ability to investigate or prosecute serious or organised crime.
- Personal/case details where there is a specific threat to the life or liberty of an individual such as protected witness scheme records.

The concept of sophisticated or heightened threat doesn't only apply to those with a high technical (IT) attack capability, but might apply to criminals who have a developed capability to intimidate or coerce individuals. If disclosure of information might result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information be tightly controlled. become the default status for material just because of the type of case or potentially severe consequences such as murder trials, or where there is a threat to life. The threat capability also be present.

HMG's most sensitive information, requiring the highest levels of protection from the most serious threats.

> Where compromise might cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level. Any business area holding or expecting to hold information at this level contact the Departmental Security Officer to agree controls.

Applying the classification system

The following considerations apply:

- Staff and delivery partners are responsible for ensuring that all information is looked after with care, to enable the business to function as well as meeting privacy needs.
- The majority of and wider government information will fall into the tier; there is a significant step up to and which are essential for national security and the very highest threat areas.
- provides for a general and sufficient level of control of information (including for systems holding such information) which is not subject to heightened threat sources. Within this, there is flexibility to apply additional operational controls to reflect sensitivity.
- In most areas of activity at , staff should continue to follow existing business instructions and procedures for handling information that apply to those activities. Such instructions should include provisions for identifying and dealing with more sensitive cases.
- The 'Working with Official information' desk aid and handling rules should be referred to when receiving, handling or creating information in any format, which is not routine or covered by general processes or instructions.
- Material at does not require a marking to be applied, but must be protected in accordance with the handling rules and any local instructions. However, information assessed to be particularly sensitive must be marked , giving a clear warning that strict control of access and special handling apply (see below).
- Staff are expected to comply with local instructions and minimum controls, but need to exercise common sense in situations where applying a control is not possible or would seriously hinder effective business or safety. In all but

the most urgent cases, seek approval from your manager or the Information Asset Owner before adopting lesser controls. Decisions must be risk based, and the assessment must be recorded at the earliest convenient opportunity.

- Existing material with former protective markings including UNCLASSIFIED, PROTECT, and RESTRICTED does not need to be retrospectively reclassified. See the transition note in this guidance.
- Descriptors, such as PERSONAL or COMMERCIAL are no longer used. In exceptional circumstances or where the recipient might not recognise the sensitivity of the information being sent, authors may include 'handling instructions' in a document or email to draw attention to particular requirements.
- The security officer for your part of the should be consulted to agree controls if you receive,handle or otherwise process any information at or .

Controls

At , any local instructions or operating procedures should continue to be followed. These should assist staff in identifying any cases that require the marking.

This guidance note and the desk aid entitled "Working with Official information" provide some general rules. You might also need to refer to local intranet pages or the handling rules if creating or processing any non-routine material.

Controls should be consistent with the minimum controls set out in the Handling Rules. These must be applied to all information within and are adequate for most information, providing defence against the sort of threats faced by a major company. These threats include, but are not limited to, 'hacktivists', single issue pressure groups, investigative journalists, competent individual hackers, potentially aggrieved participants or users of the justice system, and the majority of criminal individuals and groups.

Business areas or Information Asset Owners (IAOs) should review risks to their information, and ensure local procedures are in place, adopting additional controls where needed.

The Handling Rules document identifies additional considerations for some aspects of control. Business areas or IAOs might decide to adopt more robust controls in these areas, particularly for material marked or where information is moved, transmitted or otherwise communicated outside of the secure office environment.

Controls should be applied proportionately for information which would previously have been 'unclassified'. Such information still needs looking after if it is required for the job, but might not require controls designed to provide confidentiality.

If IAOs or staff are considering classifying any new assets or reclassifying any existing assets as or , they should consult their IA lead and security adviser, or with security in relation to technical threats, to determine whether a heightened threat might be present, and to agree necessary controls.

Marking of information

Marking is only needed for information which is , or . Classifications can be added to information in many different ways but the most important thing is that the marking is clearly visible to anyone using or receiving the information.

This could mean:

- Marking the top and bottom of documents, clearly, in CAPITALS, and CENTRED in the header and footer.
- Showing the marking in the subject line of emails:
  - Type at the start of the subject line, in CAPITALS.
  - Remember to consider whether material that is sensitive needs to be sent, and whether it is safe or appropriate to send if the recipient is outside a secure government network.
  - You must not email anything at or above.
- Marking the front of folders or binders:
  - Apply clearly in a prominent position in CAPITALS.
  - Apply the highest classification of any of the contents.

Material that needs marking must be transmitted securely. The classification of contents must not be visible on an external envelope sent by post or courier.

Transition to the classification system

For information bearing the 'old' markings, the following guidance should be followed to ensure appropriate handling. Unless there are specific instructions to the contrary, staff are expected to maintain current levels of control and use existing IT systems on which information is currently held or processed.

The old protective markings do not automatically read across, particularly at CONFIDENTIAL.

- All material up to and including RESTRICTED becomes .
- Much material at CONFIDENTIAL becomes , but some might become .
- Only a limited amount of material at RESTRICTED needs marking as .
- CONFIDENTIAL material moving into is likely to require marking as .

Old marking	New classification	Examples
UNCLASSIFIED or not protectively marked.	Treat as (unmarked). Where controls prevent otherwise safe sharing of non-sensitive information, IAOs have some discretion to relax controls, provided any relaxations are specific to their assets and have no wider risk consequences, such as for the security of IT assets and government network code of connection.	Public notices and leaflets, published information, information that doesn't contain personal data or other sensitive content, and training materials.
PROTECT.	If information relates to general administration, treat as (unmarked). Where used for personal data, maintain existing controls. Individual case records containing particularly sensitive content need to be marked , though these instances may already be marked RESTRICTED or CONFIDENTIAL.	Documents containing personal data such as personnel records, citizen or offender case records, and general administration not intended for publication.
RESTRICTED.	If it relates to general administration, there should be a presumption that it can be treated as (unmarked).	General administration, policy documents, commercial documents, or case records.
	You need to consider whether the subject matter is particularly sensitive and there is a need to rigorously enforce access controls, in which case material may additionally require handling or marking as . Anything with this level of sensitivity might already have agreed handling constraints. If in doubt, discuss with the Information Asset Owner.	Particularly sensitive case records, contentious policy drafts and advice, and sensitive negotiations.
CONFIDENTIAL hard copy previously received from another Department.	Check with the author or originating Department. The presumption should be to treat as and continue with current handling controls, unless there is a clear national security aspect or it relates to protected witnesses, in which case treat as . If you want to reproduce content in an electronic document, check the classification with the author or originating Department. See the note after the table.	
CONFIDENTIAL electronic copy received by secure government network or held on stand-alone system used for CONFIDENTIAL.	Continue to observe the operating instructions for the system you are using. Continue to use the secure government network for any reply, and use the marking applied by the original author. Otherwise, adopt controls for . See the note after the table.	

Old marking	New classification	Examples
.	Continue to treat as , subject to any formal review of the classification of the information assets involved in the particular area of activity. If hard copy, treat as and log, store, move and dispose of accordingly. If held on a stand-alone system currently rated at , treat as and observe the operating controls for the system.	Material relating to national security or counter-terrorism, and some protected witnesses.

Note: Electronic records marked `CONFIDENTIAL` should not be processed or saved on the existing standard networks such as DOM1 or Quantum, or on electronic document management systems unless or until the originator or Information Asset Owner has issued revised guidance allowing the information to be handled at , including , and the system has been rated to hold material at , with any additional access controls, or the system reclassified as .

Information classification, handling and security guide

All employees interact with information, and are responsible for its protection. Information security must be considered during the process of designing, maintaining, and securing the 's IT systems that are used to process information.

However, not all information warrants the strictest levels of protection. This is why information classification is so important to the – to ensure that the department can focus its security efforts on its most sensitive information. Information security must be proportionate to the security classification of the information, and must be considered throughout the information lifecycle to maintain its confidentiality, integrity, and availability.

Classifying information

The three information security classifications the uses are , , and . This follows the .

Each information security classification has a minimum set of security measures associated with it that need to be applied. These security measures might change, depending on the information lifecycle stage.

Classification	Description
	All information related to routine business, operations, and services. If this information is lost, stolen, or published, it could have damaging consequences, but is not subject to a heightened threat profile. For regular, unsupervised access to information, someone would be expected to have achieved Baseline Personnel Security Standard (BPSS) assessment. Very sensitive information that requires protection against highly sophisticated, well-resourced, and determined threat actors. For example, where compromise could seriously damage military capabilities, international relations, or the investigation of a serious crime. For regular, unsupervised access to information, someone would be expected to have passed National Security Vetting Security Check (SC) clearance. In exceptional circumstances, someone with BPSS might be granted occasional supervised access to UK assets, or be required to work in areas where or information might be overheard. Exceptionally sensitive information that directly supports, or threatens, the national security of the UK or its allies, and requires extremely high assurance of protection from all threats.

Securing the 's information must be done with a combination of information security measures:

Type of Measure	Description
PERSONNEL	Personnel should be aware of their security responsibilities and in turn acquire security clearances and undertake training to support the 's information security objectives.
PHYSICAL	Tangible measures that prevent unauthorised access to physical areas, systems, or assets.
TECHNICAL	Hardware or software mechanisms that protect information and IT assets.

It is important to understand that security classification is determined by the level of risk in case of loss or unauthorised access, and not by the type of information.

It is the responsibility of the Data Owner to classify the data.

- Most production data is information. Within this, some production data might be classified as information.
- Most personal data is information. Within this, some personal data might be classified as information if it meets the risk threshold defined.

The following table sets out the definitions for each security classification, as well as whether it is necessary to explicitly "mark" a piece of information with its classification type.

Classification	Definition	Marking
	All information related to routine public sector business, operations and services. Almost all personal information falls within the classification.	
	is not a separate security classification. It should be used to reinforce the "need to know" principle, beyond the baseline for .	data does not need to be marked except where , and must be marked .
	Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime.	Must be marked
	Exceptionally sensitive information that directly supports (or threatens) the national security of the UK or its allies and requires extremely high assurance of protection from all threats.	Must be marked

Additional information on how to manage information is described in the Information Asset Management Policy.

Information security classification may change throughout the information lifecycle. It is important to apply appropriate security classifications and continually evaluate them.

The consequences of not classifying information correctly are outlined as follows:

- Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.

- Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.
- Incorrect disposal can lead to unauthorised access to information. Disposal of information should be done using approved processes, equipment or service providers. Refer to the Data Destruction guide to understand when the disposal should be witnessed and recorded.

and

All of the 's information is, at a minimum, information. It is very likely that the information you create and use in your day-to-day job is information.

Examples include:

- Routine emails you send to your colleagues.
- Information posted on the intranet.
- Supplier contracts.
- Information and data you use to build a database, such as database secrets, record types, and field types.
- Most production data.
- Most non-production data.

means that the 's typical security measures are regarded as sufficient.

whilst not a formal classification, should be used sparingly, so that its effectiveness is not weakened. This is especially important when you consider that is already well-protected.

Use when you want to remind users to be careful when handling information. This asks them to use extra care, beyond what is expected for the baseline classification.

The threshold for classifying information as information is very high. It is unlikely that you will encounter information in your day-to-day job.

information should not usually be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is , contact the immediately.

To help decide whether some information should be classified as , ask yourself a simple question:

> If a hacker gained unauthorised access to the information, could it compromise the security or prosperity of the country?

The answer is most likely "No". In that case, you should consider using the classification.

If the threshold for classifying information as is very high, the threshold for classifying information as is extremely high. It is very unlikely that you will encounter information in your day-to-day job.

information should not be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is , contact the immediately.

To help decide whether some information should be classified as , ask yourself a simple question:

> If a hacker gained unauthorised access to the information, would it directly and immediately threaten the national security of the country?

The answer is most likely "No". In that case, you should consider using the or classification, as appropriate.

Reclassification examples

When deciding whether it is appropriate or desirable to reclassify information, a useful model is to consider what audience might get value from accessing the information. For example, if a hostile country might want the information, then the information might well be best classified as . Alternatively, a reclassification decision might be required as a result of changing threat advice from intelligence agencies.

Example 1

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as , with the handling caveat.

A user wishes to share a copy of the report "as-is" with their team. They cannot remove the handling caveat without prior discussion and agreement from the asset owner.

Example 2

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as , with the handling caveat.

A user wishes to share a subset of the report with their team. In particular, the report is substantially re-worked to remove all the private information. The user becomes the owner of this new asset. They are responsible for this new asset. They can decide that the handling caveat is not required.

The original report retains its classification and handling caveat.

Example 3

An asset owner creates a report. The report contains information about plans to handle a pandemic. The asset owner decides that the report should be classified as , with the handling caveat.

A user reviews the report. They realise that the information could potentially compromise the security or prosperity of the country. They decide to increase the classification of the report, and treat it as . They discuss this decision with the asset owner, so that the original report is correctly reclassified.

Handling and securing information

The is the most comprehensive guide on the security measures necessary for each of the three security classifications, including measures related to the following:

- Personnel (administrative) security.
- Physical security.
- Technical (information security).

The following sections set out the minimum measures you need to consider when handling and securing information within the different levels of classification.

Handling and securing and information

Type	Measure	Example
PERSONNEL	Make sure all staff including contractors undergo baseline security clearance checks.	A contractor working with the Security Team must undergo a baseline background check (i.e. BPSS check) at minimum. Refer to Security Vetting Guidance.
PHYSICAL	Make sure that you lock your screen before you leave your desk.	
	When working in an unsecured area, for example when working remotely, think about whether unauthorised people might be able to eavesdrop on your conversations, or look over your shoulder at your screen.	
	The has additional requirements when moving assets which can be found in the .	A software developer working from a flatshare should take calls in private, and use headphones and a privacy screen.

Type	Measure	Example
	Transferring information from one location to another requires planning and preparation, including a risk assessment. More information on this is available in the , and from your manager.	A technical architect working on the requirements for a new platform should lock their laptop before leaving their desk.
TECHNICAL	Protect information "at rest" by using appropriate encryption.	In the development of a new cloud-hosted solution, the following criteria should be considered: remote access connections and sessions are encrypted using an appropriate VPN; information stored "at rest" on end user devices and the cloud is encrypted; information in transit between the end user and the cloud service, such as payment services, is encrypted; and the cloud service used is a service.
	Appropriate encryption is also necessary when protecting information in transit.	When using any services over the PSN, make sure you fully read the agreements that you make with the service provider for details and definitions about the data you use or transfer using the service, to ensure you understand the risks to compliance, confidentiality, integrity, and availability.
	services can be used for information.	
	You must not use removable media such as an USB memory stick unless it is unavoidable. When you have to use one, it must be issued, encrypted so that the effects of losing it are minimised, and the data erased securely after use.	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the for further guidance.

Handling and securing information

Type	Measure	Example
PERSONNEL	Make sure employees and contractors undergo Security Check (SC).	A contractor working with the Security Team must have at least SC before being allowed to access information.

Type	Measure	Example
PHYSICAL	Consider using multiple layers of security to protect information. information should be held on a secure computer network which is physically isolated from unsecured networks and the internet.	Imagine you are moving locations for a server used to host information. The encrypted server is secured in a locked and monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after relevant parties, including the data owner, line manager, and the system owner, have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two SC-cleared individuals, for example, employees of a specialised commercial courier company.
	Transferring information from one location to another requires planning and preparation, including the completion of a Risk Assessment and the use of SC-cleared personnel. More information on this is available in the and from your manager.	
TECHNICAL	information at rest should be protected with very strong encryption. Contact the for more information.	
	Care should be taken to ensure that information in transit is only shared with defined recipient users through assured shared infrastructure or using very strong encryption.	
	information should be processed on IT systems which have been approved for the threat model. Advice on what commercial IT systems meet this requirement is available from the .	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the for further guidance.

Handling and securing information

Type	Measure	Example
PERSONNEL	Ensure employees and contractors undergo Developed Vetting (DV) security clearance checks.	A contractor working with the Security Team should have at least DV clearance before being allowed to access information.

Type	Measure	Example
PHYSICAL	Handling and storing information requires exceptional planning, monitoring, and record-keeping.	Imagine you are moving locations for a server used to host information. The encrypted server is secured in a locked and continuously monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after you, your manager, and senior managers have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two DV-cleared individuals, for example, employees of a specialised commercial courier company. When it happens, local police may need to be informed and involved in providing an additional layer of security.
	Working remotely with is not permitted due to the extreme sensitivity of the information.	
	Transferring information from one location to another requires even greater planning and preparation than for information, including the completion of a Risk Assessment by senior management and the use of DV-cleared personnel. More information on this is available in the and from your manager.	
TECHNICAL	When physical security measures cannot be used, information at rest should be protected with extremely strong encryption. Contact the in these circumstances.	
	Care should be taken to ensure that information in transit is only shared with defined recipient users through accredited shared infrastructure or using extremely strong encryption.	
	information should be processed on IT systems which have been approved the threat model. Advice on what commercial IT systems meet this requirement is available from the .	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the for further guidance.

Note: For further information on statutory disclosures and transfer to national archives, please refer to the .

Information Classification and Handling Policy

This document provides the core set of IT security principles and expectations on the handling and classification of information on IT systems.

The stores and processes a wide variety of information, some of which attracts an HMG protective marking or contains personal information. The has a duty to protect all the information stored and processed on its IT systems.

This policy outlines the Information Classification and Handling Policy for all information held on IT systems.

Related information

Technical Controls Policy on page 30

Scope

This policy covers all staff (including contractors and agency staff) who use IT systems.

The overarching policy on information classification and handling is maintained by Security. This document only contains IT specific policies which are in addition to the overarching policy.

The overarching policy can be found here.

All Users **must be** made aware of the Information Classification and Handling Policy, and provided with security awareness training which covers this policy.

All Users **must be** provided with refresher security awareness training which covers this policy every 12 months.

Inventory of assets

All information assets need be identified and have a nominated asset owner, to help ensure that the appropriate protection of these assets is maintained.

Examples of what an information asset constitutes are:

- Databases and data files.
- System documentation.
- User manuals, training material, operational or support procedures.
- Security documentation such as RMADS or disaster recovery plans.
- Archived backup data.

The list of information assets and associated Information Assets Owners is coordinated and maintained by individual business groups, where the responsibility resides with the business group SIRO.

All business groups **must maintain** a list of information assets, their associated named Information Asset Owner (IAO), and which IT systems they reside on.

Note: Some information assets might not be held on IT systems.

Deriving a classification

At the , all information assets are assessed against HMG guidance on business impact, and HMG guidance on the protection of personal data. This assessment is used to select the appropriate classification from the Government Security Classification scheme.

All information assets stored or processed on IT systems **must be** assessed for a Business Impact Level, where an impact level for the Confidentiality, Integrity and Availability for each asset is derived.

The Asset Owner is responsible for determining the classification that applies to an asset.

All users are responsible for applying the appropriate classification to information assets created or handled on an IT system, where a pre-existing classification does not exist.

Note: As outlined in the IT Security Policy, all data and assets must have IT security controls designed and implemented to protect Confidentiality, Integrity, and Availability.

Further information on the criteria and derivation for classification can be found at: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/.

Application of Government classification

The Government classification scheme defines how information should be labelled and handled. Output from IT systems containing information that is classified must carry classification labels where it is or higher. This includes, but is not limited to, printed reports, removable media, electronic messages (such as email) and file transfers.

All IT hardware and removable media assets **must** be labelled with the highest classification from among each of the individual information assets stored or processed on it.

Note: This classification might be reduced if sufficient security controls are applied, for example whole disk encryption, and if there is agreement with the system assurer or .

All output from an IT system **must** be given the classification of the highest of each of the individual information assets contained within that output.

Where applying a classification label is not feasible, an alternative method **must be** agreed with the system assurer or .

Further information on the criteria and derivation for classification can be found at: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/.

Information handling on IT systems

The policy for handling classified material applies to all IT assets and all outputs from an IT system.

Secrets management

A 'secret' is defined here as a sensitive piece of information that should be kept private. A secret usually has a technical system or user focus, for example a password, OAuth token or 'private key'. Private keys are secrets associated with SSH network connections, certificates, etc.

A 'secret' **not** the same as a classification.

The base principle

All secrets **must** be adequately protected from a loss of confidentiality or integrity. Secrets, much like other confidential data, must be controlled so they can only be viewed or influenced by authorised parties.

Application & infrastructure secrets

All secrets should be adequately protected and suitably stored.

Where possible, use infrastructure-based secrets management services such as AWS Key Management Service, AWS Systems Manager Parameter Store, Microsoft Azure Key Vault or Kubernetes Secrets on Cloud Platforms.

It should be rare and exceptional to store secrets within code repositories, such as in Github.com. Where secrets must be stored, they must be protected to control who has the ability to view or use those secrets. For example, to store a secret on GitHub you must use a tool such as git-crypt to encrypt the secret.

Secrets must never be stored in plain-text. This also applies to code repositories, even when the repository is set to a private mode.

Secrets for managing infrastructure must be issued as user authentication secrets, not a single shared secret.

User authentication secrets

User authentication secrets such as SSH private keys or tokens must be generated for each purpose and kept private.

Unless by intended design, authentication secrets should never be shared or published.

SSH private keys should be password protected where practical to do so.

Media handling

Removable media

Any systems or removable storage media used for work purposes must be encrypted to security standards. Security encryption is a mandatory government measure, and one of the most important methods we have to protect information.

What is 'removable' media?

Laptops and USB memory sticks are the 's most commonly used items of removable media. Removable storage media covers items available to users, such as USB memory sticks, writeable CDs/DVDs, floppy discs, and external hard drives.

Strictly speaking, magnetic tapes are also removable storage media, but it would be very unusual for the average user to have access to or to use magnetic tapes for business purposes.

security guidance specifies that USB memory sticks and other user-removable media should not be used to store departmental data. Only in exceptional circumstances, and where there is compelling business justification, should -approved USB sticks with device encryption be used.

USB memory sticks

This guidance is intended to ensure that data remains secure, and to mitigate the potential impact of lost data sticks.

1. You must only connect approved external removable storage media to systems.
2. Connecting non-approved memory sticks is a breach of security guidelines, and could result in disciplinary action.
3. If there is a genuine business requirement to save, retrieve or transfer data via removable media, fill in one of:

   - Removable media business case form
   - Data Movement form

   Additional guidance information is available about the Data Movement form. When the form is ready, send it to: .
4. Each request is evaluated by Operational Security, with a view to recommending the safest and most appropriate method to contain risk of loss.
5. Normally, you'll get a response within 5 working days.
6. Requests to use a memory stick or other removable media will normally only be granted when there is no other practical alternative. Where approval is granted. only encrypted memory sticks or other removable devices provided by the are allowed. Use of memory sticks or other removable devices will be subject to stringent conditions, and permitted only after user training.

If you need further assistance or information about this process, ask.

How do I know if my laptop, or USB stick, is encrypted?

All equipment provided through the 's recognised central procurement systems are encrypted and protected to security standards. You must use processes to obtain any equipment used for business purposes, including mobile computing devices and removable media.

What's expected of you

Keeping information safe is everyone's responsibility. Anyone using portable computing equipment must take particular care to safeguard the equipment and the information stored on it. Failure to do so may result in disciplinary procedures.

Secure disposal of IT equipment

The and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, both physical and virtual. These resources are procured and managed though suppliers, who are normally responsible for the secure disposal of the resources when no longer used.

However, there are also other physical and virtual resources across the estate which might have been procured and managed locally. It is crucial that they are disposed of in a secure manner, to prevent data being leaked.

Note: When disposing of or equipment, materials, or resources, you contact security:

Related information

Secure disposal of IT equipment on page 77
Secure disposal of IT - physical and on-premise on page 78
Secure disposal of IT - public and private cloud on page 80
Technical Controls Policy on page 30

Secure disposal of IT - physical and on-premise

This document is the guidance covering disposal of physical and on-premise media and data. It is intended to ensure that the confidentiality and integrity of data is maintained when physical hardware is decommissioned.

Related information

Secure disposal of IT equipment on page 77
Secure disposal of IT - physical and on-premise on page 78
Secure disposal of IT - public and private cloud on page 80
Technical Controls Policy on page 30

Physical Media and Associated Data

The and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, including photocopiers and printers, data centre hard and tape drives, desktop computers, laptops, USB memory sticks, and generic mobile devices. Some equipment might be the responsibility of a supplier to decommission and dispose of it safely and securely. Check asset tags or similar identifiers to determine and validate responsibility.

However, other devices across the estate might have been procured and managed locally. They be disposed of securely, to prevent information from being “leaked”.

Approved organisations

For help to arrange secure disposal by an approved organisation, contact .

and on Secure Disposal

The and give critical guidance on the secure sanitisation of storage media here and here, respectively, specifically regarding disposal and destruction of media, and the data contained within it.

The situations when sanitising data is required are:

- Re-use.
- Repair.
- Disposal; sanitising unwanted media and its associated data whilst it is controlled by the and before it is passed outside the .
- Destruction; destroying the media, and hence data it contains, onsite or offsite.

Determining data deletion and destruction methods

To determine the data disposal and the media's destruction method, based on the type of equipment and its security classification, use the following table.

The table contains two columns, called “Data deletion method” and “Destruction method”, which are defined as:

Data deletion method	Covers assets if they remain within the , and have not reached end of life. For example, the device can be re-used or reallocated to a different user, or repurposed for a different function.
Destruction method	Covers assets that have reached end of life, and need to be physically destroyed onsite or offsite.

Note: If the data is encrypted, then only the key needs to be deleted or erased, and the table does not need to be followed.

If the table does not cover your exact requirement, contact .

Note: When disposing of or equipment or materials, always contact .

Equipment or asset type	Data deletion method	Destruction method
Flash (USB)	Delete the data, or erase using manufacturer instructions.	Destroy using commercially available disintegration equipment, to produce particles of a maximum of 6 mm in any direction.
Hard disk drive. This includes data centre disk drives.	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Break the platters into at least four pieces. This can be carried out either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a lower level degauss (refer to the explanation after this table), and then apply a destructive procedure that prevents the disk from turning. For example, punch holes into the platters, or twist or bend them.
Magnetic tapes and floppy disks This includes data centre tape drives.	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Destroy using a commercially available shredder that meets a recognised international destruction standard. Particles of tape should be no larger than 6 x 15 mm. Alternatively, apply a lower level degauss and then cut the tape to no larger than 20 mm in any direction.
Optical media	Data deletion is not possible. Refer also to the note about RW-capable media after this table.	Shred or disintegrate using equipment that meets a recognised international destruction standard. Particles should be no larger than 6 mm in any direction.
Monitors	Overwrite on-board storage by displaying non-sensitive data on the screen for a few minutes before powering off. If a monitor screen has legible “burn-in” of sensitive information it be re-sold or donated.	Monitors can be disposed of by: (1) Returning the product to the manufacturer who align to formal waste disposal responsibilities, or (2) taking the item to a professional waste disposal facility, or (3) reselling or donating to a non-profit organisation, once basic sanitation procedures have been performed. Ensure there is no “burn-in” of sensitive information, and that the device has not reached its end of life. If the end of life monitor contains mercury, it is considered hazardous waste and its disposal align to WEEE 2013 Regulations using specialist methods such as disassembly to remove the mercury containing backlights for specialist treatment and the separation of the remaining material streams.

Note: A lower level degauss is a process using specialised equipment to erase data totally, by eliminating the unwanted magnetic field (information) stored on tape and disk media.

Note: Theoretically, data deletion is possible on some RW-capable media. For simplicity, however, the safer assumption is that rewriting and therefore data deletion is not possible on optical media.

Owners of the data storage devices are responsible for procuring services that meet the necessary destruction outcomes as described previously.

Wherever possible and appropriate, managers should pool together equipment with that of local colleagues to share service costs.

Data destruction verification

As part of the physical media or data destruction by the or its suppliers, validation of destruction be carried out. This is to ensure that data handling processes align with the Asset Management Lifecycle policies. This includes:

1. The or supplier scans the hard drive or physical media asset tags or barcodes.
2. The or supplier carries out data destruction (as per the previous table).
3. The or supplier confirms hard drive or physical media data destruction by providing reasonable proof. This can include:
   a. Providing an inventory of physical media in their possession.
   b. Reconciliation carried out on the physical media scanned/received matching the physical media destroyed.
   c. A witness in attendance to sign a destruction certificate that is be stored in a secure space or network share.

Note: An alternative to the previous steps is to use a leading enterprise erasure tool that provides a certificate aligned to NIST 800-88 Guidelines for Media Sanitization. Such a tool verifies:

1. When the physical media was destroyed.
2. That verification was performed.

If you are based in a London HQ site the Accommodation Team coordinates bulk secure disposal; please contact them in the first instance.

Note: All destruction certificates and destroyed assets be supplied to the hardware team to update CMDB. This can be done using the technical portal to “Bulk upload CIs - update”, or alternatively by emailing the details to: MoJITAssetManagementTeam@justice.gov.uk.

Transporting data between sites securely

If you have any concerns about moving items between sites securely, contact .

Guidance on the transportation of secure data is located in the CPNI guidance: “10. Transport of sensitive items”.

The previous guidance is also referenced in the CAS Sanitisation Service Requirement, under section “MIT001 – Keep items secure during transportation” on page 9.

Secure disposal of IT - public and private cloud

This document is the IT Disposal of Equipment Guidance covering:

- Data sanitisation and deletion within a public or private cloud environment that a Service Provider hosts.
- The decommissioning of Storage Area Network (SAN) and Virtual Machine (VM) based technology.

It is designed to ensure the confidentiality of data remains when a cloud service is decommissioned.

This information is part of the asset management policies and guidance on media handling.

Note: For disposal of physical on-premise media and data, refer to the Secure disposal of IT - physical and on-premise guidance.

Related information

Secure disposal of IT equipment on page 77
Secure disposal of IT - physical and on-premise on page 78
Secure disposal of IT - public and private cloud on page 80
Technical Controls Policy on page 30

cloud environments overview

The consumes several public (shared cloud) and private cloud platforms, operating over 900 different technology systems ranging from internal IT tools or solutions to case management solutions.

Public cloud service environments are delivered through the internet. They are shared across organisations using a "multi-tenant" model. For example, a service provider hosts a public environment that gives the and other customers a portion of the same physical server hardware to run their website or application.

Private cloud environments differ, as they are dedicated to a single tenant. They are intended to address concerns on data security. They may also offer greater control because resources are not shared with other tenants.

Public and private clouds both have different ways of ensuring compliance. Therefore, compliance should be evaluated using the government's Cloud Security Principles. In addition, these principles should be assessed against several other factors outlined in the government's technical guidance on securing your cloud environment.

NCSC on sanitisation and disposal of cloud assets

asset owners or administrators be confident that:

- All data stored in a cloud service are erased when resources are moved or re-provisioned, when the resources are no longer required, or when the asset owner requests or carries out the erasure of the data.
- Storage media that has held data is sanitised or securely destroyed at the end of its life.

Note: For more information on this approach, refer to NCSC guidance on the sanitisation of cloud assets.

Equipment destruction

asset owners or administrators ensure that for all data stored in a cloud service:

- All equipment containing data, credentials, or configuration information for the service is identified at the end of its life and before it is recycled.
- Any components containing sensitive data are sanitised, removed, or destroyed.
- Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.

Note: For more information on this approach, refer to NCSC guidance on equipment disposal.

Checklist for the sanitisation and disposal of cloud assets

Due to the possible lack of control of physical infrastructure, a checklist of questions to ask a cloud provider to establish a baseline for data sanitisation and deletion is provided.

Reference	Action to help ensure sufficient data sanitisation and deletion with a cloud provider
1.	A standardised process to be agreed including credible witnesses, describing how private/public cloud service providers store and handle hard disks for decommissioning until destruction. This be aligned to the following controls as outlined in ISO 27002: 8.3.1 - Management of removable media (Control) "Procedures be implemented for the management of removable media in accordance with the classification scheme adopted by the organization." 11.2.7 - Secure Disposal or re-use of equipment (Control) "All items of equipment containing storage media be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."

Reference	Action to help ensure sufficient data sanitisation and deletion with a cloud provider
2.	Standardised procedures agreed between the and the Cloud Provider to establish a chain of custody including crypto-shredding or an initial software erasure and then degaussing the disk and/or shred/incinerate/pulverise. This be aligned to the following control as outlined in ISO 27002: 8.3.2 - Disposal of media (Control) "Media be disposed of securely when no longer required, using formal procedures."
3.	If required, the cloud provider agrees they securely deliver in transit hard disks that contain data, which the destroy.
4.	Optionally, asset owners using the responses to checklists 1 to 3 can establish a data sanitisation strategy SLA aligned to Data Security Lifecycle Management standards, specifically sanitisation and destruction (end of life).

Note: The Data Security Lifecycle Management concept is described in the Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 (CCA CSM v4.0). Refer to section 5.1.2: The Data Security Lifecycle on page 62.

Note: To ensure that data in the cloud is sanitised sufficiently and that the devices or hard drives they are stored in meet data management security standards when destroyed, it might require specific clauses in the contract with the cloud provider.

Note: If the cloud provider has a mechanism for resilience or redundancy that duplicates data, this duplicated data also be sanitised or destroyed using the checklist provided. All duplicated data be sanitised at the same time. The destroys all decryption keys held in their possession to ensure this occurs. This makes all the duplicated cloud data unreadable. This method is called crypto-shredding.

When duplicates of data cannot be destroyed immediately, there be methods in place for protecting and controlling the data until data destruction is assured. This includes the supplier providing a formal declaration of destruction. If any destruction tasks are delayed, a confirmation date of final data destruction be provided.

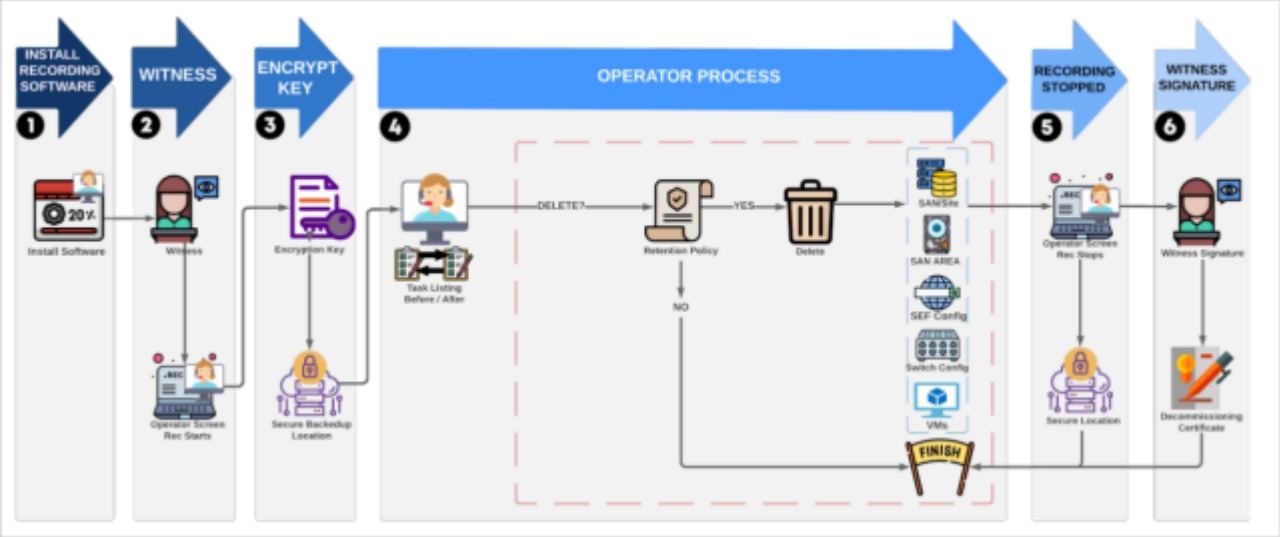
Data deletion - Verification for virtual devices and SAN allocations (public cloud or on-prem)

When working on an public cloud or on-premise virtual infrastructure, obtaining a decommissioning or destruction certificate cannot be carried out according to the method used for the 's on-premise physical servers and disk arrays when they are wiped, blanked, destroyed, or overwritten. This is because these infrastructures might be needed to support other services or infrastructure still in use.

For example, a single on-premise physical server might host eight virtual servers providing various services. If three of these virtual servers are deleted, the other five need to continue to operate. Similarly, an on-premise firewall might have a virtual context or a subset of rules that need to be removed, but the physical equipment is still required to provide services to other devices.

A soft and hard decommissioning approach for on-prem virtual devices might also be required. A soft decommissioning involves switching off the resource, ensuring that it cannot restart on a scheduled basis. This means stopping all hosted service or application, powering down the resource, and setting any remaining firewall rules to block all traffic to or from the resource. Once this soft decommissioning is complete, a hard decommissioning can take place. Hard decommissioning involves deleting the configuration, images, and storage that the virtual devices used and returning the resources to a resource pool.

The process used for SAN or VM items destruction and decommissioning is described next.



1. Install a screen recording tool on the operator's terminal. In cases where it is impossible to install a recording tool on a device, screenshots showing before and after states are acceptable if agreed in advance.
2. Ideally, have a witness sit next to the operator and start the screen recording tool. If this is not possible, the witness can view the screen recording after the decommissioning activity.
3. Encryption keys for the solution be archived for backup retention purposes, if necessary, onto a secure storage space.
4. For each of the given technologies, the operator create an initial listing of the resource, then run the decommissioning task, then finish by creating another listing to show that the change has occurred.
    a. Depending on the process used to create or maintain backups, some jobs might need to be removed. However, backups be deleted without consulting the retention policy and confirming that deletion is compliant with policy. This check applies to all decommissioning steps.
    b. The operator, if possible, formats the SAN areas used for the files and "zero's" them by overwriting all storage with binary 0 data. The operator then deletes the various SAN LUNs, Arrays, Volumes, and other storage units in the SAN. Each of the storage units is reallocated to free space. This is then verified with listings of the SAN structure.
    c. Any virtual machines are permanently deleted in the virtual machine control panel. An attempt be made to list and restart the machine; this should provide evidence that the virtual machine has been permanently removed.
    d. Any firewall or other Security Enforcing Functionality (SEF) configurations be removed from the live service.
    e. Any switch configurations, such as IP addresses or subnet masks, be removed.
5. Screen recording is stopped.
6. Witness signs the decommissioning certificate, and the screen recording is stored in a secure storage space.

Note: There are free versions of screen recorder tools that might be used. The tool be assessed, before use, by requesting an security team review using this form. Refer to the guidance on requesting that an app be approved for use. An alternative option would be to use Teams to record the decommissioning via screen share.

Working securely with paper documents and files

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.PPR.xxx**, where **xxx** is a unique ID number.

Audience

This guidance complements the overall security policy.

This guidance applies to all employees, contractors, partners, and service providers, including those on co-located sites and sites owned by other public bodies. This includes employees of other organisations who are based in, or work at, occupied premises.

POL.PPR.001: Agencies and arm's length bodies (ALBs) comply with this corporate framework but establish their own arrangements tailored to operational needs and supplement this framework with local policy or guidance for any business-specific risk.

Objective

The requires employees and contractors to get into the habit of looking after the information that they work with, whether it is on paper or stored electronically, in the same way that they would take care of their personal valuables.

Scope and Definition

This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office. It covers any information that relates to the business of the , its stakeholders, or partners, where the information has been printed out or written down on paper.

Note: This guidance applies also to the contents of personal information systems, such as notebooks.

This guidance outlines the basic principles of working securely with paper documents and files.

Context

All information is valuable. There is a requirement to protect everything that relates to the department's business, including information provided by others.

Note: The protection requirement applies to all information, not just information that is covered by the Data Protection Act or classified under the government-wide security classification system.

There are different rules for managing and protecting various kinds of paper-based information. You know how to:

- Identify the correct security level for the information you work with.
- Handle the information according to the relevant rules.

Responsibilities

All employees, contractors, partners, service providers and employees of other organisations who are on premises or co-located sites remain accountable for the security, health,and safety of themselves, colleagues, and the protection of departmental assets.

Policy statements
Identifying the correct security level

The uses the government-wide security classification system to indicate the level of security that the various types of information require. The different classifications are based upon the harm that would be caused if controls were breached.

POL.PPR.002: Within the classification, material does not normally need to have the classification written on it. However, particularly sensitive information be marked with the handling caveat if it requires more robust access and handling controls to prevent more damaging consequences from disclosure.

POL.PPR.003: Information handled in the might not always have a visible classification marking. If any file contains material with a marking, then the cover of the file be marked with the highest level of any of the contents.

To identify the right security level for information, think about:

- How sensitive that information is.
- Whether it contains personal data that could be used to identify individuals.
- What the consequences might be if the information was compromised or misused.
- Whether the information is likely to be under threat from anyone with a high intercept capability. If so, the information might require marking at a higher classification than .

If you are in any doubt, ask your line manager or contact .

Allocating security levels and marking

POL.PPR.004: If you are generating original information, you apply the standard rules to decide which classification to use. Do not set security levels higher than necessary. Set the classification that is appropriate at the time. Classification can be altered later if circumstances change, such as when material is no longer embargoed or has been released intentionally for consultation.

POL.PPR.005: For material at or higher classifications, the classification be written in capitals at the top and bottom of each page of the document. You use the header and footer facility if creating electronically, and include page numbers by using the format `Page x of y`. You only create documents at classification levels higher than on approved IT systems. Files and documents be marked according to the most sensitive piece of information included.

Data Protection Act

If the information in the documents or files can be used to identify living individuals, or could identify living individuals when used in conjunction with other material, then the information is covered by the Data Protection Act (DPA). The Act covers not only information such as name, address, and date of birth, but also expressions of opinion about or intentions towards an individual.

POL.PPR.006: Paper-based information that is covered by the DPA be managed according to the general principles of working securely with paper documents and files set out here.

Handling paper-based information in the office

Think carefully before leaving papers unattended on desks, in the same way that you would avoid leaving your own personal correspondence – or even a purse or wallet – in plain view.

The has a clear desk policy that is intended to ensure information is seen only by people who 'need to know' it.

This means:

- Not leaving documents or files on a desk when not being used.
- Locking documents or files in a secure cabinet when you leave the office.

Failure to follow this policy could expose files and papers to the risk of being seen during the working day by other staff, or visitors to the office and, out of hours, by guards and cleaners. Even apparently non-sensitive information should be looked after. Putting papers away also protects them from damage from fire, smoke, or water.

There are different controls regarding how the various levels of classified information are secured. Refer to the Information classification, handling and security guide for more information.

Taking documents and files out of the office

Occasionally, you might need to take information outside premises. Examples might be when you are working from home, or moving between buildings. At such times, it is likely that you'll be carrying valuable information within documents, paper files and personal notebooks.

POL.PPR.007: Always check first whether it is really necessary to take documents out of the office. If it is essential to do so, you get permission from your line management, especially if the information includes:

- Personal information, including anything that relates to an identifiable individual or individuals, such as staff, stakeholders, partners, or customers.
- Material marked .

POL.PPR.008: You get permission from a head of division, or from a member of the Senior Civil Service (SCS) if the information is marked at a level higher than . Removal or relocation of information marked at a level higher than be noted and recorded on a register, and a record kept of when the material is logged back in.

POL.PPR.009: If you are carrying papers out of the office, you protect them against accidental loss such as an accident or distraction, causing you to drop or misplace them.

POL.PPR.010: Ideally, carry papers in an unmarked case. For papers marked or higher, or when using public transport, you use a lockable case.

POL.PPR.011: For short journeys, such as on foot, and where you are not stopping or using public transport, it is acceptable to carry papers in a plain envelope, marked only with your name and office address.

POL.PPR.012: If carrying papers to a meeting at a different location, you allow sensitive details to be visible. The reason is that they could be photographed by a journalist.

POL.PPR.012.001: Papers be stapled together or otherwise secured in a package. This is to limit dispersal if the carrying case or envelope becomes damaged or opened.

POL.PPR.013: Cases or envelopes have the minimum details necessary on the outside to assure safe return of the item, if lost, without having to be opened to reveal the contents.

POL.PPR.014: Documents be left unattended in public places or in an unattended car. Care be taken if you are reading protectively marked information in public places where you might be overlooked, such as a train, or where it might be difficult to retrieve a document if you lost hold of it, for example if you dropped it, or it was blown away.

If you are taking papers home, ensure that they are not readily accessible to other members of your household. Take precautions to minimise their loss. If the papers would normally be locked away in the office, try to do the same at home.

Sending documents

Options for sending documents are covered in the Sending Information guidance note.

Disposing of paper information

offices have bins or bags that are specifically intended for secure waste disposal of documents or files, including:

- Personal information that relates to an identifiable individual or individuals.
- Sensitive information that be disclosed.
- Any material bearing a visible classification marking.

POL.PPR.015: You read and follow the secure waste disposal guidance on the Intranet before disposing of any document or files.

POL.PPR.016: Before disposing of information, you check whether it should be retained on a file, and whether it is covered by a 'retention schedule'. The can advise on this.

Long-term storage

The has arrangements for the secure long-term storage of paper documents and files. If you want to keep paper-based information, but no longer need to regular access to it, refer to the information on the Intranet regarding keeping, deleting, and disclosing information. The can provide additional guidance.

What to do if you think there has been a security breach

POL.PPR.017: If you suspect that the security of the information you work with has been compromised in any way, you report it immediately.

Note: A security breach does not have to involve the actual loss of information. The potential loss of information also counts. For example, if a security cabinet has been left unsecured, there may be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

POL.PPR.018: The level of risk and potential impact to assets, and, most importantly, physical harm to our people and the public, determines the controls to be applied and the degree of assurance required. The ensure a baseline of physical security measures are in place at each site, and receive annual assurance that measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, such as in response to a security incident or change in the Government Response Level.

POL.PPR.019: The implementation of all security measures be able to provide evidence that the selection was been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the , and .

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards is subject to annual review or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting .

Access control

Business requirements of access control

Access Control guide

This guide explains how the manages access to its IT systems so that users have access only to the material they need to see. This guide has sub-pages which provide in-depth Access Control guidance.

Related information

Managing User Access Guide on page 100
Minimum User Clearance Requirements Guide on page 48
Multi-Factor Authentication (MFA) Guide on page 101
Passwords on page 116
Privileged Account Management Guide on page 88

Who is this for?

This guide is aimed at two audiences:

1. The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation.
2. Any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the .

Information security principles for access control

These are the Access Control principles you need to know.

- **The 'need-to-know' principle:** Restricting access to information based on a business requirement.
- **Non-repudiation of user actions:** Holding a user accountable for their actions on an IT system.
- **The 'least privilege' principle:** Assigning the least number of privileges required for users to fulfil their work, usually done through Discretionary Access Controls (DAC).
- **User Access Management:** Managing user access to systems and services through a formal user identity lifecycle process.

Access control principles

Effective access control should be implemented by following these four principles.

1. **Identification:** The should provide a single, unique ID assigned, named and linked to a private account for each user. For example, Lesley is issued a user account that only Lesley uses, and only Lesley can access. This is important so that logging information is accurate (refer to the following Accounting section for further information).
2. **Authentication:** To access systems, users must authenticate themselves. They can do so using:

   - something they know (such as a password - the primary authentication method used at the)
   - something they have (such as a smart card)
   - something they are (biometric authentication such as a fingerprint, voice recognition, iris scan and others)

   Systems holding sensitive information, or systems that are mission critical to the , must use Multi-Factor Authentication (MFA) to prove user identity. Refer to the Multi-Factor Authentication Guide and Password Management Guide for further information. If you wish to use an additional method of authentication you should

review the National Cyber Security Centre (NCSC) guidance and contact the Cyber Assistance Team (CAT). For information on authentication methods including OAuth, refer to the Managing User Access Guide.

3. **Authorisation:** Authorisation is the function of specifying access rights/privileges and resources to users, which should be granted in line with the principle of least privilege. Reducing access privileges reduces the "attack surface" of IT systems. This helps to prevent malware and hackers from moving laterally across the network if they compromise a user account.
4. **Accounting:** Successful and unsuccessful attempts to access systems, and user activities conducted while using systems must be recorded in logs. Please refer to the Security Log Collection Guide for more information. This will help to attribute security events or suspicious activities to users who can be supported to improve their behaviours or held accountable for their actions.

Consider the following points when creating activity logs.

Logs should be:

- stored securely
- backed up, so that data are not lost if there is a system unavailability
- managed according to the sensitivity of the data they hold, for example personal information. Contact the Data Protection Team for advice on protecting sensitive personal information - .
- stored for a minimum of 6 months

Logs should not be:

- retained for longer than 2 years unless otherwise stipulated. Retention rules may vary on a case by case basis so check with the Data Privacy Team, the Cyber Assistance team, and the Data Protection Officer if a Log involves personal information. Refer to the Accounting Guide for further information.
- tampered with under any circumstances, for example through modification or removal.

Refer to the Security Log Collection Guide for more information.

Segregation of duties

In some parts of the , segregation of duties is used to help to reduce the possibility that malicious activity takes place without detection.

You can segregate duties in various ways, including:

- implementing manual or automated Role Based Access Control (RBAC), to enforce user authorisation rights.
- regularly reviewing audit logs to check for suspicious activity
- ensuring strict control of software and data changes
- requiring that a user can perform only *one* of the following roles:
    - identification of a requirement or change management request (Business function)
    - authorisation and approval of a change request (Governance function)
    - design and development (Architect or Developer function)
    - review, inspection, and approval (another Architect or Developer function)
    - implementation in production (System Administrator function)

Privileged Account Management Guide

Related information

Access Control guide on page 87

Introduction

This guide explains how to manage privileged accounts in order to minimise the security risks associated with their use. This is a sub-page to the Access Control Guide.

How to manage privileged accounts

Holders of privileged accounts, such as system administrators, have privileges to perform most or all of the functions within an IT operating system. Staff should have privileged accounts only when there is a business need, in order

to prevent malicious actors gaining privileged access to systems. The requires that ownership and use of privileged accounts must be monitored and audited on a monthly basis.

Privileged accounts should be protected with the following controls.

DO
✓ Ensure that privileged users only use their system administrator account when elevated privileges are required. Their general user account should be used for all other work activities.
✓ Ensure that management or administrative access is limited to users who have been suitably authenticated and have been authorised to perform the specific action. Only those with a genuine business need should have an administrative account, however there should be a sufficient number of administrators that there is not a single point of failure due to absence or administrators leaving the . This should be enforced through the principle of least privilege.
✓ Ensure that Multi Factor Authentication (MFA) is used where possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. MFA should also be used to access enterprise level social media accounts. Refer to the Multi-Factor Authentication Guide for details of preferred MFA types. Where MFA cannot be used on a system, this is considered an exception and should be logged in the risk register.
✓ Ensure that MFA is mandated for a privileged user to conduct important or privileged actions such as changing fundamental configurations including changing registered email addresses or adding another administrator.
✓ Ensure that MFA is used as a validation step, to confirm actions requested by users, such as a MFA re-prompt when attempting to delete or modify data.
✓ Ensure that default passwords are managed securely and safely, as described in the Password Manager guidance.

DON'T
✖ Allow privileged users to use their privileged accounts for high-risk functions. These include reading emails, web browsing, using an 'administrator' login on an end-user device (such as a mobile device), or logging into a server as 'root'.
✖ Leave default or factory set passwords for any accounts but particularly for privileged system accounts, social media accounts and infrastructure.
✖ Allow a user to have a privileged account, unless they are a service provider and require a privileged account for that specific service.

Access Control Policy

This policy gives an overview of access control security principles and responsibilities within the . It provides a summary of the policies and guides that apply to access management.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.ACP.xxx**, where **xxx** is a unique ID number.

Related information

Technical Controls Policy on page 30

Audience

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also

	includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Defined as any other business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data), for or on behalf of the .
General users	All other staff working for the .

"All users" refers to General users, Technical users, and Service Providers, as defined previously.

Policy Sections

This policy aligns to industry standards and frameworks, and is divided into four security categories (and subsections describing the controls) addressing:

1. Business Requirements of Access Controls.
2. System and Application Access Controls.
3. User Access Management.
4. User Responsibilities.

Best Practice Framework - IAAA

Identification, Authentication, Authorisation, and Accounting (IAAA) are the core principles of an Access Control Policy. The principles apply to all security categories described in this policy, as follows:

Identification	**POL.ACP.001:** The provide a unique ID that is assigned, named, and linked to a private account, for each user.
Authentication	**POL.ACP.002:** To access systems, users authenticate themselves.
Authorisation	**POL.ACP.003:** Specifying access rights, privileges, and resources to users be granted in line with the principle of least privilege.
Accounting	**POL.ACP.004:** Successful and unsuccessful attempts to access systems and user activities conducted while using systems be recorded in logs.

Note: If any of the controls within this policy cannot be applied, they are considered an exception to be assessed for inclusion within a risk register.

Business Requirements of Access Control

The 's business or strategic requirements limit access to information and information processing facilities, as described in the following subsections.

Access Control Policy

POL.ACP.005: This access control policy be established and maintained, based on business and information security requirements, to inform associated standards and guidance, for all users.

POL.ACP.006: The policy also follow the additional principles of:

- "Need-to-know".
- Non-repudiation of user actions.
- Least privilege.
- User access management.

Access to Networks and network services

This subsection aligns to the principle of least access, to protect a network and network services which are covered in other areas of this policy, specifically:

- Authorisation procedures for showing who (role-based) is allowed to access what, and when. Refer to subsections Information Access Restrictions and Management of Privileged Access Rights.
- Management controls and procedures to prevent access and real-time monitoring. Refer to the categories called System and Application Access Control and User Access Management, with monitoring covered in the subsections called Password Management System and Management of Privileged Access Rights.

System and Application Access Control

POL.ACP.007: The strive to prevent unauthorised access to systems and applications, as described in the following subsections.

Information Access Restrictions

POL.ACP.008: Access to information and application system functions be restricted by following access control policies and procedures.

POL.ACP.009: In particular, System Designers and Administrators use adequate authentication techniques to identify with confidence user access to their system or data, using the principle of "least privilege". Refer to the guidance on Authorisation for more detail.

Secure Log-on Procedures

POL.ACP.010: Where required by the access control policy, access to systems and applications be controlled by a secure log-on procedure, including the following points:

- **POL.ACP.011:** Multi-user (MU) accounts be managed carefully using PAM or a Bastion server, to avoid accountability type security risks. Refer to the Multi-user Accounts and Public-Facing Service Accounts guidance.
- **POL.ACP.012:** Front-end users accessing the 's public services authenticate via the GOV.UK Verify Service. Refer to the User Facing Services guidance.
- **POL.ACP.013:** System Designers for internal systems use the 's single sign-on (SSO) solution to authenticate via an Identity and Access system.
- **POL.ACP.014:** Passwords be stored or transmitted over the network in clear text, nor be protected with encryption that has known security weaknesses. Refer to the Password Management Guide.

Password Management System

POL.ACP.015: The 's password management systems be interactive, ensure quality passwords are used, and store and transmit passwords in a protected form, specifically:

- **POL.ACP.016:** Systems support password requirements that are provisioned and maintained by System Administrators.
- **POL.ACP.017:** System Administrators always have time-bound administrative sessions, which be protected using Multi-Factor Authentication (MFA).

  POL.ACP.018: The system regularly monitor, review, and revoke these sessions when no longer required.
- **POL.ACP.019:** Strong passwords, separate and unique for each account or service, be created and maintained by all users. Refer to the Password Management Guide, Roles and Responsibilities section, Passwords and CyberAware advice.
- **POL.ACP.020:** Users change a password initially received by a system or support team before carrying out tasks. Refer to Passwords.
- **POL.ACP.021:** Password history and blocking of commonly guessed passwords be enabled in a system. Refer to the Password Creation and Authentication Guide.
- Regular password change is not required, as it is an outdated and ineffective practice.
- **POL.ACP.022:** Password managers or vaults used at the align to industry standards to securely store and transmit passwords in a protected form. Refer to Password Managers and Password Vaults and Managers.

Note: Contact the Security team if you have specialised needs when selecting or using a storage tool.

Access Control to Program Source Code

- **POL.ACP.023:** When coding in the open, Technical users and Service Providers follow coding best practices and keep code separate from configuration and data.

User Access Management

User access management ensures authorised user access, and prevents unauthorised access to systems and services. These are described in the following subsections.

User Registration and de-registration

POL.ACP.024: A formal user registration and de-registration process be implemented to enable the assignment of access rights, specifically:

- **POL.ACP.025:** Multi-User (MU) or shared ID accounts only be used directly if there is no alternative. Refer to Multi-user Accounts and Public-Facing Service Accounts.
- **POL.ACP.026:** The identity of the new user be confirmed. For all staff members, this is established as part of pre-employment screening and vetting using the Baseline Personnel Security Standard (BPSS), which is the joint responsibility of HR (performed on their behalf by Shared Services Connected Ltd), and a line manager. Refer to Security Vetting and the BPSS information.
- **POL.ACP.027:** The hiring line manager submit a ServiceNow Order IT role-based access request on behalf of the new user. For example, a list of Role-based access control (RBAC) groups or applications.
- **POL.ACP.028:** The hiring manager's line manager (or the budget holder) authorise the application for user registration within ServiceNow My Approvals. This confirms the user's identity, and hence access rights, are correct.
- **POL.ACP.029:** Confirmation of the Clearance Level be initiated by a line manager, and carried out by United Kingdom Security Vetting (UKSV) to recruit new staff (civil servants, armed forces and temporary staff), or staff changing their roles. Refer to Clearance Levels.

Note: For Contractors or Agency staff, HR/SSCL do not seek assurance that the BPSS check has been completed; instead, the responsibility is with the line manager, via the receipt of the Baseline Personnel Security Verification Record Form, as described here.

POL.ACP.030: De-registration of users be at the request of line managers and follow the JML process found here. The following controls need to be adopted for leavers:

- **POL.ACP.031:** Line Managers authorise account removal. The associated leaver's process can be found on the HR intranet page.
- **POL.ACP.032:** User accounts and their access rights be removed once an individual has left the organisation or no longer requires access to the system(s).
- **POL.ACP.033:** Existing user accounts be reviewed every three months by the System Administrator to confirm those not used in the last three months, and then with HR to approve accounts for removal.
- **POL.ACP.034:** Remote access authentication token usage be reviewed by the System Administrator every three months, and when a token is identified as unused in the last three months, the account disabled.
- **POL.ACP.035:** Assigned User roles and privileges be reviewed every six to twelve months, and those no longer required removed.

For further information on user de-registration, refer to the Enterprise Access Control Policy.

User Access Provisioning

POL.ACP.036: A formal user access provisioning process be implemented to assign or revoke access rights for all users to all systems and services. Specifically for , this includes:

- **POL.ACP.037:** The security clearance required by staff to access specific account types align to the 's UK security clearance levels, as per requirements such as segregation of duties. Refer to minimum user clearance level guidance, by contacting .
- **POL.ACP.038:** MFA be used to ensure access to Information, and is only granted to users once their identity is confirmed. Refer to the Multi-Factor Authentication guidance.

- **POL.ACP.039:** All data access employ adequate authentication techniques to identify the system or user with confidence, where that system or user requires access to systems or data. Refer to the Authentication guidance.
- **POL.ACP.040:** System Administrators maintain the 's systems' security, with failure to comply compromising the organisational infrastructure.
- **POL.ACP.041:** System Administrators maintain an active list of all active and suspended users, and maintain their access control to services or applications.
- **POL.ACP.042:** System Administrators , on a minimum quarterly basis (rotated with other Admins), conduct an account audit to check:
  - Any escalation of privileges from non-administrator to administrator.
  - Any forwarding of email accounts.
  - Any taking ownership of user accounts.
- **POL.ACP.043:** A user leaving move their data to a shared folder if needed for retention. Refer to the Account Deletion process.
- **POL.ACP.044:** If anyone with an account leaves the organisation, system administrators retrieve the user's equipment and suspend the account.
- **POL.ACP.045:** If a user leaving has not returned all assets, the line manager initially contact the via Live Chat, or Telephone (0800 917 5148), and raise a security incident, with the following form completed and emailed to . Refer to the Leavers checklist for managers for more information.

Note: The previous points are covered by the System Administrators guidance.

Management of Privileged Access Rights

POL.ACP.046: The allocation and use of privileged access rights be restricted and controlled using the 's Access Control Policy. This includes:

- **POL.ACP.047:** Users only use their system administrator account when elevated privileges are required.
- **POL.ACP.048:** MFA be used with privileged accounts, including access to enterprise-level social media accounts.
- **POL.ACP.049:** Default passwords be managed securely and safely by privileged account users, described in the Password Manager guidance. Refer to the Privileged Account Management guidance for more information.
- **POL.ACP.050:** All users with ownership and use of privileged accounts have these secured, controlled, monitored, and audited by System Administrators every month using an industry-standard Privileged Access Management (PAM) tool. Refer to the Privileged Account Management guidance for more information.

Note: Privileged access rights provide a Technical user or a Service Provider with an enhanced level of access to the 's information systems, compared to a General user. This can include the authorisation to configure networks or systems, provision and configure accounts and cloud instances, and so on.

Management of Secret Authentication Information of Users

POL.ACP.051: The allocation of secret authentication information, such as passwords or encryption keys, be controlled through formal management:

- **POL.ACP.052:** User password management be configured, so a password is changed after the initial log-on and invalid if not used in a specified time. Refer to the Passwords guidance.
- **POL.ACP.053:** System Administrators and systems never send passwords by email, as it is an unsecured channel.

  POL.ACP.054: Instead, users receive a time-limited password-reset link or code to their registered email address or phone number. Refer to the Government guidance "Send a link to trigger password resets".

Review of User Access Rights

POL.ACP.055: System Administrators review users' access rights at regular intervals:

- The review of user access rights is covered in this policy under User Access Provisioning.

Removal or Adjustment of Access Rights

POL.ACP.056: All employees and external party user's access rights to information and information processing facilities be removed upon termination of their employment, contract or agreement, or adjusted when changing their role:

- The removal or adjustment of user access rights is covered in this policy under User Access Provisioning.

User Responsibilities

Users are required to follow the 's practices in the use of secret authentication. This is described in the following subsection.

Use of secret authentication information

- **POL.ACP.057:** All users follow the 's password policy, as referenced in the Password Management System, and the associated tools referenced in the Secure Log-on Procedures.

Enforcement

- This policy is enforced by lower-level policies, standards, procedures, and guidance.
- Non-conformance with this policy could result in disciplinary action per the department's disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they may also be prosecuted. In such cases, the department will always co-operate with the relevant authorities and provide appropriate evidence.

Enterprise Access Control Policy

All staff (including contractors and agency staff) are entitled to be granted access to the information which is required for their work, subject to their level of clearance and employment status.

Access control mechanisms provide the ability for IT systems to control the levels of access granted to an individual User or defined groups of individual Users. This section outlines the process for managing User access to IT systems starting from when a User is initially registered through to the revocation of access rights and removal of their User account.

User and Information Access management

Access control is primarily about enforcing three information security principles:

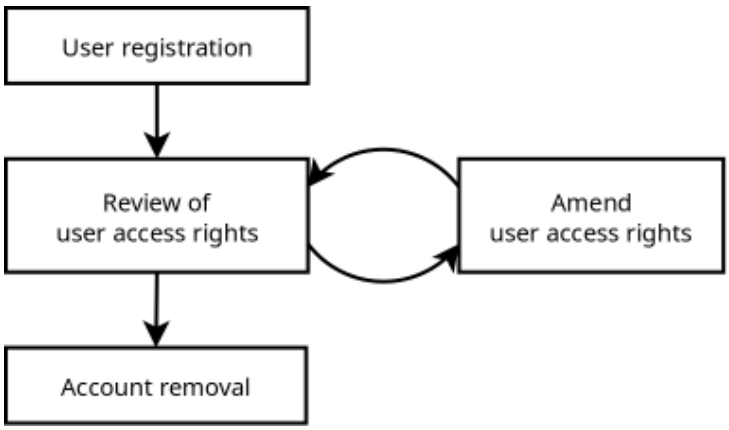
- The *'need-to-know'* principle – restricting access to information based on a business requirement.
- *Non-repudiation* of User actions –holding a User accountable for their actions on an IT system.
- The *'least privilege'* principle – assigning the least number of privileges required to fulfil their work.

At a high level, access control in is based on Role Based Access Control (RBAC). Each user is assigned a role (or set of roles) and access to a piece of information is granted on a per role basis. In general, information will either be subject to RBAC or classified as open access (for example, a HR policy document made available on the intranet).

Information made available on an open access basis (i.e. not subject to any RBAC restrictions) must be treated as an exception to general access control rules. It is important to ensure any information made available in this way has been validated by the Information Asset Owner (IAO) to ensure that the information does not have 'need-to-know' constraints that impede it's sharing beyond a defined RBAC group (refer herefor further details on the role of the IAO).

Management of User access control

The following diagram depicts the 4 stage management lifecycle for managing user access control.



The rest of this section describes each of the 4 stages and outlines what activities are required.

Note: This lifecycle aligns with the HR processes for new joiners (see: https://intranet.justice.gov.uk/guidance/hr/induction/) and leavers (see: https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/).

User registration and account creation

The following activities must be undertaken for each new User registration:

- The identity of the new User must be confirmed – for an member of staff this is confirmed by HR;
- The access rights required must be supplied (for example, the list of RBAC groups and/or applications);
- Confirmation of clearance level (refer here for further details);
- The application for User registration must be authorised by a senior manager.

Note: This authorisation is used as confirmation of the Users identity and the access rights requested are correct.

In general, individuals who are staff (including contractors and agency staff) will be provisioned with a User account and a number of roles applicable to the nature of their work so that they can access the relevant IT systems, application and information. Temporary use of a IT system may be permitted where a specific business need exists (e.g. to allow an external trainer to train staff in a new application) subject to clearance checks and a Non-Disclosure Agreement (NDA). A senior manager must assume total responsibility for the actions undertaken by that temporary User while they are using a IT system using a temporary account.

Minimum user clearance requirements

Most IT systems operate at IL3 where information with a protective marking of REST* can be processed. As these systems process HMG protectively marked data, Users must attain a certain clearance level before they can be granted access rights, the exact level depends on the type of access rights required and job role.

For the purposes of this standard, access rights have been broken down into three User account types. Table 1 provide a description for each type and the minimum clearance required.

Table 1: User account type and clearance required

User account type	Description	Minimum Clearance Required
Normal User	Include all Users with entry-level access; includes read/write and read-only Users.	BPSS
Application Administrator / Privileged User	Typically an application system manager, i.e. those with the rights to create/remove user accounts, and provide internal support.	BPSS

User account type	Description	Minimum Clearance Required
Systems Administrator	A systems administrator does not necessarily have a 'need-to-know' over any of the business information held on the systems they support however they do have administrative privileges which allows them to view data held on those systems and change their configuration.	SC

Note: The clearance level indicated in Table 1 is separate to the clearance level required for a particular job role and sets the minimum requirement for access to a IT system. Most job roles at the require an individual to attain BPSS however; some job roles require an individual to have a higher clearance such as SC or DV.

Privilege management and review of user access rights

In order to ensure that privileges are assigned on a least privileges basis, the following information must be supplied when requesting a new User account or additional privileges:

- A statement of the access required, for example, a path to a folder or functionality within an application;
- The name/identity of the User requiring access and their associated User account identify (where the request relates to an existing User account);
- Business justification; and
- Approval from a senior manager.

Review of user access rights

Access rights must be reviewed on a regular basis and may need to be updated as a result of any change in job role, security clearance, or employment status. The review schedule is captured in Table 2.

The following sub-sections outline the key roles involved in the review process and highlights further consideration which should be undertaken when granting privileges for access to knowledge repositories or remote access connectivity.

IT System owner / Information Asset Owner responsibilities

An IT System Owner or Information Asset Owner (IAO) is responsible for managing access control rules for their particular system.

The actual review and implementation of any access control changes may be performed by service management along with the relevant IT service provider on their behalf however they may be required to verify access rights in order to assist a scheduled review audit of User accounts and permissions.

IT service provider responsibilities

IT service providers operate as access control custodians (as they retain top-level administration rights) acting on the direction of an IT system manager, IAO's and senior managers.

The IT service provider will only amend access rights based on either an automatic joiners / leavers notification or from requests made from an authorised individual (as described at the start of this section). In performing these activities on behalf of the , the IT service provider has the responsibility to:

- Retain a record of all authorised users (granted accounts);
- Retain a record of all access approvals and changes.
- Retain a record of all users granted administrative privileges on any network, system, or application under their administration.

Granting system administrator privileges

Systems administrators by their very nature have privileged access to IT systems, it is important that the use of system administrative accounts is kept to a minimum, as such:

- Systems administrators must be provisioned with two system accounts, one operates as a normal user, the other as a systems administrator.
- A systems administrator must ensure that they use their normal account as their main working account and only use the elevated privileges of their systems administrator account when required.
- Further details can be found in IT Security SyOPs - System Administrators.

Non-IT service provider Users are not normally permitted to hold system administrative privileges. Exceptions may be granted where there is a legitimate business justification endorsed by a senior manager or Senior Civil Servant (SCS). Further advice must be sort from the ITSO.

Access to knowledge repositories

Knowledge repositories such as TRIM, are intended to host generally accessible information (but still internal to the), however certain categories of personnel may not be entitled to access these repositories (or subsets of information held within them) if they are deemed to contain any information that has a specific or implied access control restriction (e.g. based on clearance level or job role).

The relevant IAO is required to ensure that all information is suitable for sharing without access controls or alternatively shall restrict access to authorised personnel with an appropriate need-to-know.

Remote access

Remote access to a IT system requires the use of an authentication token (such as an RSA token) in addition to the standard network logon. Each token is unique to a particular individual and must only be issued to those Users who have a business need to access IT systems remotely, for example, home workers.

Account removal

An individual's User account and any associated access rights must be removed once that individual has either left the organisation or no longer requires access to the IT system (or application) that the account was created for.

It is the responsibility of the line manager to request account removal. The leavers process can be found on the HR intranet page (see: https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/). As part of the HR process, the line manager must inform all relevant IT service providers when a member of staff leaves the organisation and as such instruct them to deactivate and remove their user account. The leavers guidance linked previously gives detail on how to contact IT service providers.

Review of User privileges and accounts schedule

Table 2 outlines the review schedule which must be applied to all IT systems. All User privileges and accounts must be audited in accordance with this schedule, Table 2 states the review activity required with an associated frequency.

Note: It is anticipated that most IT system will be able to comply with this schedule, however it is recognised that this may not be feasible on some. Any deviation from this schedule must be approved by the system Accreditor and ITSO (for example a copy of Table 2 with revised schedule can be placed within the relevant system RMADS).

Table 2: Review of User privileges and accounts schedule

Activity	Description	Schedule
Review existing user accounts	Review all the user (and system user) accounts and identify accounts which have not been used in the last 3 months.The list of identified accounts must be reviewed with HR to identify which accounts can be removed (as the User has left the) or require deactivation (as the User is on long term leave).	Every 3 months

Activity	Description	Schedule
Review of user access / authentication tokens	Review the usages of remote access authentication tokens (e.g. RSA token) and identify accounts where a token has not been used in the last 3 months. These token must be disabled.	Every 3 months
Review of user account privileges	Review the roles and privileges assigned to a User and remove any which are no longer required.	Every 6-12 months (exact review period to be agreed with the system Accreditor and ITSO)

User access management

Authentication

The base principle

Any access to any data **must** employ adequate authentication techniques to identify the system or user to a suitable level of confidence for the system or data within.

Passwords

Where appropriate, passwords should be used as a knowledge-based factor for authentication.

The has published password guidance.

Named individual accounts

Human user access must have unique, named and private accounts issued (with shared accounts being a rare, intentional and considered exception to this rule).

For example: Jonathan Bloggs is issued with a user account only Jonathan uses and may access.

Account sharing

Accounts must not be shared unless they are defined as shared accounts, where additional authentication and authorisation techniques may be required.

For example:

- individuals must not share a 'root' account, but be issued named accounts with appropriate privileges instead;
- Individuals must not share a single Secure Shell (SSH) private key, but generate private and individual key pairs and their public key associated to locations where authentication is required.

System-system accounts

Accounts designed for programmatic or system/service integration must be unique for each purpose, particularly in separation between different environments - such as pre-production and production.

System-system accounts must be protected against human intervention.

Token-based methods are preferred over static private key methods.

Multi-Factor Authentication

Where appropriate, multi-factor authentication (MFA) should be used as a knowledge-based factor for authentication. MFA is sometimes referred to as Two-Factor Authentication (2FA).

guidance on MFA is available here.

MFA for Administrators

Administrative accounts **must** always have MFA, unless impractical to do so. Ensure there are techniques in-place such that MFA is always enabled and active for each account.

MFA for important or privileged actions

MFA should be re-requested from the user for important or privileged actions such as changing fundamental configurations such as registered email address or adding another administrator.

MFA can also be used as a validation step, to ensure the user understands and is confirming the action they have requested, such as an MFA re-prompt when attempting to delete data.

IP addresses
Trusting IP addresses

IP addresses in and of themselves do not constitute authentication but may be considered a minor authentication *indicator* when combined with other authentication and authorisation techniques.

For example, traffic originating from a perceived known IP address/range does not automatically mean it is the perceived user(s) however it could be used as an indicator to *reduce* (not eliminate) how often MFA is requested *within* an existing session.

IP address for non-production systems

IP addresses access control lists (and/or techniques such as HTTP basic authentication) should be used to restrict access to non-production systems you do not wish general users to access.

H/T https://medium.com/@joelgsamuel/ip-address-access-control-lists-are-not-as-great-as-you-think-they-are-4176b7d68f20

Management access

The base principle

Management or administrative access **must** be limited to authorised authenticated users and utilise multi-factor authentication wherever possible.

Application Program Interface (API)

APIs are preferred over Secure Shell (SSH) connections, as by comparison they generally offer greater technical security limitations without the need for parsing commands.

Automated diagnostic data collection

It should be exceptional to directly administer a server/node when adequate diagnostic data collection sends underlying technical data to a place where it can be correlated and analysed.

Pre-defined, pre-audited

Tools such as Systems Manager and comparable techniques over preferred over manual intervention (such as human interaction over SSH) as the intervention path can be carefully designed to avoid human error and effectively instruct pre-audited actions to be taken on an administrator's behalf.

Secure Shell (SSH)

Use of bastion or 'jump' boxes for access into systems is a useful technical security design that also helps 'choke' and control such sessions.

Through immutable infrastructure and server design, state-less cluster expansion/contraction and automated diagnostic data capture the need to SSH into a server/node should be increasingly less common.

It should be exceptional for an individual to login to a server/node via SSH and execute commands with elevated privileges (typically, `root`).

Using SSH

SSH must be strictly controlled, and environments should be segregated so that no single bastion or 'jump' SSH server can access both production and non-production accounts.

SSH shells must be limited to users who need shell (by comparison to users who will use SSH as a port forwarding tunnel).

Joiners/Movers/Leavers processes must be strictly enforced (optimally, automated) on SSH servers as they are a critical and privileged access method.

SSH should not be password-based, and should use individually created and purposed SSH keypairs. *Private keys must not be shared or re-used*.

Managing User Access Guide

Related information

Access Control guide on page 87

Introduction

This guide provides information on the authentication methods which should be used to manage user access to systems and information in the . This is a sub-page to the Access Control Guide.

Managing access to systems

The following methods can be used to manage access to the 's systems. They are in order of preference for their use, with 1 providing more secure management features than 3.

Rank	Method	Comment
1	Application Program Interface (API)	Where possible, APIs should be used instead of remote server configuration tools such as Secure Shell (SSH) and Remote Desktop (RDP). This is because APIs offer greater technical control over security systems without the need for parsing commands required by remote server configuration tools.
2	Automated diagnostic data collection	It should be considered the exception for administrators to directly administer a server/node when there is automated diagnostic data collection. Diagnostic data collection allows the underlying technical data to be easily correlated and analysed.
3	Remote server configuration tools	If you cannot use APIs then remote server configuration tools can be used with the following controls.

Use of bastion or 'jump' boxes for access into systems is a useful technical security design that also helps 'choke' and control sessions.

The need to use remote server configuration tools to interact with a server or node can be reduced through improved infrastructure and server design. For instance, the use of stateless cluster expansion or contraction, and the automated diagnostic data capture, can reduce the need to use SSH.

System Admins should only login to a server or node via SSH to execute commands with elevated privileges (typically, root) under exceptional circumstances.

- SSH must be strictly controlled, and environments should be segregated so that no single bastion or 'jump' SSH server can access both production and non-production accounts.
- Do not allow direct logging in as root through SSH. Administrators must have a separate account that they regularly use and `sudo` to root when necessary.
- SSHs must be limited to users who need shell, in contrast to users who might use SSH as a port forwarding tunnel.
- Joiners/Movers/Leavers processes must be strictly enforced (optimally and preferably automated) on SSH servers, as they are a critical and privileged access method.
- SSH access should not be password-based. It should use individually created and purposed SSH key pairs. Private keys must not be shared or re-used.

The Government Digital Service (GDS) recommends the use of the open authorisation standard 'OAuth2' as a means to authenticate users. Refer to the GDS guide for more information.

Multi-Factor Authentication (MFA) Guide

Related information

Access Control guide on page 87

Introduction

This Multi-Factor Authentication (MFA) guide explains how MFA is used to ensure that users are only granted access to information once their identity is confirmed. This is a sub-page to the Access Control Guide.

MFA

Users have their identity authenticated through one or more of the following methods:

- Something they know, such as a password.
- Something they have, such as a mobile phone or smart card.
- Something they are, using biometric authentication such as a fingerprint.

MFA can be used as a possession-based factor for authentication, by checking for something 'you have'. MFA is sometimes referred to as Two-Factor Authentication (2FA) if it involves a second form of authentication. MFA is referred to as 3, 4, or 5 Factor Authentication if it includes additional authentication requirements. Different methods of additional authentication identify users with varying degrees of accuracy. Care be taken to ensure true MFA. For example, password and security questions are both dependent on 'something the user knows' and therefore are just one factor of authentication.

The following list identifies the 's preference for MFA methods, with 1 ranked the highest, and 8 the least desirable. These methods can be used for 2, 3, 4, or 5 Factor Authentication as required.

Note:

- MFA Type 1 might not be suitable for all systems. In that case, other methods of delivering MFA be considered to enable additional protection beyond single sign on.
- MFA types 5 and 8 only be used when no other MFA method is appropriate. The reason is that these methods are more easily spoofed or circumvented.

Preference	Type
1.	Hardware-based. For example, a Yubikey or similar TPM enabled device is presented during the authentication process.
2.	Software-based. For example, a Google Prompt is presented on a registered mobile device.
3.	Time-based One Time Password (TOTP)-based. The code is held by a dedicated app, such as Google Authenticator, on a mobile device.
4.	TOTP-based. The code is held within a multi-purpose app, for example a password manager app that also holds other authentication information.

Preference	Type
5.	Certificate-based. A digital certificate is used to authenticate a user.
6.	Email-based. A one-time code or link is sent to the user's registered on-file email address.
7.	SMS-based. A one-time code is sent to the user through an SMS message.
8.	Phone-call based. An automated phone call is made to the user's registered on-file phone number, to provide a one-time code or password.

Note: When sending a one-time code to a mobile device, for example an SMS or phone call, the connection only be to a single user account. In other words, only telephone numbers allocated to a single individual be used. Sending a one-time code to a shared device or shared number is not permitted.

The Password Guide provides more information on the use of MFA.

Privileged User Guide

Introduction

This guide outlines the security procedures and advice that privileged users should follow when accessing the IT systems in a safe and secure manner. Privileged users are those who have elevated levels of system access in order to manage IT system components to meet IT service requirements. Privileged users might, for example, install software, configure and upgrade IT systems, input into the Service Management Tool for the systems they manage, and run day-to-day operations to satisfy continuity of service, recovery, security, and performance needs. This includes privileged users who manage Slack or Github repositories, users who have administrative access on their laptops, and users who setup and maintain platforms hosted in the Cloud.

Specific responsibilities of individual privileged users are likely to vary depending on the systems they manage. The system's Information Risk Assessment Report documents the security controls (Information Assurance Framework Process). The IRAR should be completed as part of this process. For a comprehensive list of individual responsibilities, privileged users should refer to the system specific documentation.

This page is the first in a series of guides for privileged users within the ; refer also to the related guides.

Who is this for?

This guide is aimed at two audiences, both technical.

- The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
- Any other business groups, Agencies, contractors, IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of, the .

Related guides

For further details about privileged user responsibilities, refer to the following guides.

- The Privileged Account Management Guide provides the guidelines to ensure that privileged accounts are securely managed. It is part of the Access Control Guide.
- The Logging and Protective Monitoring Guide provides information about security procedures privileged users should implement to conduct logging activities.
- The Backups, Removable Media and Incident Management Guide provides information that privileged users should follow to reduce the impact of a security incident, and understand how they should respond.
- The Configuration, Patching and Change Management Guide provides privileged users with guidance to ensure that systems are configured securely, that change is managed correctly, and that systems are patched regularly.

Management of privileged user accounts

Privileged user accounts have a high degree of risk associated with them due to the control that they give the privileged user, hence they must be treated with great care. To reduce the risk of a data breach on the systems, access rights must be managed in the following ways.

- Privileged user accounts should only be created for users with a genuine business need, and only for the duration that the business need exists.
- Privileged access must be limited and granted in line with the principle of least privilege necessary to fulfil the required function.
- The privileged accounts should be strictly controlled, and their number kept to the absolute minimum per system or app.
- Privileged user passwords must be created in line with the 's Password Guide.
- The password for a privileged user account must not be re-used for another privileged user account or a normal user account.
- Privileged user passwords must be deleted along with the account when a privileged user leaves the or changes role.
- Multi Factor Authentication (MFA) must be used for privileged user accounts where possible. Refer to the Password Guide for further details.
- Privileged user accounts must only be used when carrying out administrative tasks such as creating new user accounts or implementing software updates. At all other times a normal user account must be used, e.g. for tasks such as searching the internet and reading emails.
- Privileged user accounts on depreciated systems must be reviewed quarterly by system owners for breach as aging systems frequently cannot be, or are not, patched leaving them vulnerable to take over.
- Privileged users must not abuse the privileges they are given, such as circumventing controls put in place to protect the .

For further information on managing privileged user accounts refer to the Privileged User Configuration, Patching and Change Management Guide.

Resource monitoring

Privileged users are responsible for monitoring their systems to ensure that the system is operating effectively and providing the intended functionality. Privileged users should:

- Define each system's Key Performance Indicators (KPIs), which can be used to ensure the systems are operating effectively.
- Monitor and analyse data from the systems in order to observe malicious behaviour, and to minimise, or to prevent, system outages or slowdowns, examples being:
  - For managed infrastructure:
    - CPU usage.
    - Disk usage.
    - Memory consumption.
  - For Cloud solutions:
    - Access requests.
    - Database monitoring.
    - Monitoring storage resources and processes that are provisioned to virtual machines, services, databases, and applications.
    - Virtual network monitoring.
- Identify the root cause of excessive resource use and rectifying the issue when possible. If an issue cannot be rectified quickly, it should be reported to the system owner.
- Notify the if there is a suspected incident (refer to the contact details).

Identification and authentication

Privileged users are responsible for managing user access to systems to enable effective access control to the 's data and information. To support effective access controls, privileged users must:

- Only create user accounts once authorisation has been received from that user's line manager.
- Only grant permissions that are in line with the user's business role within the .
- Review user account usage every 90 days. If an account is dormant, the privileged user must investigate its status and suspend the account if appropriate. Refer to the Access Control Guide for details.
- Disable all user and privileged user accounts when staff members leave the , or where the account is not required due to a change of role. Privileged users will be automatically notified by HR when access changes or revocations are required.
- Retain a record of all authorised users, approvals, and changes of access rights and privileges for any network, system or application, for which privileged users are responsible.

Mobile and home working

When working remotely, it is important that privileged users operate securely by:

- Ensuring that they are not overlooked when working on administrative tasks.
- Ensuring that they use the 's Virtual private Network (VPN) to connect with systems when using Privileged user login details.
- Using only issued equipment to connect to the estate, and to carry out business.

Access to the VPN requires 2 Factor Authentication (2FA). The IT Security Policy and Remote Working guidance documents contain further information about Remote Working.

Privileged User Backups, Removable Media and Incident Management Guide Introduction

This guide outlines the security procedures and advice for privileged users to reduce the impact of security incidents, and improve the response to them. This guide is a sub-page to the Privileged User Guide.

Removable media

Whether moving data to the Cloud or accepting data from third parties, removable media increases the risk of malware being introduced to systems, and could result in the loss of critical or sensitive data. Privileged users play an important role in managing this risk, and must ensure that the following actions are undertaken by individuals using removable media.

- Any data transferred from removable media to the systems should be scanned for malware before being uploaded to systems. One option is to adopt a "sheep dip". This is a segregated system with anti-virus and other security tools. It is used to conduct security scans before data is introduced to the systems. This reduces, but does not eliminate, the risk that removable media is used as a threat vector for malware.
- The origin of any removable media must be established to understand the risk it poses.
- If removable media is required for standard system operations, privileged users must ensure data is encrypted at rest, and has suitable physical security controls in place. These include locking rooms where data is stored or using safes for storing removable media.
- Removable media must not be used for a system's operation unless it is approved by the Senior Information Risk Officer (SIRO). Advice should be sought from a risk advisor in the Cyber Assistance Team, using the contact details.

System backups

Privileged users need to ensure that there are backups of system data in order to minimise the impact of incidents, such as malware infection or data loss. Privileged users must:

- Follow the IT system's data backup schedule to meet the required Recovery Point Objective.
- Assign all backup media, whether physical or in the Cloud, a Protective Marking, and provide appropriate protection based on that marking. Backup material must only be accessible to those who have a "need-to-know", defined by the System Owner.

- Ensure backups are kept off-site in a secure location. In a Cloud environment, this would equate to a resilient data store, such as AWS Backup or Azure Backup services.
- Where required, encryption types employed to prevent disclosure are outlined in the Information Risk Assessment Report (IRAR). Details of applicable encryption standards required are outlined in the Technical Controls Guide.

Guidance for system specific privileged users:

- Where responsible for DOM1 systems, ensure backups are made to offsite locations such as to Dell EMC SANs in the off-site Ark and Ark-F data centres.
- Where responsible for Quantum systems, ensure backups are made to the redundant data centre.
- Where responsible for end user data, ensure data is not stored on or backed up to users' end devices but rather stored on OneDrive or Google Drive.

Incident management and response

Privileged users play a front-line role in detecting and responding to incidents. To ensure that they are prepared to respond to any incidents, privileged users should:

- Know and be able to implement the incident management plans and processes required for their systems. For instance, within HMPPS, privileged users should know that the HMPPS Incident Management function operates within the HMPPS Infosec and Service Team, and when they are to be contacted.
- Ensure that any system-specific incident management controls align with the 's IT Disaster Recovery Policy and the IT Security Incident Management Policy.

Privileged User Configuration, Patching and Change Management Guide

Introduction

This guide outlines the security procedures and controls privileged users should look to implement in order to ensure that systems are configured securely, change is managed correctly. and systems are regularly patched. The goal is to provide guidance for both physical environments, such as Dom1 and Quantum, as well as the Cloud estates in AWS, Azure and Google Cloud. This guide is a sub-page to the Privileged User Guide.

Secure configuration and change management

Privileged users must ensure that secure configuration and change management processes are followed so that any changes to system operating procedures are understood and support the 's risk management and mitigation activities. Privileged users must implement the following controls.

- Approve and test all changes to IT Systems, in a non-live environment, before they are implemented on the live system.
- For digital products developed by the 's in-house teams, development and hence testing should be conducted iteratively, and changes captured.
- Maintain an audit log of configuration changes, and ensure that changes do not affect the secure operation of the IT system.
- If you are working on an in-house developed product or service, configuration changes along with the approval workflow must be recorded in a Service Management Tool, which for many teams is Jira or Trello.
- If you are working on a system provided by a Managed Service Provider (MSP), changes must be input into the Configuration Management Database (CMDB). In some cases, these CMDBs will be held by the MSP, but with access rights to the , or they can be provided through ServiceNow.
- If you are working on a system provided by an MSP, do not implement changes that deviate from the standard build unless the corresponding Operational Change Request (OCR) has been approved by each approver in the Change Management workflow. Once all approvals are complete, the change can be implemented. Further information can be found in the Vulnerability Scanning and Patch Management Guide.
- Report any changes that affect the security posture or risk profile of a system to the Cyber Assistance Team, and specifically to the business area Risk Advisor before they are implemented.
- Ensure that operating systems are fully supported by the relevant platform vendor or an service team. If the system is not supported, consult with the system owner and the Cyber Assistance Team for advice. A lack of ongoing support might create security risks within the system and the wider networks.

- Privileged users must have the correct management authorisation to make changes to operational software, applications, and program libraries.
- Documentary evidence must be maintained to catalogue all changes (including configuration changes) to IT systems, and the IT security implications of those changes. This includes the case where no significant IT security impacts are identified.

Privileged User Logging and Protective Monitoring Guide

Related information

Logging and monitoring on page 192

Introduction

This guide outlines the security procedures and advice that privileged users must consider when undertaking logging activities. Maintaining and monitoring system logs will help to ensure that any suspicious activity on the 's systems is detected early. This guide is a sub-page to the Privileged User Guide.

Maintenance of system logs and protective monitoring

Privileged users are responsible for maintaining system logs (syslogs) for the systems they administer. Privileged user log management responsibilities include the following:

- Implementing logging and monitoring on the systems they manage.
- Performing regular maintenance of the logs and logging to ensure that configurations are correct.
- Reconfiguring system logging as needed based on the 's policy or guidance changes, technology changes, emerging threats or other business needs.
- Implementing automated real-time log analysis where possible.
- Reviewing results from automated real-time analysis quarterly to ensure its relevance.
- Where real-time log analysis has not been implemented, then manual log analysis must be performed at least weekly.
- Working closely with the Security Team to define requirements and ensure that when possible, automated log analysis and alerting is integrated with the 's Security Operations Centre (SOC) which provides the 's central monitoring function.
- Establishing the baseline activities for systems they are responsible for. This is essential to ensure that monitoring systems are able to detect when there is unusual activity.
- Ensuring that systems are synchronised to the centralised timing source, to enable effective malware detection.
- Ensuring that audits and compliance checks of IT systems do not adversely affect business operations.
- Documenting and reporting anomalies in log settings, configurations, and processes to the Security team (contact details).
- Managing long-term storage of system log data, monitoring log rotation, and the archival and deletion of log data.
- Any suspicious activity must be reported. Refer to the details in the IT Security Incident Management Policy.

Protection of log data

To ensure that there is an audit trail for log data, privileged users must:

- Protect the information held within system audit logs in accordance with its Information Classification. Refer to the Information Classification Handling and Security Guide for further guidance on classifying information.
- Establish log archival processes while filtering out entries that do not need to be archived to ensure log availability.
- Ensure that systems are designed with access controls, to prevent privileged users from erasing or deactivating activity logs of their own activities, without the additional approval of the product or service manager.
- Review the activity logs of other privileged users on a monthly basis, to ensure that privileged users remain impartial.

User responsibilities

Protecting social media accounts

Hostile attacks on Social Media accounts pose a serious threat to the and its reputation. When attacks happen, they quickly become headline news, and can happen to any account, anywhere in the world.

Two types of attacks are common:

- Attempts to render the account useless by 'bombarding' it with messages.
- Attempts to 'take over' the account.

Steps we can all take to protect ourselves

Ensure our passwords are secure

Passwords are the main protection on our accounts, hence ensuring they are secure is vital. The NCSC has produced guidance on making secure passwords - the summary of which is that picking three random words to make a password (for example `RainingWalrusTeacup`) is a good policy for securing Social Media accounts.

Check your email details are up-to-date

Most of the time, the first indication you'll have that something is wrong is when an email is sent to you. This could be to let you know that someone is attempting to log into your account, or that someone is trying to reset your password, or more worryingly, that a new device has logged into your account. Hence it is important that you ensure that your email details are up-to-date, and that your email is secure.

Enable Two Factor Authentication

Two Factor Authentication (2FA) involves requiring a random code to be entered before being logged in. These codes are either sent to the user via SMS or email, or generated every 30 seconds by an app or device the user has which relies on a seed key provided by the service. That seed can then be shared amongst a team, allowing for multiple owners or contributors.

If at all possible, SMS generation should be avoided, as it is theoretically possible for phone numbers to be taken over through various attacks, as well as meaning that only one person can receive the code, which isn't ideal if a team is working on a single account.

If you're using email, then it can be sent to a group account, which also allows for multiple owners or contributors - but it's important to ensure that the email is also protected by 2FA.

If you have a spare 10 minutes, watch this video for an excellent explanation of how 2FA works and why it's important to have it enabled.

Click the links for details on how to activate 2FA for Facebook, Twitter and Instagram.

Only use trusted third-party applications

In addition to the official applications, there are many tools and third-party applications that might be used to work with social media accounts.

Some of these tools provide useful extra facilities, such as 'scheduled' posts, or helping you post one message to several different social media channels.

The problem is that you have to give your account details to these tools so that they can post to your account.

This is potentially very dangerous:

- An application might post messages on your behalf, that you do not agree with or are unacceptable.
- An application might store or share your account details.

Only use applications that are trusted and approved for use with your social media accounts. For help with this, contact Cyber Security.

Remove 'unused' applications

People tend not to be very good at removing old or rarely used applications. Older applications should be checked regularly to find out if there are any updates.

A good habit is to check your applications once a month or so, and consider:

- Do you still use the application? If not, remove it.
- Whether there is an update available for the application? If so, install it.

As well as increasing safety, removing unused applications frees up storage space on your system.

Check your privacy settings

The whole point of a social media account is to share information. But that doesn't mean you want to share *everything*.

When you first create a social media account, you are normally asked to decide on the privacy settings. These control how much information you share, and who you share it with.

Typical settings that affect privacy include:

- General information about you.
- Your Profile information and photo.
- When you were last active.
- Any status updates.
- Whether you have read direct messages ("Read Receipts").
- Whether others can add you to their groups, possibly without your knowledge or agreement.

But it's very easy to forget to check the settings, from time-to-time, to make sure they are still correct.

A good habit is to check your account privacy settings once a month or so. Information on privacy settings is available for the main social media environments:

- Facebook
- Instagram
- Twitter
- WhatsApp

For example, in WhatsApp, to prevent someone adding you a group without your knowledge, change your settings: **Settings** > **Account** > **Privacy** > **Groups** > **My Contacts**. This change means that only people you know (your contacts) can add you to a group.

Limit access to your accounts

You might be tempted to share access to your social media account, for example if you want to have postings regularly, even while you are away.

Avoid sharing access to your social media account. It's easy to forget who the details are shared with. It's also possible that postings might be made on your behalf that you don't agree with, or are not acceptable.

Any social media accounts that do need to be shared will have proper access controls in place. You should never need to share your account details for work purposes.

If you need more help on this, contact your Line Manager or Cyber Security.

Don't click on suspicious links

Unfortunately, social media postings are a common way of sending you links to malware or other problem material. Postings might also be used to send you 'phishing' attacks.

In the same way that you should be careful with any links or attachments sent to you using email, you should also be suspicious of links or attachments sent to you though social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

For more information, read this article on the Intranet.

What to do if your account is bombarded
Remember that these attacks are short lived

Due to the amount of organisation and effort required to coordinate such an attack, they do not last long, and like an intense inferno, will soon burn themselves out.

Do not respond to the attack

These attacks are designed to attack the person controlling the account as well as the agency itself. By only responding to messages not involved in the attack - especially those trying to share positive messages, the attackers will run out of interest far sooner than if you engage them. If they are posting harmful or threatening messages, report the accounts.

In a single sentence - "don't feed the trolls".

Feel free to walk away

Dealing with these attacks can be emotionally draining; even just reading the messages can have a far greater impact on you than you realise. Take breaks in the event of an attack, even if it's hard to - consider going for a walk to force yourself away.

System and application access control

Account management

Introduction

This guide provides help on account management, for example when passwords should be changed or when user accounts should be locked. For more information, refer to the Password Management Guide.

The information is aimed at two audiences:

- The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPIC) team.
- Any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the .

Account lockouts

Account lockouts must be implemented within systems for the following reasons:

Failure to change passwords within the allocated time.	Systems must have a "change password" function to recover the account or contact information for the .
Unsuccessful connection attempts.	Allow no more than 10 consecutive login attempts before lockout.
Forgotten passwords.	All systems must have a forgotten password link on the login page, enabling the user to change the password on their own. Ensure this uses multi-factor authentication for user verification.
Removed or revoked access.	Users may experience account lockouts due to inactivity, need to know permissions or change of employment status such as contract termination. Access to these accounts must only be re-enabled with line manager approval.

Systems should have a way to forcibly revoke an account, and disconnect any active session instantly. This is to deal with scenarios such as suspicion that an account or access has been compromised. The session disconnect is required because revoking an account on some systems does not necessarily invalidate an existing session immediately.

Password changes

When designing and developing systems for use within the , password changes must be enforced for these events:

- A user has forgotten their password or is experiencing login issues.
- There has been a security incident involving the account or password.
- An authorised person, such as line manager or IT support, requests the change.
- The system prompts you to change a password.
- You suspect an account might have been compromised.

Password changes must be made within the following time frames:

Type of system	Maximum time allowed for a change
Single-user systems, such as laptops	1 week
All other systems	1 day

Revoking accounts

All user accounts are access controlled according to the user's 'need to know' requirements and their employment status. Accounts should be revoked at contract termination and during long-term absences, such as maternity or long-term sickness leave. The revokes user accounts in alignment with the Access Control Guide.

Authorisation

The base principle

Any access to any data **must** employ adequate authentication techniques to identify the system or user to a suitable level of confidence for the system or data within.

Least privilege principle

The principle of least privilege (also known as the principle of least authority) is effectively conferring only the minimum number of required privileges required in order to perform the required tasks.

This helps reduce the "attack surface" of the computer by eliminating unnecessary privileges.

Day to day examples include: not ordinarily using an 'administrator' login on an end-user device (such as a laptop), logging into a server as 'root' or a user being able to access all records within a database when they only need to access a subset for their work.

Administrator definition

An administrator is much broader than a technical system administrator to a server, network or service (such as 'domain admin' in Microsoft Active Directory) but someone has who has higher levels of access or control than a required for day to day operation.

Examples include those with high privileges on a GitHub repository and credentials to the communications accounts (such as social media).

AWS assume-role

Amazon Web Services (AWS) Identity and Access Management (IAM) has a `Role` function, which effectively allows explicitly permitted and explicitly denied activity (within the AWS ecosystem) to be defined on a per role-based.

This allows IAM accounts to be grouped based on role and purpose. This avoids individual IAM accounts being given permissions individually, which can often lead to over or under privilege configurations.

Where possible, IAM Roles should be used.

Maintain IP address lists

Where applicable, maintain a single source of truth with meaningful labels to describe each IP address range.

The use of infrastructure as code to both store and apply IP address lists helps reduce errors, and aids with change management.

Where practical, periodically check the IP addresses with the team responsible for those IP addresses, to cater for upcoming changes in IP spacing or change of use or scope.

Implement defensive depth

When you depend less on IP addresses as a filtration method, other activities become more important. These include:

- Monitor accesses and activity.
- Log accesses and activity.
- Perform actual authentication, using techniques such as:
  - Use of client certificates.
  - 'Magic' links.
  - Usernames and passwords.
  - Single or same sign-on.
  - Multi-factor authentication (MFA).
- Including defences against denial-of-service attacks, brute force attempts, and credential stuffing.

External IP addresses

External IP address access control lists are useful as part of a wider set of controls.

Introducing external IP address access control lists (ACLs) can filter out tertiary noise. Ensure that your use cases are rigorous, and that other defensive and authentication, authorisation, and accounting (AAA) measures are in place. This helps ensure protection from random port scans or brute force attempts.

Two real-life examples are:

- Reducing MFA prompts. Do this by ensuring that corporate and staff wifi is appropriately access controlled. This includes having a clear egress range of IP addresses. It is important also to analyse and use the proximity probability of individuals and devices.
- Make connection sessions longer. This is where you allow sessions and tokens to last for a longer period, such as 30 days instead of 7. These longer sessions are enabled only they take place from predictable and 'known' locations.

This Medium article provides more details regarding IP address access control lists.

Multi-user accounts and Public-Facing Service Accounts Guide

Introduction

This guide sets out when multi-user accounts should be used, although this is discouraged and should be avoided if possible. The guide also explains how public-facing service accounts should be authenticated. For more information, refer to the Password Management Guide.

This guide has been written in alignment with NCSC guidance.

Multi-user accounts

In this context, a multi-user account is where a single set of credentials is used by more than one person. This can be found on legacy systems where there is a dedicated administrator account. Multi-user accounts allow multiple users with individual logins and varying permissions to use the same account. Multi-user accounts need to be managed carefully using Privileged Account Management (PAM) or a Bastion server to avoid security risks associated with accountability. Multi-user accounts should only be used directly if there is no alternative.

Note: A Bastion server is a specially strengthened system that provides access to parts of the private network from an external network, such as the Internet. It provide specific access to to a well-defined set of servers or services, rather than permitting general access across the network.

The multi-user account checklist requires that you:

- Undertake a Business Impact Assessment (BIA) before implementation of a multi-user account to understand risks posed to the .

  Note: The BIA provides details on how the business views the impact to their information assets and services following a loss of Confidentiality, Integrity or Availability. This is useful because it provides a steer on what types of incidents result in the highest impact to the business and how tolerant the business is to a loss of service provision. For help on creating a BIA, contact the .
- Create a pre-defined and authorised list of users.
- Implement using the 'need to know' access principle on the PAM. Alternatively, if using a bastion host, find out what options there are to enforce this principle.
- Regularly check for redundant user IDs and accounts on either the PAM or bastion hosts. These should then be blocked or removed.

Public-facing services

Developers and administrators should ensure that front-end users who access the public-facing services or applications are authenticated through the GOV.UK Verify Service. When this is not possible, for example when an individual does not have a UK address, passwords must:

- Be easy to use, for example, pasting passwords into web forms should be enabled.
- Not be forcibly changed simply as a result of a period of time passing. However, passwords and other account access mechanisms must be revoked for an individual when they are no longer authorised to work with the account.
- Use Two Factor Authentication (the Password Creation and Authentication Guide provides further advice).
- Be changed when required, for example after a system compromise is identified, or if the limit of unsuccessful password attempts is reached and the account is locked.
- Be reset using a one-time password.

The Password Creation and Authentication Guide provides further guidance creating a strong and complex password.

Service accounts

Service accounts must be used for system and application authentication at a privileged level. Service accounts must use certificates for authentication, however if these cannot be used, then passwords are an acceptable alternative. The Password Creation and Authentication Guide provides further guidance on how you must create a strong and complex password.

Password Creation and Authentication Guide

Introduction

This guide sets out considerations for creating passwords and authenticating users for access to systems. This includes ensuring that there are appropriate authentication methods for information, accounts and systems. For more information, refer to the Password Management Guide.

This guide has been written to align with NCSC guidance.

Default passwords

All default passwords must be changed before using any system. Default passwords should not be 'guessable'. This applies to all new, modified or replaced systems, applications and end-user devices or endpoints.

Password length and complexity

Best practice for creating a strong password is to create a passphrase consisting of a string of words that is easy to remember. If using this approach, have a minimum of three words in the passphrase. Passwords must be complex and difficult to guess. When selecting a password, ensure that:

- It has a minimum of 8 characters for personal accounts.
- It has a minimum of 15 characters for high value accounts, for example administrator accounts, password managers or service accounts.
- It does not contain usernames or personal information, such as date of birth, address, phone number or family or pet names.
- It is used alongside system monitoring tools such as last login attempt notifications, rather than enforcing regular password expiry.
- You have alternative or additional authentication options, such as Single-Sign On (SSO) and Multi-Factor Authentication (MFA), depending on a system's security classification or where otherwise required.

Stronger passwords typically contain at least one instance of each of the following character types: upper case, lower case, numbers, and special characters. Special characters include: `@`, `&`, `$`, `%` or `^`. However, there is no specific obligation to include special characters for a password to be acceptable.

For more details about passwords for service accounts, refer to the Passwords guidance.

Password history and block listing

The requires a password allow list to help users create strong passwords. This is a list of commonly used passwords, which can be easily guessed or brute forced by threat actors, and so must not be used. To understand trends in bad passwords and set up password allow listing, refer to 'SecLists', found on GitHub.

The requires password history management, to prevent an old password being reused. This prevents threat actors using previously compromised passwords in an attack, and helps to enforce strong password requirements.

Multi-factor authentication

MFA provides an additional layer of security for login and access controls. Two-Factor Authentication (2FA), Time-based One-Time Password Algorithm (TOTP), and hardware and software tokens and biometric authentication are all forms of MFA that might be used within systems. The Access Control Guide provides further information.

If a service supports MFA, it must be enabled and used by default. An MFA prompt must appear when attempting to access an system, where:

- The system relies upon 'cloud' applications, cloud-based APIs, or other internet-connected services.
- A new device is used to log on to the service.
- A password change is being made for a privileged account.

Further guidance around the use of Multi-Factor Authentication can be found in the Authentication guide.

Single-Sign On

SSO solutions include Office 365, and Digital and Technology G-Suite. SSO solutions must be integrated within the application development and service delivery environment, to improve user experience by authenticating to systems using existing credentials. SSO must:

- Have a pre-defined identity source for users, such as Active Directory, Google Directory or LDAP. This means a developer or service provider must use an established SSO solution rather than creating a new one.
- Normally be based on applications rather than groups of people. This means that SSO is to a specific application or service, rather than saying something like 'all administrators of the Widget application have SSO-managed access'. Instead, SSO must be enabled for the 'Widget' application. It can be based on groups of people or roles if these have been defined.

Password Management Guide

Introduction

This guide sets out the roles and requirements for setting and maintaining strong passwords across systems.

The information is aimed at two audiences:

- The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPIC) team.
- Any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the .

Roles and responsibilities

All Digital and Technology users

Everyone must ensure that password creation, distribution and maintenance is done securely.

Passwords must not ordinarily be shared. Refer to the Password Storage and Management Guide for exceptions and alternative solutions for sharing passwords.

Passwords must be strong and complex. Refer to the Password Creation and Authentication Guide for more details.

Passwords must be changed upon indication of compromise.

Passwords must be distributed securely. Refer to the Password Storage and Management Guide.

Multi-factor authentication (MFA) must be enabled for existing systems, wherever possible. MFA must be enabled for new systems. Further guidance can be found in the Password Creation and Authentication Guide and the Multi-User Accounts and Public-Facing Service Accounts Guide.

Where a default password is applicable, it must never be guessable.

Software Developers, Technical Architects and Development Operations

Make every effort to avoid creating yet another new or modified password-based authentication system. If it is unavoidable, then ensure that the following security requirements are adhered to:

- Multi-user accounts should be avoided, but if required refer to the Multi-User Accounts and Public-Facing Service Accounts Guide for further guidance.
- Technical controls must be implemented to support requirements in the Password Creation and Authentication Guide.
- Applications or software must support MFA, and where possible single sign-on (SSO) solutions used by the .
- Passwords must not be stored in clear text or using encryption algorithms with known security weaknesses.
- Passwords must not be transmitted in clear text over networks.
- All applications or software must use HTTPS to require authentication.
- Applications or software must provide some form of role management, whereby an authorised user can take over the functions of another without having to know the other users' password.
- Passwords and other secrets (SSH Keys, DevOps secrets, etc.) must never be embedded into applications. The use of key vaults, such AWS Secrets Manager, is strongly recommended.
- Where a default password is applicable, it must never be guessable.

Suppliers and vendors

Suppliers and vendors must ensure that their systems support the password requirements set by the .

Supplier or vendor systems must be able to change, reset and revoke passwords. This must be possible using well-defined processes.

Suppliers and vendors must implement the technical controls in the guidance, such as locking accounts after repeated access attempts and blocking common password choices, to improve the effectiveness of password-enforcement and compliance.

Senior Business Owners for Contracts should ensure that when contracts are signed, the supplier receives explicit guidance on password management and it is included in the associated contractual Security Management Plan (SMP).

System Administrators

System Administrators (SAs) must ensure that systems support the password requirements set by the . When provisioning and maintaining user accounts, SAs must:

- Require a change of initial or first-time passwords.
- Verify a user's identity before resetting a password.
- Implement automated notification of a password change or reset.

SAs must also ensure privileged accounts:

- Are authorised only for a specified time.
- Are managed and regularly reviewed for user access, so that access is revoked when a user no longer needs it. This is to prevent unauthorised access.
- Use MFA for user authentication.
- Have activity logs for the purposes of review and monitoring.

Password Managers

guidance makes clear that you should have different passwords for different services. These passwords must be complex.

But how do you remember all these different passwords?

The simplest way is to use a Password Manager. If you have lots of different, and complex, passwords for all your accounts, using a password manager makes life much easier.

This article provides guidance on using password managers within the .

Password managers and vaults

A password manager stores sensitive information in an encrypted form. Password managers are sometimes called password vaults.

In the , password managers are tools that you might use for your personal accounts. Password vaults are tools that a team of people might use to look after details for shared accounts.

Password vaults usually have extra strong access controls, such as hardware tokens.

Here, we use password manager and 'password vault interchangeably, except when stated otherwise.

When to use a password manager or a password vault

The following table shows when you might use a password manager or vault:

Scenario	Tool	Notes
Single user, personal accounts	Password manager	For accounts that only you use, or have access to, then you would probably store the details in a password manager. An example would be storing the username and password for your work email account; only you should have access.
Multiple users, shared accounts	Password manager or password vault	Some accounts might be shared between a group of users. For example, a team might need to know the password for an encrypted document. If the access required is for a sensitive or operational system, then a more heavily protected tool such as a password vault might be appropriate.

Scenario	Tool	Notes
System access, no human use	Password vault	Some systems need to 'talk' directly to other systems. No humans are involved in the conversation. The passwords protecting these communications can - and should - be extremely complex. A strongly secured password vault would be ideal for this purpose.

Best practices

The NCSC is very clear:

- "Should I use a password manager? Yes. Password managers are a good thing."

This is helpful for us in the , as much of our IT Policy and guidance derives from NCSC best practices.

Good password managers

A password manager should never store passwords in an unencrypted form. This means that keeping a list of passwords in a simple text file using Notepad would be A Bad Thing.

Good password managers encrypt the passwords in a file using strong encryption. It shouldn't matter where you store the encrypted file. Storing the list "in the cloud" lets your password manager access the data from any device. This is useful if you are logging in from a laptop, or a mobile device. Storing the passwords locally means the password manager works even when offline.

A good password manager will have:

- Strong encryption for the list of passwords.
- Network access for encrypted lists stored in the cloud.
- A dedicated app but also a pure web browser method for working with your password list.
- A tool to generate passwords of varying complexity.
- The ability to fill in login pages.

What password manager to use

In the NCSC article, they are very careful not to identify or recommend a password manager. This ... caution ... is the reason why we don't say much about password managers within the guidance.

There are several password managers used within the . KeePass and 1Password are probably the most popular for personal or team passwords. To determine whether a particular password manager is suitable for work usage, check the General app guidance.

Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at 1Password. Try it out. When you decide on a password manager, request approval from your line manager to install and use it: "I'm planning to install and use XYZ to manage my passwords, is that OK?".

Refer also to the Using 1Passwords guidance.

Passwords

This article provides guidance on passwords and Personal Identification Numbers (PINs) within the . It helps you protect IT systems by telling you about choosing and using passwords and PINs. Whenever you encounter the word "system" here, it applies to:

- Hardware, such as laptops, PCs, servers, mobile devices, and any IT equipment.
- Software, such as the Operating System, or applications installed on hardware, or mobile device applications (apps).
- Services, such as remote databases or cloud-based tools like Slack.

This guidance is for all users. It also includes more detail for system administrators or developers.

Note: Except where stated, the guidance in this article applies to both passwords and PINs.

Related information

Technical Controls Policy on page 30
Access Control guide on page 87

General best practices

Note: This section applies to passwords and PINs.

You share your password or account details with anyone, unless you have documented approval to share from your Line Manager or higher senior manager.

If a system or another person provides you with a password, change it before doing any work on that system. Examples of 'single-use' passwords include:

- Your own account on a work-provided laptop.
- A shared account for accessing a data analytics service.
- All supplier or vendor supplied accounts.

You change a password whenever:

- There has been a security incident involving your account or password. For example, someone guessed your password, or you used it on another account.
- There was a security incident with the service that you access using the password. For example, if someone broke into the system that provides the service you use.
- Your line manager or other authorised person tells you to do so.

When required to change a password, you do so as soon as possible. If you don't change the password soon enough, you might be locked out of your account automatically. The following table shows the maximum time allowed:

Type of system	Maximum time to change a password
Single-user systems, such as laptops	1 week
All other systems	1 day

Best password practices for everyone

Note: This section applies to passwords only, not PINs.

The password guidance follows NCSC guidance. The NCSC recommends a simpler approach to passwords. Some agencies or bodies might have specific requirements or variations. Check your team Intranet or ask your Line Manager for more information.

Follow the CyberAware advice to generate your passwords. Always use a separate and unique password for each account or service.

The most important points to remember are that passwords should be:

- At least 8 characters long.
- No more than 128 characters long.
- Not obvious.
- Not a dictionary word. A combination of dictionary words might be suitable, such as “`CorrectHorseBatteryStaple`”.
- Unique for each account or service.

Best PIN practices for everyone

Note: This section applies to PINs only, not passwords.

Some devices, especially mobile devices, only support numerical passwords, or Personal Identification Numbers (PINs).

If the device supports passwords, then passwords be used rather than PINs.

If the device supports only PINs, you :

- Always use a separate and unique PIN for each account or service.
- Ensure the PIN is at least 4 characters long.
- Avoid using obvious PINs, such as `1234`.
- Avoid using repeating digits in the PIN, for example `0000` or `9999`.

App-based password protection for files

Some applications - including Microsoft Office tools such as Word, Excel, and Powerpoint - provide mechanisms for protecting files. A password controls whether someone can open, or edit, a file.

While these app-based password protection mechanisms are better than nothing, there are three good reasons for avoiding them if possible.

1. You depend on the application to provide and maintain strong password protection. If the password implementation fails, or has a weakness, you might not know about it. This means that you might think your information is protected, when in fact it is at risk.
2. It is tempting to use a standard password for protecting a file within the app, so that other people can share and work with the file. Changing the password becomes "inconvenient". The result is that many versions of the data file are all protected with the same password. Also, if anyone has ever been given the password to access the file, they will always be able to access the file.
3. If you forget the app-based password, there might not be a recovery process available to you.

For these reasons, advice is that you use password tools within an app to protect data files that are processed by the app. For example, you use the password tools with Microsoft Word, Excel, or Powerpoint, to protect information within files. Instead, either:

1. Store the data files in a shared but secure area, such as the SharePoint storage facility.
2. Use separate encryption tools to protect data files, separate from the app that works with the data files.

Of these two options, storing data files in a shared but secure area is strongly preferred. The reason is that you can add, modify, or revoke access permissions to the storage area easily.

If you have no choice, and have to use app-based password protection, ensure that the same password is not used indefinitely for a data file. You use a different password for:

- Each major version of a data file, for example version 2.x is different to version 3.x.
- Any data file where the password is more than three months old.

Note: This advice is a specific exception to the general guidance, that you do not normally need to change passwords.

Password expiry

You don't have to change a password because it is old. The reason is that time-expiry of passwords is an ...outdated and ineffective practice.

Some current or legacy systems don't allow passwords that follow guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to guidance.

Password managers

Use a password manager to help you keep track of your passwords.

These are tools that help you create, use, and manage your passwords. A useful overview is available here.

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager. For example, development teams in Digital & Technology use 1Password.

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services. Some managers have extra features, such as password generators. Some managers can even automatically fill-in username and password fields for you when during log in.

The password manager database is often stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for your account and service details is recommended.

You can find additional useful information about password manager tools here.

Extra guidance for system administrators or developers is available here.

System administrators or developers

Follow the Government Service Manual for Passwords when you administer or develop MOJ systems or services.

Suppliers and vendors ensure that systems support the password requirements. Systems be able to issue, change, reset, and revoke passwords. This be possible using well-defined and fully-described processes. Supply enough information and procedures to fulfil password policy.

The NCSC guidance for simplifying passwords says that forcing complex passwords has:

- Marginal security benefit.
- A high user burden.

Technical controls are more effective at protecting password-based authentication. Examples include:

- Locking accounts after repeated access attempts.
- Blocking common password choices.

User facing services

Authenticate people accessing user facing services by using the GOV.UK Verify service. It is not necessary for someone to be a UK Citizen to use the GOV.UK Verify service, but they have a UK address.

If it is not possible to use GOV.UK Verify, follow the advice presented here to support citizen passwords. Pay extra attention to the following points:

- People should have complex passwords which are different for each service they use. Make it easy for people to have complex passwords by supporting password managers. For example, services should always let users paste passwords into web forms.
- Don't force regular password expiry. Make it easy to change passwords when required.
- Do force password changes when required. For example, after exceeding a count of unsuccessful password entry attempts.
- Make the process of resetting a password like providing a password for the first time. Include a way to prevent attackers using the reset process to conduct an attack.

For more information, refer to the Multi-user accounts and Public-Facing Service Accounts Guide.

Service Accounts

System and application authentication always use service accounts. Use certificates for service account authentication. Follow NCSC guidelines for issuing and securing the certificates. If you can't use certificates, passwords are an acceptable alternative.

Service account passwords :

- Be system generated.
- Be at least 15 characters long.
- Be no more than 128 characters long.
- Be complex, including upper-case and lower-case letters, digits, punctuation, and special characters.

- Be kept secure, by using hashes or encryption.
- Not be stored in the clear in any systems or applications.
- Not be used by standard or administrative users for any purpose.

For more information, refer to the Multi-user accounts and Public-Facing Service Accounts Guide.

Default passwords

Change all default passwords when a new, modified, or replacement system arrives. Complete the changes before making the system available for any work.

When preparing devices or services for first use, system developers or system administrators configure the default password on the device or service so that it can be used once only. The “first use” of a password forces the user to change the password before the device or service can be used.

Multi-factor Authentication

Multi-factor Authentication (MFA) provides extra security for login and access controls. MFA is also referred to as Two-Factor Authentication or 2FA.

MFA be implemented and enabled on systems and services, including user accounts, wherever possible.

When performing a privileged action, such as installing or reconfiguring a system, or changing critical or sensitive details, it is important that the user is correctly and reliably authenticated. This is best done by using MFA. For example, before deleting a database configuration, MFA have been completed successfully during the authentication process, to confirm that the user is indeed who they claim to be, and that they are indeed authorised to perform that privileged task.

In general, follow the NCSC guidance for enabling MFA.

Use Time-based One-Time Password Algorithm (TOTP), or hardware and software tokens, as the preferred MFA mechanisms. If possible, avoid using SMS or email messages containing one-time login codes. If TOTP applications, or hardware- or software-based tokens, are not available to you, then SMS MFA or email MFA is still better than no MFA.

Systems offer MFA alternatives to users where they are available. For example, MFA codes sent by SMS are not suitable if mobile devices are not allowed in the room or building where the privileged task is being performed.

For more information, refer to the Multi-Factor Authentication (MFA) Guide.

Extra measures

Check that a system, service, or information protected by a password is not classified as or . Make sure that it doesn't contain delicate material. Examples include contracts, or personal data or information. If it does contain such material, you might need extra access control.

Check which other systems have access to the system or service. Make sure that the access control suits the material at both ends of the connection.

Appropriate extra measures might include tokens or other multi-factor authentication devices. Think about using an existing authentication system other than passwords. Avoid creating new authentication systems. Try to reduce what a user needs to remember. For more information about authentication, refer to the Authentication guide.

A technical risk assessment helps identifies extra controls for systems. This is mandatory for systems that need formal assurance. Multi-user systems are also subject to a Business Impact Assessment (BIA). For example, an assessment might find that you need extra checks for logging in to an account or service. The checks might depend on various factors such as:

- Time of login.
- Location of login.
- Number of previous connections from the connecting IP address.
- Whether to allow more than one login at a time.

Examples of these extra mechanisms include:

- Biometrics.
- Tokens.
- Certificate-based authentication.

Password storage

Never store, display or print passwords in the clear. If you need to store them, do so by using salted hashes.

Ensure the password storage security matches the classification of the system or data. For help with the appropriate strength of hashing, contact the .

Extra information on handling and protecting passwords is in the Password Storage and Management guide.

Password access attempts

If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is locked. A successful use of the password resets the count to zero again.

Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator or the . The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work. Checks ensure that an attacker cannot use the password reset process.

Blocking bad passwords

You should not try and use obvious passwords. Attempts to do so will be blocked.

Developers and administrators should configure systems to check for and block obvious passwords embedded within a password. For example, `MySecretPassword` is not a good password! Use password and hash lists from SecLists or Have I Been Pwned, to help prevent bad passwords.

Distributing passwords to users

There are times when a system needs to send a password to a user. An example is when granting access to a service for the first time. To send a password to a user, the mechanism used be secure. The protection should match the sensitivity of the information protected by password.

Passwords created for a user should always be single-use. Use an out-of-band channel to send the password to the user. For example, send the password to the user's line manager who will give it to the user.

For more information, refer to the Password Storage and Management Guide.

Single-use passwords

Some passwords are 'one time' or single-use. Administrators and developers use these to grant access to a service for the first time. After using the password once, the user immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they become invalid.

The following table shows the valid lifetime of a single-use password:

Type of system	Lifetime of a single-use password
Single-user systems, such as laptops	1 week
All other systems	1 day

Multi-user systems and services

All multi-user systems and services check for redundant User IDs and accounts. If necessary, remove the redundant IDs or accounts.

The Access Control Guide discusses the management and removal of accounts.

If someone is no longer allowed to access a system, check for and change any shared account or common password they might still have.

For more information, refer to the Multi-user accounts and Public-Facing Service Accounts Guide.

Identity Providers and Single Sign-On

When you need an authentication solution, try to use existing services. Examples include Identity Provider (IdP) or Single Sign-On (SSO) services, such as Office 365 or Digital and Technology G-Suite.

This helps reduce the need to design, create, deploy and manage yet another solution.

SSO integration in existing IdP solutions improves the user experience. This is because you can authenticate to systems using existing credentials.

For more information, refer to the Multi-user accounts and Public-Facing Service Accounts Guide.

Account management

This guidance on passwords is separate from the guidance on account management. You should still follow the rules and processes for managing accounts. In particular, while you don't need to change passwords after a period of time, you should still expire accounts promptly. Examples would be when accounts are no longer required, or have fallen out of use.

For more information, refer to the Account management guide.

Password Storage and Management Guide

Introduction

Do not attempt to implement your own password storage mechanism. Always use an existing, approved password storage solution.

This guide sets out how passwords must be stored securely to prevent unauthorised access or compromise. The encourages the use of password managers to reduce the burden on users for maintaining password security. For more information, refer to the Password Management Guide.

This guide has been written in alignment with NCSC guidance.

Password storage

Passwords must be securely stored within approved storage tools. The following tool is approved and preferred for use:

- 1Password

Do not store sensitive information, such as passwords or credit card details, in unapproved tools. In particular, do not use "Autofill" tools to help fill in forms, unless the tools are provided and approved by the .

Contact the if you have a specialist need to use a different storage tool.

Sharing passwords

Passwords should not normally be shared. Sharing of passwords should be avoided by delegating privileges to other accounts, for example to provide access to a document or inbox.

Passwords can be shared for the following exceptions:

- For an encrypted document that has to be shared to make sense.
- For generic administration accounts on third-party services or applications, which support only a single account for administration purposes. If multiple individuals will perform the role, then the account password would have to be shared. Privileged Access Management (PAM) should be used where possible for systems that are administration only.

Some applications, for example, some social media tools, do not have 'role awareness'. This means you can't have access associated with a role; it must be through an individual account. This is sometimes 'solved' by having a PAM tool, where the PAM tool provides a more comprehensive managed 'gateway' to the underlying tool.

If there is a strong business need for shared access to a resource, account or system, then access to the password should be monitored and continually reviewed. This would be performed by:

- Regular auditing of who should have the password.
- Access revocation by changing the password if someone should no longer have access.
- Using proactive monitoring where it is enabled, for example by cross-referencing instances where the password is used with the dates and times that an authorised person could be using the password.

A shared password must be:

- Governed by PAM, and only be used by known and trusted users.
- Changed if any user in the group is no longer allowed access.
- Shared using a password manager.

Password vaults and managers

A password vault is a tool that stores passwords and other high-value secrets or credentials in an encrypted form. A password manager provides extra user-friendly tools for working with a password vault, for example helping you log in to applications or websites using the credentials stored within the vault. Password managers allow you to keep track of multiple passwords and avoid weak passwords.

The prefers 1Passwords for Team use, or business use by an individual.

Some teams, particularly service development and administration, have specialised needs that make other password vault tools more suitable. These project-specific tools include:

- AWS Key Management
- Azure Key Vault
- Hashicorp Vault
- Kubernetes Secrets

For further guidance on password strength, refer to the Password Creation and Authentication Guide. Contact the if you have a specialised need to use a different password manager or vault.

Policies for Google Apps administrators

Note: This document is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact the .

These policies must be adhered to by all Google Administrators, including Super Administrators. All Administrator activity is recorded, auditable and notified to all other Administrators.

Why?

These policies ensure two things:

1. That administrators have a clear understanding of what is considered acceptable, so that they do not inadvertently perform an administrative action which is later considered unacceptable.
2. In the event that a security incident does occur in relation to Google Apps, that there is a clear policy which can be referred to, to support any action that is taken.

Actions requiring authorisation

The following actions require formal authorisation (e.g. an email confirming that the action can proceed) from at least 2 of the following 3:

- The Chief Digital Officer.
- The for the .
- The Digital Information Assurance Lead.

Actions:

1. Elevate any single user access to administrator from non-administrator.
2. Access any other users' emails or data (active or suspended).
3. Changing any 'global' configuration within Google Apps which affects all users.
4. Transfer any user's data (active or suspended) to another user. This also requires a request from the business area Service Manager.

Things you must do

1. Maintain the active list of all users (active and suspended) and maintain their access control to applications.
2. If anyone who has a Google Apps account leaves the organisation for any reason.
3. Suspend the account.
4. Transfer user's data to a user decided on by their line manager. This also requires a request from the business area Service Manager.
5. On a minimum quarterly basis (rota'd with other Admins) conduct an audit to check:
    - Any escalation of privileges from non-administrator to administrator.
    - Any forwarding of email accounts.
    - Any taking ownership of User accounts.

Policies for MacBook Administrators

Note: This document is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact the .

All User accounts are created as 'Admin' to allow for software installation as part of normal business requirements.

Each laptop has a separate Admin account (created on build) to allow for User deletion and password resets

These policies must be adhered to by all MacBook Fleet Administrators.

Why?

These policies ensure two things:

1. That administrators have a clear understanding of what is considered acceptable, so that they do not inadvertently perform an administrative action which is later considered unacceptable.
2. In the event that a security incident does occur in relation to the MacBook Fleet, that there is a clear policy which can be referred to, to support any action that is taken.

Actions requiring authorisation

The following actions require formal authorisation (e.g. an email confirming that the action can proceed) from at least 2 of the following 3:

- The Chief Digital Officer.
- The for the .
- The Digital Information Assurance Lead.

Actions:

1. Creating a Mac account for a non member of Staff.
2. Access any other users' locally held data (active or suspended).
3. Transfer any user's locally held data (active or suspended) to another user. This also requires a request from the business area Service Manager.

Things you must do

1. Maintain the active list of all active users.
2. Raise an incident with the when leaving Staff have not returned all assets in their possession.
3. If anyone who has a MacBook account leaves the organisation for any reason.

4. Retrieve the Users equipment and suspend the account.
5. If requested by a Head of Profession, transfer user's data to a user decided on by their line manager. This also requires a request from the business area Service Manager.
6. On a minimum quarterly basis conduct a random percentage audit to check the encryption status of Mac Books and/or Airs.

System Users and Application Administrators

Note: This document is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact the .

How to use this document

This policy applies to all staff and contractors who work for the .

Who does it apply to?

All Users of the "[ORGANISATION]" Information and Communications Technology (IT) systems.

This document is designed to help Users utilise and access "[ORGANISATION]" IT systems in a safe and secure manner. Everyone using "[ORGANISATION]" IT systems must follow these procedures.

When and how should these procedures be used?

Users' Security Awareness training will cover these procedures.

Users must read this document prior to using any "[ORGANISATION]" IT Systems for the first time, and revisit it every six (6) months to remind themselves of the procedures. Regular audits will be performed to check that these procedures are being followed.

Users must understand that they are responsible for maintaining the security of "[ORGANISATION]" systems, and that failure to comply with these SyOPs could lead to compromise of the "[ORGANISATION]"'s infrastructure or even the entire GSI. Users must note further that either failure to comply with this SyOPs or failure to return the security sign off form would be considered a breach of the "[ORGANISATION]" IT Security Policy.

For further all the security related information required, please refer to:

- The "[ORGANISATION]" staff intranet Security homepage
- Remote User Security Operating Procedures (SyOPs) (if applicable)
- Blackberry User SyOPs (if applicable)

Area of control	All Users	Application Administrators Only
Shut-down and start-up	Start-up: • A physical inspection of the workstation must be carried out for any signs of tampering prior to switching the machine on. • The sharing of credentials, and attempting to logon as someone else (or with credentials which you are not authorised to use), are strictly forbidden. Shut-down: • Users must log-off the workstation and ensure it is switched off whenever left unattended for more than 4 hours or overnight.	

Physical access controls	• Only authorised members of staff with registered user accounts are permitted access to the system. • The equipment used to access the system must be checked on a daily basis for evidence of tampering or suspicious devices attached to it, for example unknown Universal Serial Bus (USB) devices attached to the rear of the main workstation. • Protectively marked and sensitive hardcopy material must be securely stored away under lock and key following the [ORGANISATION] Clear Desk Policy, published on the [ORGANISATION] intranet. • When accessing the system from portable computing devices, access is only to be made in approved area (refer to the SyOPs for Remote Access use. • Visitors must be supervised during working hours, and any sensitive documentation being worked on is to be hidden from line of sight as much as possible.
Awareness	• When visitors are present, ensure that they are only able to access information for which they have a need-to-know. • Users must be aware of anyone 'shoulder surfing' and viewing information for which they do not have a need-to-know. • Users must not hold conversations over any telephone or send communications via fax or email if the information being discussed is protectively marked RESTRICTED.

Identification and authentication	• Users must not attempt to log on as another user, or share their system access credentials with others. • Users must not allow unauthorised users to observe their screen. • Users must not allow any person to observe them entering their system access credentials (e.g. password). • Passwords used on the system must be created in line with the [ORGANISATION] Password Standard. • Users must invoke the screensaver before leaving their workstation unattended (by pressing 'windows' key + L). • A User account must only be created with permissions commensurate to that User's business role, and are only to be enabled once a signed copy of these SyOPs have been received from the user. • A User account must be disabled when that staff member leave the [ORGANISATION] or where their business role does not require them to have access.
Resetting user passwords	• To change a password, Users must hold down Ctrl + Alt + Delete on their keyboard and select 'Change Password'. • If the password requires resetting, contact the #unique_634.
System Use	• Users must not exceed (or attempt to exceed) their given access privileges, amend the system configuration or plug in any unauthorised devices. • Any unauthorised attempt at changing the configuration of the system, escalating privileges or installing devices/software may be subject to investigation and formal disciplinary action. • Unauthorised software must not be installed or used on the system. • Administrator level accounts should only be used when carrying out administrative tasks; at all other times a Normal User account should be used.

Acceptable use	• The system must only be used in accordance with the [ORGANISATION] Acceptable Use Policy. • The system must only be used for the business purposes for which it is intended. • Any attempt to use it for other reasons may constitute a disciplinary offence.
Import/Export	• A log must be maintained of all file imports/exports, this can either be a paper based or held electronically. • All imports/export of electronic data/files to the System must be scanned for malicious code. • Users must check and file exports to ensure that only files that they intended to export from one environment to another are exported. • Where a network printer are used, Users must ensure print outs are collected promptly to minimise the risk of inadvertent disclosure.
Anti virus	In the event of a User suspecting a virus attack on the network, they must carry out the following steps: • If operationally possible, leave the system switched on in its infected condition; • Disconnect the affected workstation from the network (where possible); • Mark the system and any associate storage media with a label stating that the machine has a suspected virus; • Inform the #unique_634 who will provide assistance.

Removable media	• No System media or document is to be removed from the building without prior authorisation from the Information Asset Owner.
	• All media and documents exported from the system must be registered in the media/document register and clearly marked with their protective marking in accordance with the Information Classification and Handling Policy.
	• When a media/document is sent outside the [ORGANISATION] to an external body the following procedures must be adhered to:
	  • The export must be covered by an Information Sharing Agreement between the Authority and the external body which has been approved by the Information Asset Owner.
	  • Each export must be authorised by the Local/System Manager.
	  • Each export must have a data export receipt filled out and returned by the receiver to account for the transactions successful delivery

Secure Disposal of Protectively Marked material	• Protectively Marked material must be disposed separately from general waste. Such waste should not be accessible to those without the proper authority. • PROTECT and RESTRICTED classified information can be disposed via standard office provided shred bins allocated to hold material up to and including RESTRICTED. • For CONFIDENTIAL, SECRET OR TOP SECRET information, Corporate Security Team must be contacted when securely disposing of paper documents, and [ORGANISATION] Security Team must be contacted for the secure disposal of IT devices. • Further instructions can be found on the [ORGANISATION] Intranet, Confidential Waste Disposal page.

Security Incident and General Reporting Procedures	• All requests for IT support and all reports of IT failures must be logged with the . • Any incident involving a suspected or known security breach involving personnel, hardware, software, communications, document or physical security must be reported immediately to the IT System Manager and the [ORGANISATION] Security Team. • Any loss of IT equipment, [ORGANISATION] or personal data should be reported. Report also to the Users' line manager, the and to the Data Access & Compliance Unit (DACU). To ensure a quick response all emails must be marked Urgent and have 'Data Incident' in the title/subject heading.

By signing I acknowledge that I have read the Security Operating Procedures (SyOPs) and agree to be bound by them.

Name:
Date:
Signature:

Using 1Password

What is 1Password?

1Password is an online password management tool that we make available to you to help you create, store and share passwords. Using it means you no longer need to remember dozens of passwords, just a single primary password. It keeps all your website logins protected, helps with creating new 'strong' passwords and password sharing when required.

1Password is available as a browser extension for popular browsers, as well as a full software suite (for use outside of browsers) for Microsoft Windows and Apple macOS.

1Password securely saves your credentials in your own 'Vault' and then offers to autofill those credentials the next time you need them.

The has the Business tier of 1Password.

Who should use it?

Currently, 1Password accounts can be requested by service or operations teams that have a need for shared passwords.

How to get it

Contact the to request access.

Make sure you include in your message:

- which team you're in
- your role in your team
- why you need access

What it can be used for

1Password can be used for sharing passwords within a team, when individual named accounts cannot be created in the service. A good example is running a shared Twitter account.

Note: If you have a business need for a shared Twitter account, consider using a more enterprise-orientated tool for social media posting, such as TweetDeck or Hootsuite. You need formal approval to use tools like these.

Personal use

You use your 1Password account to store personal non-work information as it is a work account belonging to the . You may lose access if you change role. You will lose access entirely if you leave the .

Operations Engineering cannot routinely access the contents of vaults but can reset accounts to gain access if there is a good reason to do so.

What it shouldn't be used for

1Password be used for storing personal passwords, or for storing documents. Use existing approved services such as Office 365 or for storing documents.

You use 1Password for 'secrets' that belong to systems, only credentials to be used by humans. There is separate guidance on how to handle system secrets.

How to use it
Getting started

You will be sent an email to your work email account inviting you to create your account. 1Password have 'getting started' guides on their website.

Creating your primary password

You need to create a primary password - this is the only password you'll need to remember.

It be at least 14 characters long (the longer the better).

You can choose to make it pronounceable and memorable (passphrase) such as `CyberSecurityRules!` or `Sup3rD00p3rc0Mp3X!`, as long as you're comfortable remembering it and won't need to write it down.

There are password guidance standards here.

Your primary password be unique and you use it anywhere else (including a similar version, for example, by simply adding numbers to the end)

Multi-Factor Authentication

You setup multi-factor authentication (MFA, sometimes known as 2FA) for your account.

1Password has a guide on setting up MFA.

The has an 'order of preference' for which types of MFA to use:

- Hardware-based (for example, Yubikeys)
- Software-based (for example, Google Prompt on a mobile device)
- TOTP-based (the code is held by a dedicated app such as Google or LastPass Authenticator on a mobile device)
- SMS-based (a one-time code sent via SMS)

If you don't have an -issued work smartphone you may use a personal device for MFA.

Sharing passwords

To share a password, create a Vault.

You make sure the credentials you're sharing are only available to the people who need to access them for work. It is your responsibility to remove items or people from vaults when access to the credential(s) is no longer required.

You share your 1Password main password with anyone, even your line manager or security.

Using it overseas

Taking a device (such as personal smartphone) that has 1Password installed counts as travelling overseas with information.

The has existing policies on travelling abroad on the intranet, which require various approvals before travel.

It may be simpler to 'log out' of the 1Password applications or enable Travel Mode to remove vaults from your devices. These can be reinstated when you return to the UK.

Keeping 1Password update to date

Like all software, it is important to keep the software up to date (sometimes known as 'patching'). 1Password software generally self-updates to the latest version by itself, however make sure you approve or apply any updates if 1Password asks you to.

Need help?

If you need help *installing* 1Password contact the relevant .

If you need help using 1Password such as getting access to vaults or resetting your primary password as you have forgotten it, contact s.

Cryptography

Cryptographic controls

Automated certificate renewal

Note: If you want client certificates, contact .

Where technically suitable, all new domains **must** use automated certificate techniques and services, such as AWS Certificate Manager (most preferred) or Let's Encrypt (uses ACME)

Over time, existing domains **must** also be considered for migration to automated certificate provisioning and management techniques (preferably on their next certificate renewal cycle in advance of expiry) in order to reduce the consequences and management overheads of manual certificate renewal.

The acknowledges that not all systems support automated certificate management but leveraging such technology where possible reduces management overheads, the costs of such overheads and the consequences of unexpected certificate expiry.

Manual certificate requests

Where automated certificate renewal is not possible, new certificates **must** be acquired through the Certificates team.

To request a manually issued certificate, complete the certificate request form and send it, with a Certificate Signing Request (CSR) (and an authority email approval if not an employee e.g. 3rd party supplier), to .

Note: If you want client certificates, contact .

Cryptography

The base principles

- All data **must** employ adequate and proportionate cryptography to preserve confidentiality and integrity whether data is at-rest or in-transit.
- Existing cryptographic algorithms (and implementations thereof) should be used - at the highest possible abstraction level.

In-transit

In-transit encryption techniques can both protect data during transit through cryptography but also help facilitate the establishing of identity of devices on one or more sides of the connection.

Transport Layer Security (TLS)

The National Cyber Security Centre (NCSC) have published information on good TLS configurations https://www.ncsc.gov.uk/guidance/tls-external-facing-services.

In general, subject to document exceptions (such as end-user needs and required legacy backwards compatibility).

Testing

Tools such as Qualys SSL Server Test and Check TLS services from checktls.com **must** be used where applicable to help identify most common issues and configuration problems.

While these tools are not a replacement for skilled testing, the outputs of these tools can help you identify inefficient or insecure configurations which should be considered for remediation.

Configurations should be periodically re-validated.

Internet protocol security (IPsec)

NCSC have published information on good IPsec configurations https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data.

At-rest

At-rest encryption techniques can protect data while being stored and even during some processing. At-rest techniques usually protect against physical theft or attack methods.

Server-based

Local storage (such as operating system locations) and filestores (such as storage area networks) should be considered for at-rest encryption to help mitigate again physical interception (such as theft) threats.

Given the autonomous nature of server provisioning and management, it may not always be technically practical to implement such encryption (particularly when a physical server restart would require human intervention with a decryption passphrase).

In general, at-rest encryption **must** always be proportionally considered, even if documented as not reasonable to implement.

Cloud-based

Vendor managed at-rest encryption **must** be enabled by default unless there is a good reason not to (for example, licensing restrictions or severe performance issues).

Vendor managed at-rest encryption (the vendor will typically managed encryption keys, on-the-fly encryption and decryption) is preferred, shifting management to the vendor under the shared responsibility model.

In some circumstances, it *may* be reasonable to self-managed encryption keys but should be relatively rare.

End-User Device based

Native at-rest encryption such as Apple macOS FileVault, Apple APFS or Microsoft Windows BitLocker **must** be used, preferably controlled by central enterprise device management and key management systems.

The NCSC have published end-user device guidance that discusses such technologies.

Portable storage

Portable storage such as CDs, DVDs and USB sticks can be safely used to move data. As usual, data must be adequately protected based on the overall governance and information risk requirements.

While the following certifications are preferred, they may not be required based on the data and data methods being stored or transported.

- FIPS 140-2 Level 3
- NCSC CPA
- NATO Restricted Level Certified

The prefers the use of network-based transfers compared to the use of portable storage (even if the portable storage is encrypted).

Portable end-user devices

Portable end-user devices such as laptops, tablets and smart phones must utilised at-rest encryption to protect on-board data (and subsequent configured accounts) while the device is 'locked' or powered down.

The NCSC End-user Device Security Collection discusses per-platform configuration advice.

Summarily, native at-rest encryption must be enabled with a suitable and proportional decryption code (typically, a password) and hardware-backed cryptography is preferred.

Hashing

Data that should be kept confidential or is worthwhile to otherwise obfuscate should be hashed. This **must** apply where authentication credentials are stored, such as a password.

The published Password Standard has a section on hashing as part of password storage.

HMG Cryptography Business Continuity Management Standard

Introduction
Scope

This Business continuity plan is limited to all HMG cryptographic material procured by the Crypto Custodian for and on behalf of any part of the with the exception of BRENT encryption requirements.

Who needs to read this document

This document is for the Crypto Custodian, the Alternate Crypto Custodian and any authorised signatories and or people who have access to the safes where encryption that is managed by the Crypto Custodian is stored.

Background

All HMG encryption is procured from CESG which is the National Technical Authority for Information Assurance and is based in GCHQ. It is typically produced to support a CESG Assisted Products Service (CAPS) product which means that it has gone through rigorous testing to give HMG assurance that it is secure. HMG Cryptography is produced under special circumstances to provide additional assurance and that process, distribution and storage of this material is protected and secure.

HMG has specific standards on the management of Crypto and other associated products called the HMG IS4, it is the policy of the to follow and comply with HMG IS4 and this document is intended to support and augment that standard.

Encryption Media
Types of encryption and how they are distributed

Key Variables are typically loaded onto Floppy discs, or CD.

Hard disc encryption

Products such as Becrypt, Eclypt and Bitlocker are procured and distributed to by suppliers through the Crypto Custodian and transferred to them to deploy and manage for the lifetime of the key variable which is determined by the CESG Security Operating Procedures (SyOPs).

Transmission encryption

Products such as XKryptor, Datacryptor and Ultra AEP are procured and managed by the Crypto Custodian and distributed to suppliers as and when necessary and returned to the Crypto Custodian for storage.

Segregation and supersession

Key variables that are issued from CESG are typically issued with two editions. The first is for immediate deployment and the second is for emergency supersession. In the case of hard disc encryption the supplier holds the live edition and the Crypto Custodian holds any others. All supplier crypto deployment environments are not at the same site as the Crypto Custodian and this provides natural segregation of the editions.

Eclypt uses a lifetime key variable and does not have more than one edition, In the event of compromise, the usual CINRAS report and request to CESG for emergency replacement of the key variable will be required.

Protection of Key Variables

All encryption is stored in a CPNI (Centre for the Protection of the National Infrastructure) Class 4 safe which also has a certified 2 hour burning time. Protecting the safe is a fire suppressant sprinkler system.

Access to the safe is strictly limited to the Crypto Custodian and the Alternate Crypto Custodian. A copy of the master code for the safe is stored with the Departmental Security Officer. Only the DSO or ITSO are permitted to open the safe in the event of an emergency.

Work ethic with key variables

The area that the Custodian works is open plan in an accredited IL3 environment. The DSO has further accredited the immediate area surrounding the Crypto Custodian in 5.31 of 102 Petty France for Crypto Management on the understanding that the personnel surrounding them are SC cleared and because there are desks immediately by the safe to allow a clear line of site from the Custodian's desk to the safe.

All key variables must be kept in the safe and only removed when specific action is required on a key variable.

Emergency procedures for evacuation and invacuation

Applicable to anyone who has access to any of the safes:

1. If the alarms sound return all encryption that is out and in use to the fireproof safe.
2. **Lock and check** all safes are secure.
3. Leave by the nearest exit in accordance with Fire Evacuation procedures.

Post action to emergency evacuation and invacuation

If there has been any damage to any of the encryption stored at the :

- Notify CESG immediately on: 01242 221491 extension 31950

  notifying them of the event and request an immediate record of holdings list.
- A CINRAS report must be generated and issued to CINRAS (contact via Security Team)

  and a copy to the Security Team:
- A muster of all key variables and a check against the record of holding list undertaken and an order to CESG raised of any replacement key variables.
- Upon receipt of a replacement key variable emergency plans to change the key variable of the associated product must begin.

Public Key Infrastructure Policy

Introduction
Scope

Within the , there are a number of requirements for Public Key Infrastructure (PKI) services to support confidentiality, integrity and authentication. This document defines the mandatory policy requirements for PKI use.

The policy contained in this document refers specifically to PKI Services used for the following functions:

- PSN Wide Area Network VPN cryptography
- Server-side certificates for:
  - Internet applications
  - Intranet applications
  - PSN/GSI applications
- User and Device Certificates for Network Access Control using 802.1x EAP/TLS
- User certificates for digital signature functions

For PKI Services in respect of other functions, including RAS VPNs, contact the appropriate system Accreditor or Crypto Custodian.

Out of Scope

Any information or component, which operates at or (e.g. Private Keys with a classification higher than) fall outside of the scope of this policy

Certificates used for authentication of users or organisations used in token or PKI based authentications systems other than 802.1x are out of scope.

Defined Terms

Term	Definition
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, validate and revoke digital certificates.
Certificate Authority (CA)	An entity that issues digital certificates. Certificate Authorities are hierarchical, with subordinate CAs being authorised to issue certificates by a trusted, top level, "Root" CA.
Registration Authority (RA)	An entity that validates the identities of actors in a PKI, and processes certificate signing requests and certificate revocation requests on behalf of authorised actors sending these to the CA for processing.
Validation authority (VA)	A service that authenticates and validates the certificates of a PKI. The VA provides a public key directory and also enables access to certificate revocation information either by providing CRLs or using the OCSP protocol.
Certificate Policy (CP)	A document that states the different actors of a public key infrastructure (PKI), specifying their roles and their duties. Its content and structure is described in IETF RFC3647 [Ref.16]. This is often a legal document forming part of a contract.
Certificate Practice Statement (CPS)	A document from a Certificate Authority which describes their practice for issuing and managing public key certificates in line with the root CA Certificate Policy. . Its content and structure is described in IETF RFC3647.
Certificate Revocation List (CRL)	A signed list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked before they expire, and therefore, entities presenting those (revoked) certificates should no longer be trusted. CRL is described in IETF RFC5280.
Online Certificate Status Protocol (OCSP)	An Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in IETF RFC 6960
Trust Anchor	An authoritative entity for which trust is presumed and not derived. Root CAs must be Trust Anchors.
Certificate Signing Request (CSR)	A message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Normally complies with PKCS #10 as defined in IETF RFC 2986
Certificate Revocation Request (CRR)	A message sent from the registered owner of a digital certificate to a certificate authority in order to revoke a compromised digital certificate. Normally complies with PKCS #10 as defined in IETF RFC 2986.

Key	A piece of information that determines the functional output of a cryptographic algorithm or cipher.
Public Key Cryptography	A class of cryptographic algorithms which requires two separate keys, one of which is kept private (secret) and one of which is made public usually embedded in a certificate.
Private Key (PrK)	A secret key used to decrypt or digitally sign information.
Public Key (PuK)	A non-sensitive key that is used to encrypt information or validate digital signatures.
PKI Services	The services provided in the delivery of Public Key Infrastructure. PKI Services includes those provided either as a root or subordinate Certificate Authority, Registration Authority, and Validation Authority. The usage of digital certificates for cryptography or digital signatures within applications and other IT systems is not considered a PKI Service, but those systems would consume PKI Services.
PKI Customer	An entity (a user or organisation) that is authorised to access the PKI Services for the purposes of signing or revoking digital certificates. Some PKI customers may also provide delegated PKI Services.

General PKI Policy
Overview

This section describes the common PKI policy that applies regardless of the type of PKI service in question. It covers the following subsections:

- Governance Structure
- Technical Architecture
- Operational Policy
- Process Requirements

Governance Structure

Roles and Responsibilities

- Senior Information Risk Owner (SIRO) – Responsible for all risks to do with the PKI Services. Final point of escalation for incidents.
- Chief Security Officer (CSO) – Responsible for the operational governance of the PKI Services and the report line for the ComSO.
- Communication Security Officer (ComSO) – Responsible for day to day management of the PKI Services, relationship management with CESG and UKKPA (GCHQ's UK key production authority), mustering and other formal processes. First point of escalation for incidents and managing initial incident response.
- Crypto Custodians – Responsible for day to day operation of the PKI services, including the distribution of keys from the UKKPA. Where keymat is provided from the UKKPA they shall be formally trained and authorised Crypto Custodians. For other services they should be formally trained. Note that the Authority's Crypto Custodian may delegate key management responsibilities to Supplier Crypto Custodians.
- IT Security Officer (ITSO) – Responsible for operational IT security management.
- Administrators – Responsible for configuration, maintenance and support of the PKI services
- Auditors – Internal and external auditors including UKKPA and MoJ Information Assurance who ensure that the PKI Services are running within specification and comply with legal and regulatory requirements, HMG Policy and Policy.

Incident Response

1. There shall be an Incident Response and Escalation process in place.
2. The incident response process shall cover procedures for:

- Impact minimisation
- Escalation
- CRL issue
- Digital Forensics
- BC / DR

1. The escalation shall be from the person discovering the incident to the local Crypto Custodian, then the Cypto Custodian, then ComSO, then CSO then SIRO. Escalation to CINRAS and other external bodies shall only be performed by the ComSO, CSO or SIRO.

User Registration

1. Any individual who requires access to the IT Systems providing PKI Services shall be subject to stringent background checks shall be vetted to at least Security Check (SC) before any access to the system is permitted.
2. **Important:** Interim access pending security clearance must not be allowed under any circumstances. The impact of allowing such access in the event that the individual is not subsequently cleared would be to revoke and reissue all certificates signed by the PKI Services.
3. When clearance is confirmed and identity is validated by , the user shall be enrolled in the services required and shall be issued with the relevant credentials for access.
4. Users shall be removed from the systems and their credentials revoked as soon as they leave the role related to the PKI Services. The relevant HR Processes must be reviewed, and updated if necessary, to account for this policy.

Authentication

1. All Users of the PKI Services shall be authenticated beyond reasonable doubt for the purposes of legal admissibility of evidence in accordance with BS 10008. Password strength, complexity and expiry rules must comply with Password requirements.
2. Access to Root CA Services must be subject to multi-factor authentication and subject to two-man rule.
3. Access to specific signing functions shall be subject to specific authentication and access control policies including two man rule.

Accounting

1. Auditing and accounting of all PKI functions must be carried out in accordance with HMG Good Practice Guide 13. The integrity and confidentiality of accounting logs must maintained to British Standard BS 10008 as appropriate for legal admissibility of evidence, in the event that disputes need to be heard in a court of law.
2. Internal audit by authorised auditors shall take place at least every quarter
3. Where PKI Services are subordinate to external services, e.g. UKKPA or PSNA, then the audit and accounting regime must comply with the policies of the relevant authority.
4. Audit reports shall be provided to the CSO and SIRO quarterly.

Compliance

1. The PKI Services shall at all times comply with Legal and Regulatory requirements including (but not limited to):

- Data Protection Act (1998 and 2003)
- Official Secrets Act (1989)
- Cryptography Export Regulations
- Regulation of Investigatory Powers Act (2002) (RIPA) Part 3
- Export Controls Act (2002)
- Electronic Communications Act 2000
- SI 2002/318 The Electronic Signatures Regulations 2002

1. The PKI Services shall at all times comply with HMG Policy including:

- Security Policy Framework
- HMG IA Standard 4
- HMG IA Standard 5

1. The PKI Services shall at all times comply with any Code of Connection, Memorandum of Understanding or other connection criteria that applies to the environment in which the services are deployed. These shall include as a minimum:

- PSN Code of Connection
- GSI Code of Connection (while GSI connections remain)

Technical Architecture

Technical Design Considerations

The design of PKI systems must ensure:

- Resilience
  - Redundancy
  - Business Continuity
  - Disaster Recovery
- Accessibility
  - Availability of Registration; Enrolment; and Validation services
- Security
  - Confidentiality of system assets (hardware, operating systems, and software)
  - Confidentiality of PKI assets (private keys, authentication credentials etc)
  - Integrity of PKI assets
  - Availability of PKI services
  - Confidentiality, Integrity and Availability of information assets that are protected by PKI assets
- Assurance
  - System and Product Assurance: Products should be assured to a formal evaluation recognised by the Authority and appropriate to the sensitivity of the material being processed. For cryptographic material this is normally CESG Assisted Products Scheme (CAPS) or CESG Product Assurance (CPA). Other assurances, such as FIPS 140-2 (Level 2 or better) may be permitted in some cases and, in exceptional circumstances, other forms of assurance may be considered. Where system assurance is required, at the discretion of the Accreditor, then a formalised process will be necessary, e.g. Bespoke Assurance by a CESG approved company. In some cases, again at the discretion of the Accreditor, an IT Health Check may be scoped to provide the necessary assurance.
  - Service Assurance: The security aspects of the service e.g. forensic readiness, auditing, accounting, processes and procedures will be assured through the formal process of accreditation.

Operational Policies

General Operational Policy

1. The Crypto Custodian must be informed of any IT system deployed in support of PKI Services including:

- Certificate Authority devices and software
- Key generating devices
- Random number generating devices used to create entropy for cryptographic components
- Removable media used to transport Certificates and Signing Requests
- Certificate Revocation List services, including OCSP responders

1. The Crypto Custodian reserves the right to audit equipment and processes used in the delivery of PKI Services. The Crypto Custodian requires that all cryptographic components are managed and processed in accordance with HMG Standard IAS4.
2. Any remedial action required by the Crypto Custodian, to meet the requirements of HMG IAS4. must be agreed and implemented within reasonable timescales set by the Crypto Custodian. "Reasonable timescales" means with sufficient time for the supplier to assess the remediation impact, acquire materials for compliance, test the remediation, and to schedule and deploy the remediation on the production equipment with minimum disruption to business.

3. The Crypto Custodian may require key escrow of private keys for lawful purposes. The Crypto Custodian will specify the means by which key material may be exported, stored and transported.

Key escrow may be used for encryption keys but shall under no circumstances be used for signing keys, especially those for use with digital signatures.

Trust Anchor Operational Policy

1. Root CAs for services shared with other parties must be appropriate for the other parties. Trust Anchors for PKI used to deliver services to external parties may be provided by external authorities, e.g. commercial roots, PSN or UKKPA.
2. Root CAs must be off-line to prevent direct attack against the top level trust anchor. Root CAs shall have appropriate controls, as agreed with the Crypto Custodian and reviewed every six months, to protect the signing functions when in operation.
3. The Trust Anchor or root Certificate Authority for all FITS services shall be one of the following, as applicable for the specific use case(s) for each FITS service:

- Provided by UKKPA where required; or
- Provided as a standalone/offline capability as the default for most FITS services; or
- Provided by a suitable Commercial CA, as agreed with the Authority, where appropriate for external-facing services.

1. The Trust Anchor shall only be used for signing Sub-CA or Issuing CA certificates and related CRLs.
2. Assurance of the Trust Anchor CA shall be appropriate to the data assets protected by the digital certificates, as agreed with the Crypto Custodian and Accreditor. For and material, recognised assurances are stated as follows:

- CAPS Baseline
- CPA Foundation
- FIPS140-2 (Level 2)
- Other assurance (permitted in exceptional circumstances when other assurances are not available, and must be supported by a business case, agreed with Accreditor, and signed off by the IAO or SIRO)

Registration Authority Operational Policy

1. The Registration Authority (RA) shall identify, validate and authorise PKI Customers, i.e. organisations that are permitted to make certificate signing requests of the PKI Service. The RA shall also identify, validate and authorise nominated representatives of the PKI Customer, i.e. individuals who are authorised to represent the PKI Customer in respect of the PKI Services. Authorisation will be dependent upon a mutual agreement between the Authority and the PKI Customer specifying the conditions for registration. This may be in the form of a Memo of Understanding or a formal contract.
2. Subordinate Registration Authorities, i.e. those that register entities at a lower level in the trust authority than the root, must comply with any obligations set by the root authority, including the right of the root authority to audit compliance.
3. Identity validation shall comply, where possible, with HMG Good Practice Guide 45 (Identity Proofing and Verification of an Individual) and Good Practice Guide 46 (Organisational Identity).
4. A Registration Authority shall register each authorised organisation requesting certificates for subordinate CAs. On registration, the Registration Authority shall ensure that the registered party is provided with the Certificate Policy of the required service. The registered party shall provide a Certificate Practice Statement in response.
5. The PKI Customer shall at all times have at least two nominated representatives registered with the RA that can act on behalf of the Customer and are authorised to submit CSRs, CRRs and perform other formal tasks.
6. The PKI Customer must notify the RA when any of their nominated representatives are no longer authorised to access the services. Individuals will become unauthorised if their security clearance is expired or revoked, if their employment is terminated, if they are under investigation for malpractice, or if they no longer work on the account.
7. The RA must notify the appropriate Crypto Custodian for potential escalation in respect of the incidents specified at para 2.4.3.6 or any other relevant security incident.

8. Certificates issued to PKI Customers must be revoked when the business relationship is ended. It may be permitted to transfer ownership of certificates in some cases where responsibility is transferred to another party, e.g. contract novation, but each case must be individually agreed with the Crypto Custodian.
9. Auditing and accounting of RA functions must be carried out in accordance with HMG Good Practice Guide 13. The integrity and confidentiality of accounting logs must maintained to British Standard BS 10008 as appropriate for legal admissibility of evidence, in the event that disputes need to be heard in a court of law.
10. For online submission of CSR and CRR the RA shall use two-factor authentication to authenticate and authorise enrolled users.
11. The CSR/CRR form shall have fields for all mandatory information and attachment of a public key in PKCS#10 format.
12. The CSR/CRR shall be approved by one person (e.g. ComSO) and actioned by another (e.g. Crypto Custodian), except in cases where this process is automated. For automated process, e.g. automated generation of device certificates for EUCS client devices, the Crypto Custodian and ComSo must approve the automation process.
13. The CA shall distribute certificates in PKCS #7 format to the requestor and VA as appropriate.

Certificate Authority Operational Policy

1. This section is applicable to root and subordinate CAs. For policy that is specific to Trust Anchor CAs, refer here.
2. Any CA shall be patched against all known vulnerabilities for which a vendor-published patch is available, in accordance with the Authority's patching policy. The operating system supporting the CA must be less than five (5) years old and must have three (3) or more years of vendor support remaining (5/3 rule).
3. Assurance of CA shall be appropriate to the data assets protected by the digital certificates, as agreed with the Crypto Custodian and Accreditor. For and material, assurance preferences are stated as follows:

- CAPS Baseline
- CPA Foundation
- FIPS140-2 (Level 2)
- Other assurance (permitted in exceptional circumstances when other assurances are not available, and must be supported by a business case, agreed with Accreditor, and signed off by the IAO or SIRO)

1. Any CA connected to a network shall be protected from unauthorised access by a security Gateway that minimises the exposure of the CA to attack.
2. Auditing and accounting of RA functions must be carried out in accordance with HMG Good Practice Guide 13. The integrity and confidentiality of accounting logs must maintained to British Standard BS 10008 as appropriate for legal admissibility of evidence, in the event that disputes need to be heard in a court of law.
3. The CA shall be operated in accordance with HMG IS4.

Validation Authority Operational Policy

1. Any VA shall provide authorised access to Certificates and the CRL for the associated CA. This should be automated as far as possible with a Public Key Directory (PKD).
2. The VA shall ensure that the Certificates and CRL are properly signed and authentic before they are published.
3. The VA shall operate a certificate repository that is visible to all authorised users.
4. Auditing and accounting of VA functions must be carried out in accordance with HMG Good Practice Guide 13. The integrity and confidentiality of accounting logs must maintained to British Standard BS 10008 as appropriate for legal admissibility of evidence, in the event that disputes need to be heard in a court of law.

Audit, Accounting and Mustering Policy

1. All requests (CSR/CRR) shall be logged: on receipt; on processing, on certificate/CRL issue and on destruction
2. All access to the systems and use of credentials including failures shall be logged
3. All keymat sub-classified as ACCSEC or CRYPTO shall be mustered quarterly, and in accordance with the individual keymat procedures
4. Audit and accounting logs shall be managed in accordance with BS 10008

Change Control Policy

1. All software shall be patched with the latest security patches. Such patches shall be regression tested before implementation on the live system.

2. All software version updates and hardware changes, including configuration changes shall be approved by the ComSO and implemented by the Administrator.
3. All patches and other minor changes shall be approved by a Crypto Custodian or ComSO and implemented via the change control process.
4. All changes to a trust anchor or standalone/offline root CA shall also be witnessed and signed off by any two of: Crypto Custodians, ComSO, and CSO.

Physical Security Policy

1. The PKI Services shall be located in an HMG Government building or Supplier building with appropriate physical controls for information, as assessed by the Authority's CSO or delegated representative.
2. PKI Services are critical to the security of the information they protect, and therefore should not be housed in open or shared areas. The PKI Services shall be in a room or cage or locked cabinet that has strictly controlled access to named individuals. The strength of the physical controls will depend on the sensitivity of the specific service.
3. The Trust Anchors and any standalone/offline Root CAs shall be kept in a safe or security cabinet protected by a CPNI Class 2 lock or equivalent when not in use. Only the ComSO and CSO, and their delegated representatives, shall know the combination. The ComSO and CSO shall not have credentials to operate the CA devices.
4. The combination code must be changed at least annually, and immediately on permanent departure of any personnel who know the code.

Personnel Security Policy

1. The CSO, ComSO, Crypto Custodians, Administrator(s), and individuals holding other key PKI roles shall have been subjected to BPSS checking and shall maintain a current and valid SC clearance as a minimum. Evidence of clearance will be maintained in an up-to-date register in a format agreed with the and made available to the .
2. The Crypto Custodians shall have formal training from CESG or MoD on key management and PKI operation.
3. No other person shall have access to the PKI infrastructure without prior written permission of the CSO.

Process Requirements

Required Processes

1. The following formal processes shall be written and implemented:
    - Registration and de-registration of an organisation
    - Registration and de-registration of an authorised user of the PKI Services
        - Including identification according to GPG45 and GPG46
        - Audit trail of identification, role allocation and access rights
    - Registration of a nominated individual by a registered organisation by the RA
    - Enrolment
    - Certificate Expiration and Renewal
    - Management of requests (CSR/CRR) by the RA
    - Trust Anchor and root CA operation including signing functions
    - Incident Response, escalation, digital forensics and aftercare
2. Other processes should also be formalised and documented

Required Standards for each function

1. Certificates shall comply with ITU-T Recommendation X.509 and RFC 5280 unless required for a specific application in which case written approval from the SIRO will be required
2. CRLs shall comply with X.509 Version 2 and RFC 5280.
3. All key material management and PKI operations shall be performed in accordance with all relevant HMG standards.

Certificate Policy requirements

1. The CP shall be written by the supplier providing the issuing Certificate Authority in line with RFC3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
2. The PKI service shall not re-sign any public key into a certificate. All public keys shall be new and unique.

3. There shall be a CP for each certificate hierarchy where the scope (including user base), use or liability model is different

Certification Practices Statement requirements

1. The CPS shall be written by the supplier providing the issuing Certificate Authority in line with RFC3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
2. There shall be a CPS for each signing certificate.

References

The following are FITS PKI Policy specific references used within this document.

Ref:	Title & Location
1	HMG Security Policy Framework (SPF) v11.0 Nov 2013 https://www.gov.uk/government/publications/security-policy-framework
2	CESG Cryptographic Standards – Cryptographic Mechanisms, Algorithms & Protocols v1.0 July 2010
3	CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT Systems v1.7 – Oct 2012
4	HMG IA Standard No.4 - Management of Cryptographic Systems v5.3 – Oct 2013
5	HMG IA Standard No.4 - Supplement 1 - Roles and Responsibilities v3.0 - Apr 2013
6	HMG IA Standard No.4 - Supplement 2 - Concepts and Terminology of Cryptography v1.0 - Apr 2011
7	HMG IA Standard No.4 - Supplement 4 - Labelling of Cryptographic Items v2.0 – Nov 2012
8	HMG IA Standard No.4 - Supplement 5 - Account Management v1.0 - Apr 2011
9	HMG IA Standard No.4 - Supplement 6 - Personnel & Physical Security of Crypto Items v3.0 - Nov 2012
10	HMG IA Standard No.4 - Supplement 7 - Accounting of Cryptographic Items v1.0 - Apr 2011
11	HMG IA Standard No.4 - Supplement 8 - Movement of Cryptographic Items v1.0 - Apr 2011
12	HMG IA Standard No.4 - Supplement 9 - Destruction & Disposal of Cryptographic Items v2.0 - Apr 2012
13	HMG IA Standard No.4 - Supplement 10 – Compliance v2.0 – Oct 2013
14	HMG IA Standard No.4 - Supplement 11 - Incident Reporting for Cryptographic Items v2.0 - Apr 2012
15	HMG IA Standard No.4 - Supplement 13 - Assurance Standards v4.0 – Oct 2013
16	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://datatracker.ietf.org/doc/rfc3647/
17	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://datatracker.ietf.org/doc/rfc5280/
18	RFC 6960 - Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP http://datatracker.ietf.org/doc/rfc6960/

19	https://shop.bsigroup.com/SearchResults/?q=BIP%200008 • BIP 0008-1:2008 Evidential weight and legal admissibility of information stored electronically. Code of Practice for the implementation of BS 10008 • BIP 0008-2:2008 Evidential weight and legal admissibility of information transferred electronically. Code of practice for the implementation of BS 10008 • BIP 0008-3:2008 Evidential weight and legal admissibility of linking electronic identity to documents. Code of practice for the implementation of BS 10008
20	CESG Good Practice Guide 45 - Identity Proofing and Verification of an Individual v2.3 – July 2014
21	CESG Good Practice Guide 46 – Organisational Identity v1.0 – Oct 2013
22	HMG IA Standard No. 5 – Secure Sanitisation – v4.0 – April 2011
23	ITU-T Recommendation X.509 – Public-key and Attribute certificate frameworks [10/2012) http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11735
24	RFC 2986 - Certification Request Syntax Specification – November 2000

Use of HMG Cryptography Policy

Related information

Technical Controls Policy on page 30

About this document

This document is the IT Security – Use of HMG Cryptography Policy. It provides the core set of principles, expectations, roles and responsibilities for using HMG cryptographic material.

How to use this document

Each policy statement outlines a security requirement and where applicable, a reference is provided to further material. A unique identifier is associated with each statement for easy reference. The format of each statement is illustrated as follows:

POL.CRYPTO.XXX: Policy statement text.

The policies outlined in this document form the baseline standard. However this policy is not a replacement for HMG Information Assurance Standard No. 4 - Management of Cryptographic Systems [Ref, 2]. HMG IAS4 remains the primary reference source where this policy provides a supplement to it.

Use of HMG Cryptography Policy
Introduction

POL.CRYPTO.001: It is the policy of the to follow the policy of HMG Information Assurance Standard 4. This document endorses and augments that policy. Where the local policy contained herein, if different to HMG Policy, the local policy overrides HMG policy and must be adhered to.

Scope

This policy is concerned with the use of HMG cryptographic material used on any IT system and/or where HMG cryptographic material is obtained through the .

Purpose

uses a wide range of cryptography products or various classifications and is serviced by several suppliers. This policy is intended to supplement the HMG IAS4 [Ref, 2] and assist suppliers to procure encryption from CESG and manage its life cycle.

Audience

Anyone who wants to obtain encryption from CESG and everyone who is, or needs to be, CRYPTO or ACCSEC authorised (refer to the glossary) to handle Key Variables (KV) or hardware.

In accordance with HMG IAS4 [Ref, 2] encryption is only provided for fully accredited systems. There are long lead times to obtain encryption products from CESG (which fluctuate between 8-12 weeks and are always subject to change). It is recognised that there needs to be some flexibility in the process to order encryption and this guide helps meet that requirement.

Definitions

Trusted Hand	An individual who is at least BPSS cleared and recognised as a member of staff of a supplier.

Communication

POL.CRYPTO.002: The use of secure email **must be** used a primary method of communication for all and any communications from suppliers in respect of cryptography to the Crypto Custodian, Communications Security Officer (COMSO) and IT Security Officer (ITSO) regardless of whether the protective marking is UNCLASSIFIED or NOT PROTECTIVELY MARKED and up to RESTRICTED.

Acceptable secure email methods are GSi, xGSi and CJSM accounts. All queries towards CESG must be forwarded to the Crypto Custodian and/or COMSO. CESG must not be contacted direct.

New requirements for encryption and/or hardware

As soon as the need for encryption is identified the system Accreditor, the COMSO must be informed by the Project Manager and agreement sought for the need for the hardware, software and encryption from CESG.

The process requires that an applicant is appointed and that applicant is responsible for ensuring that the product is suitable for the requirement and it is their responsibility to familiarise themselves with the CESG Security Operating Procedures (SyOPs) for that product. The applicant can delegate this element to someone else but that person must be identified to the other parties of this approval process.

POL.CRYPTO.003: The Project Manager **must appoint** an applicant. Exceptionally, the applicant can be the Project Manager. The applicant **must contact** the vendor of the encryption product and obtain the latest version of the CESG macro enabled word application form to complete.

This form must be completed by the applicant with a full explanation of the requirement and attached with, if appropriate, a diagram (e.g. MS Visio diagram) which explains the solution and this must be sent to the COMSO, Accreditor and Crypto Custodian for approval with the application form.

Note: The applicant is responsible for ensuring that the product is suitable and meets the desired business requirement.

If the solution requiring encryption has not yet been Accredited (at the time the application is being drafted), or if the current RMADS need to be updated to accommodate this requirement, a timetable must be set out for the delivery of draft RMADS and SyOPs, this **must be** attached to the application form.

The COMSO and Accreditor must both approve and notify the Crypto Custodian in order for the form to be sent to CESG for processing.

If any of the previous conditions have not been met the form cannot be processed and this may cause delays.

Further processing is required by the Crypto Custodian and upon dispatch to CESG the Crypto Custodian will give the applicant a reference number (hereafter referred to as the IAB account number) which must be referred to in any future communications regarding the requirement.

Increase in a community (usage of Crypto)

When it is necessary to increase the number of licences, changes to hardware or otherwise change how Crypto used, the applicant must obtain the latest form from the vendor and send the form to the Accreditor and COMSO for approval. The applicant must refer to the CESG X reference which can be found in the documentation that the supplier holds.

POL.CRYPTO.004: The applicant **must determine** whether or not a change to the RMADS or SyOPs are necessary and confirm this on application. If changes are required it must be declared how and when this will happen.

POL.CRYPTO.005: The Accreditor and COMSO **must** both agree and approve the change and advise the Crypto Custodian.

The Crypto Custodian will forward the approved form to CESG for processing and any notifications from CESG will be advised by the Crypto Custodian to the applicant.

Authority to Operate Certificate

The Crypto Custodian and the Vendor will be advised by CESG of the Authority to operate and this will be forwarded to the applicant by the Crypto Custodian, with this certificate the applicant can purchase the relevant hardware or licences from the vendor.

It is the responsibility of the applicant to raise any relevant purchase orders though the purchase order system or progress the financial procurement for the product through other channels.

CRYPTO and ACCSEC authorisation

If there is a requirement to store Key Variables locally, the supplier must appoint a Local Crypto Custodian (LCC) and Local Alternate Crypto Custodian (LACC). Both must attend the CESG training course for Crypto Custodians and be sponsored by the Crypto Custodian.

Any subject who handles Key Variables for the must be SC cleared and CRYPTO or ACCSEC authorised initially by the Crypto Custodian. The subject must provide the details on the Crypto Authorisation form through secure channels and provide the contact details of the vetting office which approved their clearance.

POL.CRYPTO.006: Every 12 months the LCC and LACC **must re-authorise** each other and check that their clearances are still valid and this must be evidenced and recorded with the authorisation form for audit purposes.

If the LCC or LACC CRYPTO or ACCSEC authorises anyone else locally, there are responsible for checking the security clearances and maintaining and renewing the authorisation or de-authorisation process and keeping records available for inspection and audit by the Crypto Custodian or Authority.

Delivery of Key Variables

When Key Variables arrives and has been checked and recorded by the Crypto Custodian an email will be sent to the applicant to inform them that their Key Variables has arrived.

Key Variables distribution

All Key Variables is stored and managed centrally by the with some exceptions such as hard disk encryption which suppliers need to store locally.

There are special arrangements for the local storage of Key Variables which must be agreed with the COMSO.

POL.CRYPTO.007: Key Variables **must not** be deployed unless the encryption solution is accredited or the timetable has been set out and agreed on its delivery, draft RMADS and final SyOPs must be made available to the Crypto Custodian.

POL.CRYPTO.008: The applicant **must agree** with the Crypto Custodian how the Key Variables is to be deployed, or provide the details of the person who will manage this if it is not the applicant. Generally speaking the Key Variables is retained at HQ and issued out for a short period of time in order to encrypt the system and then returned to HQ for storage.

Key Variables distribution as follows (in order of preference);

1. Collected from and returned to HQ by a CRYPTO or ACCSEC authorised person and transported in a secure lockable container (such as a lockable briefcase or a CPNI approved transportation container).
2. Collected and returned by trusted hand for transportation in a secure lockable container to a CRYPTO or ACCSEC authorised person in tamper evident packaging using the usual Government Protective Marking Scheme (GPMS).
3. Dispatched from and returned by a reputable courier who guarantees delivery within 24 hours and provides a tracking service (not Royal Mail). The Key Variables must be sealed within tamper evident packaging and appropriately protected. Suppliers must take full responsibility for this process and arrange for courier to collect and return.

Key Variables Management

POL.CRYPTO.009: The management of Key Variables **must be** in accordance with HMG IAS4 Supplement 7 [Ref, 3].

Key Variables Destruction

POL.CRYPTO.010: Suppliers **must not** under any circumstances destroy Key Variables. All Key Variables must be returned to the Crypto Custodian for destruction.

Business continuity

POL.CRYPTO.011: The Crypto Custodian, the Alternate Crypto Custodian and any authorised signatories and or people who have access to the safes where cryptographic material that is managed by the Crypto Custodian is stored must conform to the IT Security Policy - HMG Cryptography Business Continuity Management Standard [Ref, 4].

Annual Audit of Crypto

Every 12 months the COMSO will inspect the arrangements for sites locally storing Key Variables. A date will be agreed with the COMSO to inspect the premises, audit the paperwork and check the crypto stock.

References

ID	Title	Version / Issue
1	IT Security Policy	V1-00
2	HMG IS4 - Management of Cryptographic Systems	Issue 5.1, Apr 2011
3	HMG IS4 - Supplement No.7 - Accounting of Cryptographic Items	Issue 1.0, Apr 2011
4	IT Security Policy - HMG Cryptography Business Continuity Management Standard	V0-01

Physical and environmental security

Equipment

Clear screen and desk

There are many helpful policies and best practices that improve safety and security.

Note: In addition to this advice in this document, you should review and follow the guidance in the remote working guidance, for example thinking before you print.

Clear screen

Users comply with the following:

- equipment be left logged on when unattended. Users ensure that password-protected screensavers are activated when any equipment is left unattended.
- Computer screens be angled away from the view of unauthorised persons.
- Computer security locks be set to activate when there is no activity for a short pre-determined period of time. This timeout be set to 5 minutes, by default. The screen lock be manually activated when required.
- Computer security locks require passwords to be re-entered to reactivate the computer.
- Desktops and laptops be shutdown if you expect to be away from them for more than half an hour.

- Users log off or lock their computers when they leave the room.

A best practice is to keep your screen 'desk top' tidy:

- Avoid leaving files on your desk top where the name might attract attention. For example, having a file on your desk top called `MyPasswords.docx` is a bad idea, for several reasons!
- Avoid having files or information labelled displayed or stored on your desk top.

Clear desk

Users comply with the following:

- Where possible, paper and computer media be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, particularly outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards, or similar secure storage areas are not available, doors be locked if rooms are left unattended. At the end of each session all and information be removed from the work place and stored in a locked area.
- When handling documents security follow the requirements laid down in the Government Classification Scheme (GCS).
- or information, when printed, be cleared from printers immediately.

Think before you print.

It is good practice to lock all rooms and office areas when they are not in use.

Information left on desks is also more likely to be damaged or destroyed in a disaster such as fire or flood.

Equipment Reassignment Guide

Introduction

This guide describes how to reassign equipment. It applies to laptops, mobile phones or other issued equipment. Reassignment is from one user to another.

Who is this for?

This guidance applies to:

1. **Technical users**: these are in-house Digital and Technology staff. They are are responsible for implementing equipment controls. The controls apply throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
2. **Service Providers**: defined as any other business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, and storing data) for, or on behalf of the .
3. **General users**: all other staff working for the .

"All users" means General users, Technical users, and Service Providers.

Returning Equipment

When a project completes, or a colleague leaves or moves to a new role, equipment no longer required be returned. The Line Manager (LM) is responsible for using the Service Catalogue to request a return of the item. The equipment might then become available for use by other employees. It might not be cost-effective to consider reusing or reassigning the equipment. Possible reasons include:

- Older technology that might have been heavily used.
- The likelihood of operating problems and failures.
- Lack of support, updates, or patches.
- Slower performance.

As a result, it might be preferable to use a new machine, rather than repurposing a reassigned device. The decision depends on the expected use of the reassigned device.

The LM is responsible for ensuring a review of the equipment. This is to ensure that sensitive data be lost by erasing the contents of the device. This task be delegated to the team member most familiar with the data. The LM remains responsible. Any sensitive data identified be copied and relocated to a secure location. This can be the Teams facility or to Sharepoint. This happen before the device is made ready for reuse or destroyed.

Any IT equipment which is no longer needed, or has reached its "end of life" have its data securely deleted and confirmed to be unreadable and unrecoverable before destruction, redistribution, or reuse of the equipment.

Equipment Reassignment

Equipment be passed from one user to another without being formally reassigned.

Equipment be completely "cleaned" to an "as-new" state before it is reused or reassigned. This means that all storage media in the device be fully erased. A sufficiently secure method for "wiping" equipment be used. Deleting visible files, emptying files from the "Recycle Bin" of a computer, or reformatting a device are not considered sufficiently secure methods for wiping equipment. The reason is that data recovery software might be used by a new owner to "undelete" files or "unformat" a device.

To erase data securely, use appropriate "data-shredding" tools for the media being erased. Typically, these tools do not simply delete data, they overwrite it multiple times. The overwriting erases all traces of the data, making it almost impossible for any retrieval. Another option is to re-encrypt the device using a different password, then delete the data to free up space.

Equipment reassignment be recorded by the LM in the appropriate asset register.

Equipment that cannot be reused

If IT assets are no longer needed by the , and cannot be securely wiped, then the equipment need to be destroyed physically. More information can be found at Secure disposal of IT equipment

Regrettably, for security reasons, redundant IT equipment be donated to charities, schools, or similar organisations.

Leased equipment

Managers ensure that any equipment that is leased has a data destruction clause written into the contract. Under such an arrangement, the supplier ensure that data is wiped when it is returned. For an example of a data destruction clause, refer to the Modern Security Clause for formal promises (Contracts). This is available from the .

Laptops

The guidance applies to all staff.

Related information

Lost devices or other IT security incidents on page 339

Storing data on laptops

If you need to store data on your computer you should always remember to move it into:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An shared drive.
3. Your -provided 'home' drive.

Do this as soon as you can next connect to the network.

Where data should be saved when using a laptop

It is best to avoid saving any data on a laptop hard drive. However, if you absolutely must, you should always remember to copy or move the data to the network as soon as you next can connect to it, either via secure remote access or by direct connection.

In order to avoid potential data loss, save data in:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An shared drive.
3. Your -provided 'home' drive.

There is a better chance of recovering lost data if you have saved it to the network, as data stored on the network is backed up daily.

The impact of hard drive failures

Hard drive failures can lead to the irrecoverable loss of data. Any data loss can have security implications for the , and a significant impact on:

- Our business opportunities.
- Our reputation.
- Our ability to deliver services to the public.

If you experience any issues with your laptop or IT service, ask for help.

For more information about the main security issues that are likely to affect remote and mobile workers, refer to the remote working guide.

How to reset your password

To reset your password, you will need to contact the #unique_738. They will carry out checks to confirm your identity. This might include asking your line manager or court manager to confirm your identity, by sending an email to the . Once your identity is confirmed, your password will be reset and you will quickly regain access to your laptop.

Locking and shutdown

The has made a commitment towards sustainable IT. The intentions are:

- To reduce overall power consumption for the by switching off machines and saving energy.
- To reduce the 's overall carbon footprint.

Shutting down a desktop computer

- Close all applications.
- Shut down the computer by clicking the 'Start' button at the bottom left hand corner of the screen. Next, click 'Shut Down'.
- A pop-up box will appear with a drop-down box. Select 'Shut Down' and click 'OK'. After a short delay, your computer will automatically shut down.
- Switch off your monitor screen.

The benefits

By switching off our computers at the end of each working day, we are contributing towards being energy efficient and environmentally friendly. We are all responsible for our own Carbon Footprint. So, please switch off your PC monitor along with your desktop computer at the end of each working day. In addition, please switch off any other PC monitors if you notice they too have been left on overnight.

Dealing with issues preventing you from switching off your computer

If there are any issues preventing you from switching off your desktop computer overnight, then please raise this with the #unique_743 immediately as there could be an underlying fault that needs resolving.

If you require any further information regarding this policy, ask for help.

Locking your computer sessions

Access to most computer systems is controlled by a user name and password. If you have the correct information, you are able to 'log in' or 'log on'. The user name identifies the user as a valid user of the system and the password authenticates that the user is who they say they are.

You are responsible for what you do with an system or service. You might be held responsible for any actions carried out using your user name and password. You must therefore not allow any one else to do work on any system using your user name and password. If you leave your computer logged on when you are away from it, it might be possible for sensitive information held on the computer system to be used, read, changed, printed or copied by someone not authorised to access it.

If you are leaving your computer unattended for a short period of time, 'lock' the computer by activating the password protected screen saver or similar 'locking' facility. A simple and quick way to lock a Windows computer is:

1. To LOCK - press the Windows key and L key, at the same time.
2. To UNLOCK - press the Ctrl, Alt and Delete keys, at the same time, then log in as normal.

A simple and quick way to lock a Mac computer is:

1. To LOCK - press the Ctrl, Cmd and Q keys, at the same time.
2. To UNLOCK - move the mouse or press any key, then log in as normal.

Laptops

All laptops have hard disk encryption installed. This protects the entire contents of a laptop's hard disk drive to prevent any data stored locally from being accessed in the event the laptop is either lost or stolen.

Laptop incidents

Investigations into security incidents indicate that a common reason for problems is where the correct security procedures are not being followed. For example, laptops are being left logged on overnight.

This is not good security practice.

If a device is lost or stolen whilst the machine is in locked mode, the data on the machine is more vulnerable to a potential security breach.

Leaving the laptop in premises is not sufficient to guarantee the equipment's security. Laptop losses do sometimes occur within offices. There is a greater risk of data loss when a laptop is left partially logged on overnight, so you should always fully log off the laptop at the end of your working day.

Laptop security

- Switch off the machine completely at the end of each usage.
- Do not attach the password to the machine or keep the password with the machine.

If you need further assistance or information about this process, ask for help.

Policies for MacBook Users

Any User of an -supplied MacBook must ensure they comply with this policy, to ensure that security is not compromised when using these devices.

These Policies are supplementary to the GOV.UK and Enterprise policies, procedures and guidance.

If you are unsure about any of the requirements or content, ask for help.

Policies

- You must not share your login details or password with anyone under any circumstances.
- You must change your password if you suspect it has been compromised, or if instructed to do so by your line manager or other authorised individual.
- You must not attempt to access any other person's data unless you have been authorised to do so.

- You must only collaborate with authorised personnel.
- Get help if you are subjected to any security incident, or suspect you might be.
- You must logoff or lock your computer when leaving it unattended.
- You must keep your Digital& Technology equipment close to you and in sight at all times when in public areas.

Top things to remember

You are responsible and accountable for the security of your equipment at all times.

If you don't think you should do something, you probably shouldn't. If in doubt, always seek advice.

System Lockdown and Hardening Standard

This standard is designed to help protect IT systems by providing basic configuration details for how IT systems should be hardened to defend against malicious attack.

The describes mandatory requirements for security controls. To comply with the , the requires that IT systems and services are:

- Locked-down: All unnecessary or non-essential services or capabilities are switched off, or restricted to the bare minimum of functionality.
- Hardened: All system options and capabilities are configured for maximum possible resistance to attack or unauthorised use.

Specifics of the lockdown policy are covered in the Technical Controls Policy. This document provides more information about the implementation of the lockdown policy.

Related information

Technical Controls Policy on page 30

Scope

This standard provides some high level guidance on IT system hardening. It applies to all IT systems.

Note: This standard is a generic standard, designed to provide high level direction. It does not replace platform- or system-specific hardening guidance, such as vendor advisory or best practice recommendations.

This standard be read in conjunction with the , the , and the .

Demonstration of Compliance

The NCSC GPG40 Information Assurance Maturity Model (IAMM) provides useful guidance on the security levels expected for systems and services. All demonstrate compliance that meets or exceeds maturity Level 1, or equivalent.

Generic hardening standard

This standard provides a generic set of hardening details, designed to guide IT system development and to supplement the Technical Controls Policy.

Those configuring IT systems consider additional sources of reference such as vendor-supplied platform-specific materials to ensure that specific systems, such as SQL server or UNIX-based servers, are built and configured to a secure standard. A selection of external reference sources can be found in this guidance.

Where this standard provides a generic set of hardening procedures, other material in the security guidance provides vendor- and system-specific hardening guides which have been approved for use in IT systems.

The secure configuration of an IT system be examined during the assurance process. This might include an IT Health Check (ITHC), and a review of the system's build configuration.

Details provided in this standard address:

- General procedures which can be commonly applied to most IT systems.
- External devices.
- Account log-on.

- Services, security and networking applications.
- Server-specific procedures which can be commonly applied to servers.

General procedures

Name	Description
BIOS Lockdown	Access to the BIOS be restricted to system administrators only.
Removal of unnecessary applications and services	All applications and system services which are not required be uninstalled or disabled.
Auto-run of data on remote media devices	Auto-run be disabled.
Screen lockout	Desktops and servers be configured to lock after 5 minutes of inactivity. Unlock be by password only.
Time and Date	The Time and Date setting be configured to central synchronisation servers, which themselves synchronise with the UK Government time server.
System Preferences	Users without system administration privileges have access to change the desktop background or screensaver setting, the date or time, network settings or internet browser settings, and system security settings or group policy settings. Users without system administration privileges have access to the system settings or utilities including the system registry or administrative equivalent, access to operating system directories and files, access to CMD or Command Line Prompt, access to terminal commands or tools, or access to local system utilities such as disk defragmenter and disk cleanup.

External Devices

Name	Description
Bluetooth	Bluetooth be disabled by default. If required due to business need, Bluetooth devices be set as 'discoverable'.
Webcam	The webcam lens be obstructed when not in use.
Infrared receiver	The IR receiver be disabled, ideally at the hardware level by physically disconnecting the component.
Sound input (microphone)	Sound input from a microphone be kept at zero level when not in use.
Media drives and external data ports, such as USB, FireWire, CD/DVD drive, and similar	All media drives and external data ports be disabled by default. Where there is a business justification to allow access, that access be audited and restricted to an individual user, for example when using an approved tool for an approved business purpose.

Account Log-on

Name	Description
Passwords	All passwords conform to the password guidance.

Name	Description
Guest and 'null' accounts	Guest and 'null' accounts (accounts with a blank username or password) be disabled and removed where possible.
Fast User Switching	Fast User Switching be disabled.
Login failure logging	Failed logins be logged after the 1st failed attempt.
Automatic log in	Any automatic log in feature be disabled. This does not include Single Sign On functionality, where a user has already authenticated themselves to the system.
User list	During logon, the option to display a set of possible usernames, or the previous usernames that logged on successfully, be disabled.
Logon Banner	The standard login banner be displayed at login, both locally and remotely. The standard banner is provided in Appendix A.

Services, security, and networking applications

Name	Description
Firewalls	An application firewall be installed. The firewall be configured to 'allow only essential services', log firewall activity, and operate in 'stealth mode' (undiscoverable).
Anonymous FTP	Anonymous FTP be disabled. Where there is a business requirement for file transfer between systems, FTP(S) or SFTP be used.
Simple Network Management Protocol (SNMP)	Where SNMP is required, version 2.0 or a more recent version be used.
Cisco Discovery Protocol (CDP)	CDP be disabled.
Telnet based administration interface	Telnet access be disabled.
SSH based administration interface	SSH access direct into an administrative account or service be disabled.
HTTP based administration interface	All web based administration interfaces which are accessible over a network (in other words, not restricted to a localhost) be encrypted for the entire session using SSL version 3, or TLS version 1.2, or higher.
Connection Timeouts	Idle connections be disconnected after a default period; normally less than 30 minutes.
ICMP Redirects	ICMP redirects be disabled.
Clear text authentication protocols	All plain-text authentication protocols be disabled and their functionality replaced with encrypted alternatives.
Initiating outbound connections	An system or service initiate a connection to a non-system or service, unless such outbound connections have been reviewed and approved as a standard part of their design. Firewall rules and other network configuration prevent unapproved outbound connections.

Server specific

Name	Description
Internet access from web browsers	External Internet access from web browsers on a server be disabled.
Example, test and temporary installation files.	All example, test and temporary installation files be deleted when no longer required.
File share access control	Server file shares be subject to access control restrictions.

External reference sources

The following external reference sources provide a good source of information on IT system hardening and secure system configuration.

CPNI

CPNI provides general information on security IT systems including advice on how to build secure systems: https://www.cpni.gov.uk/cyber-security.

NIST

NIST is a US standards body and provide a wealth of information which can be used to build secure systems: https://www.nist.gov/cybersecurity.

SANS

The SANS Institute provides a source of best practice advice for designing and configuring secure systems including Apple MAC OS and Linux based systems: https://www.sans.org/reading_room/.

Microsoft

Microsoft provides detailed information and configuration details covering the lockdown and hardening of Microsoft server and desktop products.

Appendix A: Login banner

The standard login banner be displayed at login:

> THIS SYSTEM IS FOR AUTHORISED USERS ONLY.
>
> This is a private system; only use this system if you have specific authority to do so. Otherwise you are liable to prosecution under the Computer Misuse Act 1990. If you do not have the express permission of the operator or owner of this system, switch off or disconnect now to avoid prosecution.

Operations security

Operational procedures and responsibilities

Mail Check

The service

The Mail Check Service from NCSC is part of the Active Cyber Defence suite of services.

The service helps public sector email administrators improve and maintain the security of their email domains by preventing spoof email.

Domains operated by, or on behalf of, the **must** be added to Mail Check under at least the central Mail Check account.

When to use the service

Mail Check (and the underlying DMARC and SPF configurations) **must** be implemented regardless of whether the domain is expected to send or receive emails on a routine basis.

This is important to ensure domains that are not expected to send emails are still monitored for being spoofed, as they are still legitimate domains which attackers may attempt to exploit in order to attack users.

How to use the service
Requirements

The email domain name is required. It must be publicly contactable for SMTP from the general Internet.

DMARC (which requires SPF and DKIM) TXT records must be available for creation or iteration, as per the GOV.UK DMARC configuration guide page.

is permitted to use the service for free as a central government organisation, but suppliers to currently are not.

Get started

Contact the Cyber Security team to be added into 's subscription of the service.

Offshoring Guide

Related information

Technical Controls Policy on page 30

Introduction
Document Purpose

This document is the IT Information Assurance (IA) Policy and Guidance for offshoring of Information Systems, development, or other support services. The document states the IA requirements that must be complied with for offshore developments, and presents considerations to be taken into account when deciding whether to offshore an element of capability.

This document has not been developed in isolation. It draws heavily and intentionally on other guidance, particularly HMG Good Practice Guide (GPG) 6: Outsourcing & Offshoring: Managing the Security Risks. This document collates the high-level points from the CESG and CPNI guidance, and interprets these in the context of the .

The target audience for this document includes personnel with a requirement to make offshoring decisions; and suppliers who are considering, or currently engaged in, delivery of capabilities with an offshore element.

Background
General

Some suppliers are keen to offshore elements of IT service delivery, due to a perception that this will reap strong financial benefits. Reasons often cited for offshoring decisions include: cost savings in wages and other business expenses relative to the domestic (UK) market; access to specific specialist technical skills; and access to a large labour pool to support peak loading or large-scale projects.

Offshoring is not, however, without its potential issues. Badly managed offshoring of a project can lead to over-runs in project costs and timescales which eclipse any anticipated benefits. In the worst cases, project over-spend, over-run and quality issues can lead to project failure. Also, there are a number of scenarios where offshoring would introduce unmanageable risks; and/or result in a direct breach of UK law; and/or result in unexpected financial exposure for the . These risks are not necessarily a blocker to offshoring, but must be balanced carefully against the anticipated benefits.

Quality, Cost and Time

Offshoring presents a range of ubiquitous project risks which must be considered. There can be a tendency to over-estimate the savings that can be made, and to underestimate the potential configuration management and integration issues. Much of the cost saving from offshore development comes from the labour-cost-differential between the UK and favoured offshore locations. High levels of inflation as those economies expand, often through development as offshore centres, can shrink or even overwhelm any predicted cost savings. This may make the supplier's position

untenable. Cultural differences can also exaggerate normal project stress points that occur during integration and handover of outsourced elements. Customers and suppliers often fail to fully appreciate increased incidental costs, e.g. due to the additional testing overhead incurred. The long delivery chain can also become a difficulty to manage. In some less stable locations, risks due to war, civil uprising and the availability of Critical National Infrastructure also lead to unique business continuity issues.

Legal Risk

Offshore projects may also fall foul of more pedestrian but no less severe risks due to local laws at the offshore location. It is important to ask questions such as: to what extent are the contractual conditions legally binding for an offshore company in a proposed location; how difficult and expensive would it be to mount a legal challenge in the case of contract breach, and is this any less likely to be successful; and who would have priority over information and other assets in the event of a dispute. This is not just an issue which the will face when engaging an offshore supplier directly; it is also an issue that 's suppliers will face, but may not be aware of, when subcontracting elements of delivery.

Risk to "UK PLC"

Many information systems handle HMG Protectively Marked and/or personal and sensitive personal data. These add a number of specific risks exceeding the more usual project risks. Local data protection laws may not provide an appropriate level of legal protection, for the data or data subjects involved, against rogue individuals and criminal groups who misappropriate personal data. This may be more of a problem for countries outside of the European Economic Area (EEA), where the legal framework may not be familiar. Commercially sensitive information may be similarly at risk. Political instability may lead to facilities being over-run, which as well as having business continuity implications may also have severe consequences from potential disclosure of Protectively Marked information. Also, organised criminals are able to operate more actively and openly in some overseas jurisdictions. Such activity may be driven by political or economic advantage. It is not only the physical site but also application development that can present a risk to data. A vulnerability or backdoor, engineered into an application either maliciously or inadvertently, could be used to leak information over an extended period or even indefinitely without being identified. The Open Web Application Security Project (OWASP) presents a list of common vulnerabilities that occur due to careless programming and ineffectual testing. Deliberately engineered vulnerabilities and backdoors are considerably more difficult to identify and address.

Personnel Risks

Most people are reliable and honest. However, for work on systems which will handle sensitive Government information, a small number of unreliable or dishonest individuals can cause a disproportionate amount of harm. It is critical, therefore, to identify such high-risk individuals. Pre-employment screening is a critical element in helping to do this, along with aftercare to balance risks identified during screening, and monitor changes to an individual's status that may affect their reliability. Similarly, legal defences provide a complementary means to deter inappropriate behaviour.

Scope

This document covers offshoring of business activities. Offshoring is defined here to include development or provision of services, from outside the UK or otherwise using non-UK resources, for domestic (UK) consumption.

The scope of offshoring is a broad one. This may involve, for example:

- Development of applications, and/or provision of second-line and/or third-line support for these applications, from non-UK locations and/or by non-UK Nationals.
- Follow-the-sun technical support for commercial products, so that suitable technical resources are available at times when domestic support would be unsociable.
- Remote managed services for wholesale provision of capabilities from non-UK locations and/or by non-UK Nationals.
- Other provision of support to the from non-UK locations and/or by non-UK Nationals.

The scenarios which are to be treated as offshoring are set out in the following bulleted list. This is not necessarily an exhaustive list; in case of uncertainty please contact IT IA for advice: .

Captive centres	Refers to an office that forms part of a Government department but is physically located outside the UK.
Far-shoring	Covers scenarios where development is to be transferred to locations outside of the EEA. Far-shoring may enable more cost-effective development than near-shoring, or may enable access to specific technical skills. However, far-shoring may require additional National Security and/or legislative considerations to be taken into account relative to near-shoring.
Landed resources	Covers scenarios where resources from outside the UK are brought to the UK. This may be, for example, to provide: low-cost labour, specialised skill-sets, and/or support for peak loads. Use of landed resources makes it possible to obtain considerably more control over the working environment of non-UK Nationals on HMG programmes, and can enable a more robust screening and aftercare regime for personnel, traded off against increased development costs.
Near-shoring	Covers scenarios where development is to be transferred to other countries within the European Economic Area (EEA), where legislation on key issues such as data protection, electronic communications and human rights is broadly aligned with UK legislation. It should be noted that although key legislation is broadly aligned across the EEA by a requirement to meet common EU Directives, the legislation that has been implemented by different EEC nations in order to comply with these directives has some important differences.
Other	Any other activity using non-UK locations and/or non-UK Nationals to deliver elements of HMG capability.

Exclusions from Scope

Exclusion 1: This document does not address UK or overseas legislation. The legal team, the Data Access and Compliance Unit (DACU), and the Data Protection EU and International Policy Teams must be consulted on legal issues. Contact for assistance.

Exclusion 2: This document also does not address protection of individuals' personal data, except within the context of HMG Security Policy. The Data Access and Compliance Unit (DACU) must be consulted on personal data, the DPA, and related issues.

With the exception of Landed Resources, deployment to locations within the UK does not count as offshoring and is therefore beyond the scope of this document. It is noted, however, that there will be other geographical factors to be taken into account even within the UK. For example, there are special security arrangements for Northern Ireland, and different freedom of information legislation between England and Scotland. These differences should in no way be considered as a justification not to outsource to other UK locations, but would need to be addressed in the local controls deployed.

Outsourcing is beyond the scope of this document, except insofar as outsourcing arrangements are directly related to offshoring requirements (e.g. contractual obligations to be included in supplier contracts and subcontracts). Outsourcing is defined by HMG GPG6 as:

> a contractual relationship with an external vendor that is usually characterised by the transfer of assets, such as facilities, staff or hardware. It can include facilities management (for data centres or networks), application development and maintenance functions, end-user computing, or business process services.

Document Overview

The remainder of this document is structured as follows:

- The relevant IA Constraints and Considerations for offshoring.
- A checklist of assessment activities at different points in the development lifecycle.

IA Constraints and Considerations
General

There are a number of specific IA Constraints which must be satisfied by any offshoring arrangements. There are also a number of key considerations that must be borne in mind in deciding whether to offshore a particular capability or service.

This section of the document sets out the general IA requirements and constraints that must be complied with when offshoring capabilities. This document is derived from some of the good but generic CESG and CPNI documentation on the subject, outlined in the Further Reading section. This guidance should not be used as a substitute for engagement with the Accreditor or with IT IA, who will be able to provide tailored guidance to support individual decisions; it is intended more as general guidance on policy, to support initial decision-making and project planning.

Accountability

The development or management of a capability can be outsourced, however, ultimate accountability and responsibility for a capability remains with the end-customer for that capability: in this case the . The remains accountable for work performed by third parties on its behalf, whereas outsourcing and offshoring can make it difficult to directly identify and manage information risks and issues. Strong governance and clear lines of accountability and responsibility are required to address this.

REQUIREMENT 1: The remains ultimately responsible for the security and overall delivery of offshore application development and other services. All supplier and subcontractor contracts must ensure that the retains overall control over all security-relevant elements of the delivery. The enforceability of supplier and subcontractor contracts in overseas jurisdictions must be ratified by legal experts.

If a capability is delivered late, is substandard, fails completely or is compromised, then the will need to put measures into place to ensure business continuity while a remedial plan is developed and worked through, otherwise essential public services may not be deliverable in the interim. In some cases, the may find itself financially or legally liable for shortcomings in supplier subcontracts. Also, the rather than the supplier will almost certainly suffer the brunt of any bad publicity.

The core function of the is to deliver services for the general good, rather than commercial commodities. As such, the impact of failure is not quantifiable in purely financial terms. Failure or compromise of services cannot therefore be fully remedied through financial penalties in supplier contracts, although financial penalty clauses can nonetheless serve as a motivation for suppliers to deliver on time and to quality.

The responsibility of the for its own security and overall delivery is reinforced within the HMG SPF, at Paragraph 7, under Roles and Responsibilities:

> Accounting Officers (e.g. Head of Department/Permanent Secretary) have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. This responsibility must be supported by a Senior Information Risk Owner (SIRO) and the day-to-day duties may be delegated to the Chief Security Officer (CSO), IT Security Officer (ITSO), Information Asset Owners (IAOs), supported by the Lead Accreditor.

REQUIREMENT 2: The SIRO remains accountable for information risks, including risks to Protectively Marked and personal data, in an offshore context. These risks must be documented and presented to the SIRO, and must be explicitly agreed to before any contract with an offshore element is accepted. In some cases, a submission to the Cabinet Office IA Delivery Group may be necessary. The Accreditor, IT IA, DACU and Legal experts must be engaged by the project team as soon as a potential offshoring requirement is identified, to enable identification of these information risks. Close engagement with these Special Interest Groups must be maintained for the delivery lifetime. This engagement must be formally set out in the delivery plan.

The will bear the main impact of any compromise of the Confidentiality, Integrity and/or Availability of public services that are delivered or managed on its behalf.

The ultimate decision on whether the IA risk of outsourcing is acceptable will therefore be made by the SIRO, as advised by the IAO and the Accreditor. HMG security policy requires that the SIRO must personal approve all large-scale information-related outsourcing and offshoring decisions. The SIRO is also required to approve the offshoring of personal data sets and, in some cases, submit plans for scrutiny by the Cabinet Office IA Delivery Group. The Accreditor, IA function and SIRO must be involved as soon as a potential offshoring proposal is identified, so that a decision on whether the proposal presents an acceptable level of information risk can be made at the earliest opportunity. This limits the likelihood of nugatory work by the project team.

The requirement for early and ongoing engagement with the Accreditor and IA function is reinforced by HMG GPG6 :

> The risk assessment and treatment plan must be reviewed by the Accreditor and presented to the SIRO at each stage of the procurement process.

Risk Assessment

Before any sensible dialogue can be had around whether or not offshoring is acceptable, the value of the assets to be offshored and the threats for the offshore location and/or personnel must be properly understood. Asset valuation and threat assessment must therefore be conducted as an upfront activity for any proposal, and will require early engagement with all interested parties. Risk assessment must be conducted as an initial activity, and regularly revisited as the project progresses. All threat assessment and risk assessment activities will need to be conducted in collaboration between the supplier as risk manager, and the as the owner of the threat and the risk.

REQUIREMENT 3: All assets and/or activities to be offshored must be identified, and a Threat Assessment for those assets/activities at the proposed offshore location carried out. This includes not only physical and software assets but also information and service assets. The value and business impact of compromise for each information asset must be determined against the HMG Business Impact Table and Business Impact guidelines; valuations must be agreed with the Information Asset Owner for each asset. A Privacy Impact Assessment (PIA) is also required, as discussed further in the following REQUIREMENT 5.

The set of assets to be offshored not only includes any specific capabilities to be developed or managed, but will also include any incidental assets which are required to support these activities. For example:

- Development will require test data and schemas which may in themselves attract a Protective Marking or have other particular sensitivities.
- Some development activities may be deemed to require real or anonymised data, rather than fully synthetic test data, to ensure the robustness of critical applications or to test revised applications against historical data from extant capabilities.

  Wherever it is considered that there may be a requirement to use real or anonymised data, rather than synthetic data, the "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, refer to this guidance.
- Effective application development may require knowledge of real configuration information to support pre-integration-testing activities, or of broader network infrastructure designs in order to tailor and optimise development. Some of this information may attract a Protective Marking or have other particular sensitivities. The information shared with offshore developers should be minimised to the fullest extent that is possible.
- Poor coding practices often result in sensitive information such as network configuration information, user and administrator credentials, and other sensitive details being hard-coded into applications. Support for development, for third-line support and application maintenance, and for upgrades to IT capabilities may therefore necessitate some unavoidable access to sensitive information for which there is no specific need-to-know by the development or maintenance team.

REQUIREMENT 4: Sensitive assets and/or activities should not be offshored to Countries where Special Security Regulations Apply, or to Countries in which there is a Substantial Security Threat to British Interests.

It is the policy of the that Protectively Marked or otherwise sensitive assets, and development or support activities relating to these assets, should not be offshored to Countries where Special Security Regulations Apply, or to Countries in which there is a Substantial Security Threat to British Interests. The ITSO can provide further details of these, on a need-to-know basis, in response to specific requests. It is the policy of the that activities involving Protectively Marked or otherwise sensitive information should not be offshored to these locations. In cases where there is an exceptionally compelling business case for offshoring to one of these locations, the ITSO must be

consulted and will advise the business on suitability, weighing up all of the relevant factors and assessing the extent to which the proposed compensating controls mitigate the risk.

REQUIREMENT 5: assets and/or activities should not be offshored to countries where political stability, practical considerations and/or legal issues (e.g. compliance with the DPA) may result in a significantly-beyond-baseline risk to the confidentiality, integrity and/or availability of Protectively Marked or other sensitive data, or where there is not an adequate level of protection for the rights of data subjects in relation to their personal data.

Not all countries which have issues with political and/or economic instability are listed as CSSRA or Substantial Security Threat countries. There are several other countries that are not on the list which nonetheless present a high risk for offshore development and operations. These countries should be avoided on the general principle of avoiding development environments where the local threat is significantly more than baseline. Also, as discussed previously, the CSSRA and the list of Substantial Security Threat countries change from time to time. By not offshoring in unstable locations, the risk of outsourcing to a country that subsequently ends up on one of these lists is reduced.

In addition to the previous points, there are some politically stable locations where it is nonetheless difficult or impossible to meet other essential requirements for the handling of Protectively Marked or other sensitive data (e.g. personal data). Inability to assure the identity and history of personnel, and local legislation on disclosure of data (for example, in response to local FoI or law enforcement obligations), are common examples which can lead to issues with screening and with retaining control of information.

In addition to countries with political and/or economic issues, as discussed previously, there may also be threats and risks as a result of other nations' legal systems. Legal constraints in some countries may:

- Conflict with IA requirements under the HMG SPF and supporting guidance;
- Conflict with requirements under the Data Protection Act (DPA) and/or other UK Law; and
- Expose the to untenable legal liabilities in the event that something goes wrong.

A particular consideration for offshoring is DPA Principle 8: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

Legal advice must be engaged, separately to IA advice, to identify any potential legal issues in advance of making any offshoring decision.

REQUIREMENT 6: An information risk assessment for each offshore location must be conducted by the Offshoring Company or organisation. This risk assessment must be subject to review and acceptance by IA. This should include an IS1 Risk Assessment, an assessment against ISO27001 controls, and a "Delta Assessment" setting out any HMG requirements that may be unenforceable, any variations to HMG policy that may be required, and how it is proposed to address these Deltas. A Privacy Impact Assessment (PIA), taking into account local legal considerations at the offshore location, must also be conducted. The risks, and the costs of mitigating the risks, must be balanced against the benefits to be gained from outsourcing. A Risk Management Plan must be developed and maintained to identify the mitigations required to address offshoring risks and estimate the costs of implementing these mitigations.

An information risk assessment for the offshore location must be conducted. This must include an IS1 Risk Assessment in line with current HMG guidance. It must also include an assessment of physical, procedural, personnel and technical measures at the offshore location set against the ISO27001 requirements and highlighting the additional controls in place to address the concerns set out within HMG Good Practice Guide 6 for specific ISO27001 controls. It must also include a "Delta Assessment" setting out any HMG requirements that may be unenforceable, any variations to HMG policy that may be required, and how it is proposed to address these deltas.

The high-level information risk assessment is required at the proposal stage, prior to contract negotiations. This must be developed incrementally into a more detailed risk assessment as the project progresses. This risk assessment must take into account all assets to be offshored and the specific Threat Assessment for the offshore location and/or personnel. The risk assessment must meet the requirements of both HMG IS1 and HMG GPG6. The requirements of HMG IS6 relating to personal data can be more difficult to meet in an offshore context, so particular care must be taken to ensure that the PIA takes the offshore location into account and offshore elements of the contract are compliant with IS6.

A Risk Management Plan is essential to address the risks identified through offshoring. As well as providing evidence that the supplier has adequately considered these risks, this will also provide the basis for estimating the cost overhead

of mitigating offshoring risks, enabling a more accurate assessment of whether offshoring truly represents value for money. For example, the cost of provisioning a suitably segregated technical environment to support offshore development work; combined with the cost of providing a suitably secure link to enable remote access for offshore workers; and the cost of sending out suitably trained personnel for regular inspections of an overseas site; may significantly erode any cost savings.

Supplier Arrangements

REQUIREMENT 7: IA constraints and requirements for offshoring must be made clear to suppliers prior to contract award and explicitly set out in contractual arrangements with suppliers to the . These constraints and requirements must be flowed down to all subcontractors along the chain of supply. Conversely, Intellectual Property Rights must flow up contractually from the offshore supplier or suppliers to the .

IA requirements must be determined as an integral part of the initial requirements for any capability, and an assessment of competing solutions against IA requirements must be a critical part of supplier selection during the tender process. Offshoring is no exception to this. Offshoring constraints and requirements must be made clear to suppliers prior to contract award, so that there can be no ambiguity during costing for any solution to be delivered to the . There will almost certainly be additional time, effort and cost involved to implement the required physical controls, testing and decommissioning activities required to meet IA requirements in an offshore development environment.

Some suppliers with UK bases may wish to offshore and/or subcontract elements of their contracts with the . If elements of a contract have been offshored to a subcontractor working in one location, that subcontractor may themselves wish to offshore elements of their subcontract to a different offshore location. IA constraints and requirements must be applicable to all of those who are party to the contract. For example, an offshore organisation based in Country A, which provides second-line support for an application from Country A, might rely on teams from its offices in Country B to conduct development and third-line support activities. This would have an impact on the Threat Assessment and hence the risks to the capability.

The is responsible for all offshore activities that are being conducted on its behalf, and must retain oversight of these activities. This requirement must be enforced within supplier contracts, through robustly worded requirements for contractual flow-down of IA responsibilities through the supplier chain. The must be given both visibility and an over-riding right of approval or veto for subcontractor arrangements. A right of audit without warning must be maintained by the , including full access to all physical sites, logical capabilities, accounting logs, etc.

Ownership of all information assets, and all Intellectual Property Rights, developed as part of contracts must flow up to the . All information, including vestidual information, which is held on a supplier's physical assets, must be erased and/or disposed of to the satisfaction of IT IA during decommissioning. Again, legal limitations on the enforceability of contractual conditions in some locations must be taken into account and specialist legal advice will be required to ensure that all necessary contractual conditions are enforceable at offshore development locations.

The previous issues with contractual flow-down of responsibilities and flow-up of ownership are best managed if the retains control of the subcontract chain. Ideally, wherever practicable, supplier contracts should only allow further subcontracts to be let with the explicit permission of the . This enables the cost and complexity of due-diligence checking and contractual enforcement, not just for offshoring considerations but also more generally, to be more effectually bounded and controlled.

REQUIREMENT 8: Suppliers must ensure that offshore development is conducted according to UK and other relevant IA standards and legislation.

The requirements of the HMG SPF must be adhered to for offshore development. This may require significant changes to local working practices in some cases. The requirements of other relevant British and International standards must also be adhered to. Most notably for IA considerations, this specifically includes ISO27001 (Information Security Management System) and ISO25999 (Business Continuity). Offshore sites and processes must be demonstrably compliant with ISO27001, and must be subject to a combination of scheduled and snap audits to ensure this. In addition to all of the usual ISO27001 conditions, particular considerations for offshore development are set out within HMG GPG6. Any issues found during audit must be addressed over timescales that are agreeable to IT IA, with formal progress tracking of issues as they are addressed and resolved. Business Continuity can introduce particular issues in some offshore contexts, where events such as natural disasters, pandemics, criminal activity, acts of war, etc. may be sufficiently probable to merit more rigorous mitigations than for UK development. Factors such as staff turnover may also present particular issues in an offshore context, particularly where Landed Resources are used.

REQUIREMENT 9: The robustness of development and integration testing activities must be reconfirmed. Regular development and integration testing activities by the System Integrator are particularly essential for offshoring, where there will potentially be less visibility or direct control over the development environment. Additional code review must also be conducted to a level that is agreed by IT IA to be commensurate with the value of the information that will be handled by the live application, or otherwise accessible to the live application.

REQUIREMENT 10: Security Enforcing Functionality elements of applications must not be offshored. For other elements of application code which process, store and transmit sensitive information assets, an onshore security code review must be conducted. This should be to a level that is agreed by IT IA to be commensurate with the value of the information handled by the live application, or otherwise accessible to the live application. This is likely to include a combination of manual and automated testing, and should be supplemented by a more comprehensive ITHC scope where appropriate.

The basic principle of ensuring thorough testing during every stage of application development must be reinforced where elements of development and/or maintenance are to be offshored. Requirements for testing against internationally recognised standards (e.g. the OWASP standard for secure code development) must be secured in supplier contracts and flowed down to offshore and other subcontractors. A test data strategy must be agreed prior to contract award. A high-level test strategy must also be agreed prior to contract award, and should be developed and maintained as a living plan as the project evolves. There should be assurance that provision for testing is adequate to mitigate the Information Assurance and other System Integration risks identified.

Testing, including security testing, must be conducted at every stage of the development (unit testing, integration testing, acceptance testing, etc). The must retain executive control over the testing process, maintaining visibility of all test results and progress on remedial activities. This includes control by IT IA over security elements of testing. The must be contractually able to exert control over testing, through clauses to reject as substandard any delivery where test scopes are not agreed by the , where results are not fully disclosed or where remedial activities are deemed to be insufficient.

Some applications which are deemed to be relatively low value in themselves may be used to handle information with a significantly higher value, or may be able to easily access sensitive information (for example, other information within the same business domain or information that is directly accessible from connections to servers in other business domains). Additional code review must also be conducted as part of the development testing of these applications, with particular emphasis on Security Enforcing elements of the application. In some cases, the Accreditor and the IA Team may require the use of automated test tools and/or line-by-line code review for elements of the application to be conducted by UK Security Cleared personnel at onshore locations.

In some cases, the additional testing overhead required will outweigh the benefits gained by offshoring. This is most likely for particularly complex and/or sensitive applications. Back-doors and vulnerabilities become increasingly easy to engineer (either deliberately or accidentally) for complex applications, and increasingly difficult to identify. Based on experience, it is likely that suppliers will underestimate the true time and expense that would be necessary to test complex applications. It is important that supplier proposals are realistic about the benefits of any offshoring elements of the proposals, and have accommodated realistic costs for testing to address offshoring risks. Where test costs are not realistic, this does not represent a cost saving for the . If the supplier is not making an acceptable profit on a contract, then relationships between the supplier and the will undoubtedly deteriorate. The supplier is likely to try to recoup losses by streamlining test processes (driving operational risk); by reclaiming costs from elsewhere (driving project cost); or by delivering less than expected or not at all (driving project risk). Such unrealistic proposals should be either corrected or rejected during supplier selection and contract award.

Use of Landed Resources

REQUIREMENT 11: Where landed resources are used to support project activities they must be vetted to a level appropriate for the value of the information assets and collateral assets that will potentially be available to them. Where it is not possible to meet some BPSS evidence requirements, suitable alternative evidence must be obtained and compensating controls such as technical lockdown, supervision and monitoring must be applied. If it is not possible to lock down the physical environment to the satisfaction of IT IA then landed resources must not be used. For higher levels of clearance such as SC, if a landed resource cannot achieve the required level of clearance or if there are prohibitive conditions on the individual's clearance, then that landed resource must not be used.

The most basic level of Government security checking, the Baseline Personnel Security Standard (BPSS) check, is designed to provide an assessment of three key features of the individual to be vetted: their identity; their right to work; and the reliability, integrity and honesty of those individuals.

The BPSS requires that an individual's identity be confirmed, by matching some evidence of identity such as a passport or drivers licence, with evidence of address and activity in the community such as bills and bank statements. This provides a level of information that can be followed up for UK applicants if an individual raises any particular concerns. Further checks can be cheaply and easily conducted, to provide additional evidence that an individual with the asserted identity and address exists, and to confirm that the individual asserting that identity and address is not attempting identity theft. Where individuals originate from outside of the UK, and have not been in the UK for a suitably long period of time, it can be more difficult to obtain a suitably reliable history for those individuals (long-term footprint) to support effective screening. The Baseline Standard requires at least three years' worth of previous employment history. From experience, it is considered that a commensurate length of time is also required to build up a suitably rich credit history and social footprint to enable reliable checks to be conducted.

Even confirming an individual's true identity may be problematic in some non-EU locations, where proofs of identity may be non-existent or considerably less reliable. It should also be noted that, for countries where record-keeping is managed locally rather than centrally, engagement at a local level to support checks can very quickly become prohibitively expensive for a moderately-sized workforce and/or where there is a high rate of staff turnover.

Personal and employers' references are used, partly to support confirmation of identity, and partly to enable checking of an individual's reliability, integrity and honesty. Criminal records declarations and supporting criminal records checks are also used as part of BPSS clearance. Criminal record checks for UK citizens are generally comprehensive and accurate. However, the accuracy of police and criminal records checks varies widely between different countries. The CPNI has compiled information on such checks for a reasonably broad set of overseas jurisdictions. The CPNI documentation also provides useful information on the reliability of identify checks overseas. A risk-balance decision by the SIRO is likely to be required on whether to accept the additional BPSS vetting risk for the offshore workforce.

To compensate for any shortcomings or uncertainty in vetting, landed resources brought to the UK are likely to require a heightened level of monitoring and supervision, as well as additional technical measures to limit and audit their physical and logical access to HMG information systems. HMG information systems to which landed resources have access must be locked down and supported by tight access controls exceeding the usual HMG baseline.

Where higher levels of clearance such as SC are required it may not be possible for a specific landed resource to achieve the required level of clearance, or there may be prohibitive conditions on the individual's clearance. In those cases, the specific landed resource must not be used. For example, a non-UK National who has been within the UK for a sufficiently long period of time may be able to obtain an SC clearance. However, if a role requires handling of UK Eyes Only material, then the prohibitions on the SC clearance for that non-UK national would make them inappropriate to use for that role.

In exceptional circumstances, the use of landed resources from countries where Special Security Regulations Apply, or to countries in which there is a Substantial Security Threat to British Interests, depending on why that specific country is on the list. The ITSO should be consulted in such cases and will advise the business on suitability, weighing up all of the relevant factors and assessing the extent to which the proposed compensating controls mitigate the risk.

Assessment Activities

Every offshoring decision must be made on a case-by-case basis, after balancing all of the facts of the situation. The project activities required to ensure this are set out as follows.

REQUIREMENT 1 and REQUIREMENT 2
Project Scoping & Supplier Selection

Project Team:

- Ensure that the SIRO, Accreditor, IT IA and Central IA are engaged from project conception.
- Ensure that any contracts which may require personal data to be offshored outside of the EEA include suitable contractual clauses developed from reliable templates. For example, for personal data transferred outside of the EEA, the European Commission approved model clauses as per Directive 95/46/EC of the European Parliament and of the Council, provides a useful template. The legal framework for managing the export of Protectively

Marked information must be no less restrictive than this. Consider whether additional contractual clauses are required to mitigate risk and avoid legal problems arising from local laws and jurisdictional issues.

- Ensure that offshoring elements of all Invitation To Tender (ITT) or other supplier requirements documentation are developed in consultation with Legal functions, DACU, and the Accreditor and IT IA. Ensure that these parties are key reviewers for all tender requirements.
- On the advice of the Accreditor, DACU, IT IA, and Central IA, present and obtain approval for a SIRO Submission comprehensively setting out the risks and mitigations of any offshoring proposals.
- Understand and advise the SIRO of any requirement that may exist for a submission to the Cabinet Office IA Delivery Group. Prepare any required submission on behalf of the SIRO, for approval.
- Ensure that the operational assessment and investment appraisal of competing supplier proposals factors in the additional IT IA effort requirement to address offshore elements of the proposal, as per the following Requirement 11.
- Reject any bids that do not meet IA, DACU or Legal requirements for offshoring.

Accreditor/IA:

- Develop the elements of tender requirements which cover offshoring constraints and requirements.
- Review outsourcing elements of supplier bids and other proposals.
- Advise the Project Team on the suitability of offshoring proposals.

Note: IA includes both IT IA and the Central IA team. Both IA functions should be kept informed and engaged about offshoring proposals.

Contract Award

Project Team:

- Ensure that offshoring requirements and constraints are worked up to a robust level of detail within the final supplier contract, and subject to a further round of review by the Accreditor and IT IA prior to acceptance and contract award.
- Update any SIRO Submissions and submissions to the Cabinet Office IA Delivery Group to reflect the changes in the information risk between project scoping and contract award. Obtain acceptance for any changes from the SIRO prior to acceptance and contract award. Engage IT IA to advise and liaise with the SIRO.

Accreditor/IA:

- Provide review support and remedial input to the Project Team.

Development

Project Team:

- Use supplier audit as a mechanism to ensure that contractual requirements are being met. Where supplier indiscretions are found enforce remedial action.
- Where remedial action is not implemented, or ineffectually implemented, invoke contractual penalty clauses.
- Add and maintain any submissions to the SIRO and the Cabinet Office IA Delivery Group as necessary. Engage IT IA to advise and liaise with the SIRO.

Accreditor/IA:

- Provide review support, remedial input and recommendations to the Project Team.

In-Service & Beyond

Service Management:

- Use supplier audit as a mechanism to ensure that contractual requirements are being met. Where supplier indiscretions are found enforce remedial action.
- Where remedial action is not implemented, or ineffectually implemented, invoke contractual penalty clauses.
- Add and maintain any submissions to the SIRO and the Cabinet Office IA Delivery Group as necessary. Engage IT IA to advise and liaise with the SIRO.

Accreditor/IA:

- Provide review support, remedial input and recommendations to the Project Team.

REQUIREMENT 3

Project Scoping & Supplier Selection

Supplier:

- Identify what hardware, software and information assets need to be offshored.
- Set out asset valuations for the Confidentiality, Integrity and Availability of all assets. Core information assets must be valued according to the SAL and clarification sought for any ambiguities. Collateral information assets (crypto, credentials, etc) must be valued in line with and HMG guidance.
- Asset valuations for all hardware and software assets must be clearly justified in the proposal documentation, and submitted to the Accreditor for review.

Project Team:

- Ensure that supplier proposals include unambiguous asset valuations. Request clarification on any points of ambiguity. Ensure that the Information Asset Owner(s), the Accreditor and IT IA are engaged on an on-going basis.
- Reject any proposals that do not meet with Requirement 3.

Accreditor/IA:

- Ensure that a clear and detailed SAL is generated on a per-project basis, setting out the valuations for all information assets.
- Review hardware, software and asset valuations on supplier proposals.

Contract Award

Project Team:

- Ensure that the supplier contract includes an explicit requirement to develop and maintain hardware, software and information asset registers. The requirement should explicitly stipulate that registers be maintained in the standard format, or in an equivalent format which contains (as a minimum) all of the information in the standard format. Ensure that the supplier is supplied with a copy of this standard format in advance of contract award, so that they can take any additional overheads into account in their proposal.
- Ensure that the supplier contract includes a right of audit, including no-notice audit, by the . The scope of audit must encompass hardware and software asset registers, all hardware and software assets, and all other elements related to the provision (physical sites, personnel, etc.)

Service Management:

- Maintain a standard format for hardware and software asset registers.

Development

Supplier:

- Develop and maintain hardware, software and information asset registers, covering all hardware, software and information assets. This must be developed in the standard format, or in an equivalent format which contains (as a minimum) all of the information in the standard format.

Project Team:

- Maintain visibility of the hardware, software and information asset registers. Ensure that there is a regular joint (supplier/) activity to audit physical and software assets against these registers. Conduct irregular spot audits of assets against the registers. Ensure that remedial activity is time-lined, tracked and completed according to schedule by the supplier.

Accreditor/IA:

- Advise physical and logical audit of assets, and remedial activity.

In-Service & Beyond

Supplier:

- Ensure that the hardware, software and information asset registers are maintained as part of an ITIL service wrap for the delivered service. This must be maintained in the standard format, or in an equivalent format which contains (as a minimum) all of the information in the standard format.

Service Management:

- Maintain visibility of the hardware, software and information asset registers. Ensure that there is a regular joint (supplier/) activity to audit physical and software assets against these registers. Conduct irregular spot audits of assets against the registers. Ensure that remedial activity is time-lined, tracked and completed according to schedule by the supplier.

Accreditor/IA:

- Advise physical and logical audit of assets, and remedial activity.

REQUIREMENT 4 and REQUIREMENT 5

Project Scoping & Supplier Selection

Supplier:

- Ensure that any potential requirements to offshore any elements of service delivery are explicitly communicated with the as part of the tender response.

Project Team:

- Ensure that suppliers are explicit about any proposals for offshoring any elements of the delivery when they develop their bids to supply a capability.
- Ensure that the Accreditor, the IA Team, DACU and Legal advisors are aware of any potential requirements to offshore elements of the delivery.
- Work with the Accreditor and IT IA to identify and resolve any potential IA issues for work at these offshore locations or involving personnel from these locations.
- Work with DACU to identify and resolve any potential DPA issues for work at these offshore locations or involving personnel from these locations.
- Obtain confirmation from Legal Advisors that work at these offshore locations or involving personnel from these locations will not cause any potential conflict with UK Law or leave the exposed to any additional legal liability.
- Reject any proposals that do not meet with Requirement 4 or Requirement 5.

Accreditor/IA

- Advise the project team on any potential offshoring problems and unacceptable offshoring proposals, and recommend mitigation options where necessary.

Contract Award

Project Team:

- Ensure that the supplier contract explicitly prohibits offshoring except where locations and controls are explicitly set out within the contract.
- Ensure that the contract prohibits offshoring to CSSRA and Substantial Security Threat countries, and any other identified problem countries, and that the contract contains flow-down provisions of all offshoring constraints for all subcontracts.
- Ensure that the supplier contract includes a requirement to consult the before offshoring any elements of the delivery except where explicitly set out in the contract.
- Ensure that the Accreditor and IT IA are critical reviewers for all supplier contracts with an offshoring requirement.

Accreditor/IA:

- Advise the Project team on what countries are currently on the lists, and advise on exceptions on a case-by-case basis.
- Review offshoring elements of supplier contracts.

Development

Supplier:

- Ensure that any potential emerging requirement to offshore any elements of delivery are communicated immediately to the .

Project Team:

- Deal with any emerging requirements on a case-by-case basis, through engagement with the Accreditor, the IA Team, DACU and Legal advisors, and Information Asset Owners.

In-Service & Beyond

Supplier:

- Ensure that any potential emerging requirement to offshore any elements of delivery are communicated immediately to the .

Service Management:

- Deal with any emerging requirements on a case-by-case basis, through engagement with the Accreditor, the IA Team, DACU and Legal advisors, and Information Asset Owners.

REQUIREMENT 6

Project Scoping & Supplier Selection

Supplier:

- Conduct an initial IS1 Risk Assessment, In line with the -provided threat assessment, which includes offshoring risks. This must include an HMG GPG6 compliance assessment, highlighting specific low-level risks due to any offshoring proposals, as part of the overall proposal to supply a capability.
- Develop a specific Risk Management Plan to address offshoring threats and risks, detailing how these identified will be mitigated. The Risk Management Plan must provide an estimate of the costs required to implement the proposed mitigations, and any consequent issues that may arise.
- Conduct a Privacy Impact Assessment (PIA) for the proposed solution, including an assessment of the PIA requirements covering the elements of information to be outsourced and documenting how the proposals meet these requirements.

Project Team:

- Ensure that suppliers are aware of the requirement to include an IS1 Risk Assessment, HMG GPG6 compliance, and supporting low-level risk assessment.
- Reject any proposals that do not contain a PIA, or which contain a PIA that is deemed by DACU, the Accreditor, or IT IA to be inadequate.
- Reject any proposals that do not contain a risk assessment, or which contain a risk assessment that is deemed by the Accreditor and IT IA to be inadequate.
- Reject any proposals where the mitigations proposed in the Risk Management Plan are deemed by the Accreditor and IT IA to be inadequate, or the costs of implementing those mitigations are deemed by the Security Architecture Team to be unrealistic.

Accreditor/IA

- Develop bespoke threat assessments and advice for any proposed offshore locations and for use of non-UK personnel for development. Engage with the UK Security Authorities as necessary to support this.
- Review Risk Assessment elements of supplier proposals.

Contract Award

Project Team:

- Ensure that the supplier contract includes terms requiring the supplier to update the Risk Assessment and Risk Management Plan, including offshoring considerations, immediately following contract award and maintain this as a through-life activity. As a minimum, the supplier should be required to update the risk assessment (and have

this approved by the) for any contract change and as part of the acceptance criteria for each distinct phase of the development.
- Ensure that the Accreditor and IT IA are critical reviewers for all supplier contracts with an offshoring requirement.
- Ensure that the outcomes of the PIA are folded into the supplier contract.
- Ensure that the project budget includes a suitable level of contingency to accommodate any changes in offshoring costs due to change in Threat Assessment for the offshore environment.

Accreditor/IA:

- Review offshoring elements of supplier contracts, including the terms and conditions surrounding risk assessment.

Development

Supplier:

- Maintain the risk assessment, including offshoring considerations, in line with contractual requirements.
- Ensure that offshoring arrangements do not break obligations arising from the PIA.
- Maintain the Risk Management Plan, including offshoring considerations, in line with contractual requirements.

Project Team:

- Ensure that suppliers meet their contractual obligations regarding risk assessment and PIA.

Accreditor/IA

- Provide support for any required review of the supplier risk assessment, including offshoring considerations, in line with contractual requirements.

In-Service & Beyond

Supplier:

- Maintain the risk assessment, including offshoring considerations, in line with contractual requirements.
- Ensure that offshoring arrangements do not break obligations arising from the PIA.
- Maintain the Risk Management Plan, including offshoring considerations, in line with contractual requirements.

Service Management:

- Ensure that suppliers meet their contractual obligations regarding risk assessment and PIA.

Accreditor/IA

- Provide support for any required review of the supplier risk assessment, including offshoring considerations, in line with contractual requirements.

REQUIREMENT 7
Project Scoping & Supplier Selection

Supplier:

- Identify any potential offshoring requirement as soon as possible in the tender process. Where proposals include an element of offshoring, it must be explicitly stated in the supplier's response to the security requirements. This must explicitly state how security will be maintained in an offshore context (including responses to User Security Requirements, System Security Requirements, etc.)

Project Team:

- Ensure that supplier proposals to deliver a capability are demonstrably compliant with offshoring security requirements.
- Reject any proposals that the Accreditor and IT IA deem to either not address security requirements comprehensively enough or not give sufficient weighting to these requirements.

Accreditor/IA:

- Engage with the Project Team and the supplier to support development and assessment of security requirements, including offshoring requirements, for the capability.

Contract Award

Project Team:

- Ensure that the supplier contract specifically mandates compliance with all offshoring security requirements.
- Ensure that the supplier contract mandates blanket flow-down of all contractual constraints and obligations to all of the suppliers' suppliers, all of the way down the supply chain.
- Ensure that the contract makes provision for routine and no-notice audit of supplier compliance with offshoring requirements, at any-and-all supplier locations and subcontractor locations that are relevant to the work.

Accreditor/IA

- Support the Project Team in the development of contractual requirements around offshoring. Review contractual clauses relating to offshoring.

Development

Supplier:

- Inform the upfront if any emerging requirements develop to offshore elements of the solution. Demonstrate how these requirements will be compliant with contractual obligations, and highlight and contractual obligations that would need to be relaxed in order for the proposal to work, balancing this against the potential benefit and considering a range of practicable options (as determined through engagement with the Project Team, the Accreditor and IT IA. Work with to ensure that this can be managed in a secure way.

Project Team:

- Retain engagement with the Accreditor and IT IA for all aspects of the project development relating to offshoring.

Accreditor/IA:

- Provide support to the Project Team on offshoring, including direction for audit, remediation and emerging requirements as necessary.

In-Service & Beyond

Supplier:

- Inform the upfront if any emerging requirements develop to offshore elements of the solution. Demonstrate how these requirements will be compliant with contractual obligations, and highlight and contractual obligations that would need to be relaxed in order for the proposal to work, balancing this against the potential benefit and considering a range of practicable options (as determined through engagement with the Project Team, the Accreditor and IT IA. Work with to ensure that this can be managed in a secure way.

Service Management:

- Retain engagement with the Accreditor and IT IA for all aspects of ongoing development (e.g. third-line support) relating to offshoring.

Accreditor/IA:

- Provide support to the Project Team on offshoring, including direction for audit, remediation and emerging requirements as necessary.

REQUIREMENT 8
Project Scoping & Supplier Selection

Supplier:

- Ensure that proposals include an explicit assessment of compliance (including any points of non-compliance) of offshoring elements of proposals with relevant Legislation and Standards. This includes: the DPA and other relevant legislation; the HMG SPF and supporting documentation (specifically, but not exclusively, HMG IS6, HMG GPG6 and the SPF MRs themselves); relevant ISO standards (most notably ISO27001 and ISO25999); Cabinet Office Guidance on IT Offshoring; and local IA Requirements.

- Ensure that named CLAS Consultant resources are used on the supplier proposal to ensure that this proposal addresses all relevant HMG IA requirements and documentation (including offshoring requirements), and is compliant with these.

Project Team:

- Ensure that IA Requirements are made available to suppliers, and that they are aware of their obligations to explicitly demonstrate compliance with offshore elements of their proposals against these.

Accreditor/IA:

- Engage with the Project Team and Supplier security resource to review supplier bids for compliance with HMG IA requirements and documentation (including offshoring requirements).

Contract Award

Project Team:

- Ensure explicit supplier compliance with all relevant identified legislation and standards (as per the list set out in the previous column, plus any other relevant standards identified during the tender process) are set out in the contract.
- Ensure IA are engaged in the procurement process, and that IA concerns relating to offshoring elements of the contract are addressed to the satisfaction of the Accreditor prior to awarding the contract.

Procurement:

- Support the Project Team in the development of contractual requirements around offshoring. Review contractual clauses relating to offshoring.
- Ensure IA are engaged in the procurement process, and that IA concerns relating to offshoring elements of the contract are addressed to the satisfaction of the Accreditor prior to awarding the contract.

Development

All:

- As per the previous Requirement 7.

In-Service & Beyond

All:

- As per the previous Requirement 7.

REQUIREMENT 9 and REQUIREMENT 10
Project Scoping & Supplier Selection

Supplier:

- Ensure that the proposal includes provision for through-development testing, including security testing. Demonstrable compliance with the OWASP Testing Guide (downloadable from the OWASP web-site) is encouraged. The level of security testing required must be agreed with the Accreditor, and will need to be directly commensurate with the risk involved.

Project Team:

- Ensure that suppliers are aware of the requirement for testing, including not only functional testing but also security testing. Reject any proposals that do not make provision for this.
- Ensure that supplier proposals are realistic about the benefits of any offshoring elements of the proposals, and have accommodated realistic project costs and timescales for testing to address offshoring risks. Conduct an internal sanity check of supplier estimates for security and other testing. Reject any proposals where cost or time estimates are unrealistic.

Accreditor/IA:

- Support assessment of functional and security testing proposals.

Contract Award

Project Team:

- Ensure that the contract requires the supplier to test the solution against internationally recognised standards at all stages of the development (unit testing, integration testing, acceptance testing, etc). Suppliers must be contractually required to agree test scopes, including security test scopes, with the before the start of testing. The must be contractually entitled to visibility of all test results and progress on remedial activities to the . Ensure that the scope of testing in the contract includes security testing of the solution, at a level agreed with the Accreditor and the IA Team.
- Ensure that the contract retains executive control over the test process by the , with the ability to reject substandard delivery, require remediation and enforce contractual penalty clauses.

Accreditor/IA:

- Review offshoring elements of supplier contracts, including test arrangements. Provide input to the Project Team as required to support contractual terms for test, particularly security elements of testing.

Development

Supplier:

- Maintain a regular forum with the Project Team to discuss progress against test requirements and milestones, exceptions and remedial planning.

Project Team:

- Ensure that the Accreditor and IT IA are involved in test forum(s) during development. Proactively track progress of remedial action against test defects.

Accreditor/IA:

- Support test review and remedial activities.

In-Service & Beyond

Supplier:

- Maintain a regular forum with the Project Team to discuss progress against test requirements and milestones, exceptions and remedial planning.

Service Management:

- Ensure that the Accreditor and IT IA are involved in test forum(s) during development. Proactively track progress of remedial action against test defects.

Accreditor/IA:

- Support test review and remedial activities.

REQUIREMENT 11

Project Scoping & Supplier Selection

Supplier:

- Ensure that any proposal to use landed resources is clearly stated. Ensure that any associated costs and risks are identified.
- Where landed resources are to be used, ensure that the proposal clearly sets out what information assets and collateral assets would be made available to those resources, how many landed resources are proposed, from where, what level of clearance would be required, and how clearance information requirements would be satisfied.
- Where clearance is not possible to an equivalent level for a landed resource as for a UK resource, identify what the additional residual risks of this will be, how it is proposed to mitigate these risks. The proposal should identify any practical difficulties with these arrangements and how they will be overcome, as well as setting out the additional costs involved.

Project Team:

- In liaison with the Accreditor and IT IA, ensure that proposals for using Landed Resources are realistic.
- Ensure that the costs associated with the use of landed resources have been fully considered in the proposal.
- Reject any unrealistic or un-costed proposals for use of Landed Resources.

Accreditor/IA

- Support assessment of security risk and residual risk with supplier proposals to use landed resources.
- Advise on the feasibility of using landed resources from high-threat countries if relevant.

Contract Award

Supplier:

- Ensure that use of landed resources is in line with contractual requirements.

Project Team:

- Ensure that the supplier contract includes provision to enforce suitable security controls surrounding landed resources, as agreed during supplier selection.
- Ensure that the project budget includes a suitable level of contingency to accommodate any changes in offshoring costs due to change in Threat Assessment for landed resources.

Accreditor/IA:

- Review offshoring elements of supplier contracts.

Development

Supplier:

- Ensure that all landed resources are vetted to a level commensurate with the value of the information to be handled by that landed resource. Where it is not possible to effectively vet a landed resource to the required level, landed resources must not be used.
- Inform the immediately if resource requirements change.

Project Team:

- Ensure that the Accreditor and IT IA are kept fully informed of any change in supplier requirements, and that no change in Landed Resource requirements is agreed without the explicit approval of the IA Team.
- Ensure that the supplier is kept fully informed of any change in Threat Assessment relating to landed resources and of the impact on project delivery.

Accreditor/IA

- Ensure that the Project Team are made aware of any change in Threat Assessment relating to Landed Resources, and of how this will impact the project.

In-Service & Beyond

Supplier:

- Ensure that all landed resources are vetted to a level commensurate with the value of the information to be handled by that landed resource. Where it is not possible to effectively vet a landed resource to the required level, landed resources must not be used.
- Inform the immediately if resource requirements change.

Service Management:

- Ensure that the Accreditor and IT IA are kept fully informed of any change in supplier requirements, and that no change in landed resource requirements is agreed without the explicit approval of the IA Team.
- Ensure that the supplier is kept fully informed of any change in Threat Assessment relating to landed resources and of the impact on project delivery.

Further Reading

Title	Version / Issue
CPNI Personnel Security in Offshore Centres	04/2009
CPNI Good Practice Guide: Outsourcing: Security Governance Framework for IT Managed Service Provision	02/08/2006
CESG Good Practice Guide 16: Taking and Using Cryptographic Items Overseas	Issue 1.0, 08/2009
CESG Good Practice Guide 23: Assessing the Threat of Technical Attack Against IT Systems	Issue 1.0, 04/2010

Notes

http://www.owasp.org

Wherever it is considered that there may be a requirement to use real or anonymised data, rather than synthetic data, the "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, refer to this guidance.

A particular consideration for offshoring is DPA Principle 8: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

For example, an offshore organisation based in Country A, which provides second-line support for an application from Country A, might rely on teams from its offices in Country B to conduct development and third-line support activities. This would have an impact on the Threat Assessment and hence the risks to the capability.

The Baseline Standard requires at least three years' worth of previous employment history. From experience, it is considered that a commensurate length of time is also required to build up a suitably rich credit history and social footprint to enable reliable checks to be conducted.

http://www.cpni.gov.uk/advice/personnel-security1/overseas-criminal-record-checks/

For example, for personal data transferred outside of the EEA the European Commission approved model clauses as per Directive 95/46/EC of the European Parliament and of the Council, provides a useful template. This can be found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF. The legal framework for managing the export of Protectively Marked information must be no less restrictive than this.

IA includes both IT IA and the Central IA team. Both IA functions should be kept informed and engaged about offshoring proposals.

The additional costs for offshore proposals will include potentially significant additional costs for IA and Accreditor resources to support bid assessment, solution review, initial Accreditation, re-accreditation and through-life support. An increased requirement for IA engagement and design scrutiny will be inevitable, and would need to be determined by IA. Activities such as audit and remediation are likely to involve an increased time overhead and travel expenses (e.g. for physical site visits to remote sites at overseas locations to conduct audits and follow-up remediation). Other additional project and in-service assurance is almost certain to be necessary.

Public Sector DNS

The service

The UK Public Sector DNS Service from NCSC is part of the Active Cyber Defence suite of services.

The service acts as a typical DNS resolver however includes a Response Policy Zone (RPZ) that is managed by NCSC and blocks resolution attempts to known-bad malicious DNS record (such as those used for phishing, malware distribution or command & control).

Where to use the service

The service can be used wherever a typical internet-facing DNS resolver is required. It can be used on end-user compute solutions (supporting laptops etc) through to in Infrastructure-as-a-Service (IaaS) environments such as AWS and Azure.

How to use the service
Requirements

The service requires IP source address information to be provided to NCSC as while the solution is available on public IP space, it is not publicly available on the Internet for any organisation to use.

The is permitted to use the service for free as a central government organisation, but suppliers to currently are not.

Get started

Contact the Cyber Security team () to be added into 's subscription of the service.

Web Check

The service

The Web Check Service from NCSC is part of the Active Cyber Defence suite of services.

The service scans provided URLs for a series of indicators (negative and positive technical security configurations) and reports them through a web interface, email alerts and exportable report file.

Domains operated by, or on behalf of, the **must** be added to Web Check under at least the central Web Check account.

How to use the service
Requirements

The fully-qualified domain name or URL is required. It must be publicly accessible from the general Internet and present as a website on HTTP (TCP/80) and/or HTTPS (TCP/443).

The is permitted to use the service for free as a central government organisation, but suppliers to currently are not.

Get started

Contact the Cybersecurity team to be added into 's subscription of the service.

Protection from malware

Malware Protection Guide - Overview

This guide introduces the information which explains your responsibilities in helping the to prevent, detect and recover from malware. The has a three layer defence approach aligning with the National Cyber Security Centre (NCSC) guidance to mitigate the risks posed by malware. If one layer of defence is compromised then malware should be blocked or detected by the next layer.

Related information

Email blocking policy on page 271
Technical Controls Policy on page 30

Detailed information

For further guidance around implementing the three lines of defence to protect the from Malware, refer to the following guides.

- Malware Protection Guidance - Defensive Layer 1: Preventing malicious code from being delivered to devices - This section explains the preventative measures which should be taken to prevent malware from entering the 's systems.

- Malware Protection Guidance - Defensive Layer 2: Preventing malicious code from being executed on devices - This section explains the controls which should be implemented to prevent malicious code from executing on the 's systems if it evades Layer 1.
- Malware Protection Guidance - Defensive Layer 3: Increasing resilience to infection and enabling rapid response should an infection occur - This section explains how to minimise the impact of a successful malware intrusion through backing up information and limiting malware's ability to spread if the first two layers fail.

Assessing the malware risk

Malware can affect different systems in very different ways depending on how they store, process and execute files and potentially attacker-supplied content. Each system needs to be assessed to understand the potential threat from malware to it, and to design appropriate controls for that situation. The Assurance Framework provides information on how this may be achieved. Contact the Cyber Assistance Team for help regarding the Assurance Framework.

Who is this for?

The Malware Protection information is aimed at two audiences:

1. The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
2. Any other body, agency, contractors, IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the .

Malware Protection Guide: Defensive Layer 1 Introduction

This guide explains the types of controls that need to be implemented to form the first of three layers of defence. Layer 1 reduces the likelihood that malicious content will reach the network through implementing the controls outlined in this guide. This guide is a sub-page to the Malware Protection Guide.

Who is this for?

This Malware Protection information is mainly intended for in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the , will also find this information helpful.

Defensive Layer 1: Preventing malicious code from being delivered to devices

Do
✓ Ensure that all public facing URLs that are assigned to services owned or managed on behalf of the are protected by enrolling them in the NCSC Web Check service. Contact security@justice.gov.uk to add URLs to this service.
✓ Use of the Protective Domain Naming Service subscription service should be configured for end users. As a Central Government department, systems owned or managed on behalf of the are permitted to use the service for free. Contact security@justice.gov.uk to be included in this service.
✓ Ensure that if you are developing a system or application where any element is outsourced, such as hosting a service in the cloud, you must understand and record security related responsibilities of the , of the cloud service provider and any other supplier. For guidance on what responsibilities to consider, refer to the NCSC guidance on Cloud Security or ISO27017. These provide guidelines for information security controls applicable to the provision and use of cloud services.
✓ Ensure that if you are managing an email system, all inbound emails to the are scanned for malware. For Microsoft systems this is provided by Office 365 which quarantines any suspected malware.

Do
✓ Avoid the need for removable media by using existing approved online collaboration services where possible, for example Office 365. Where removable media has to be used, it must be scanned by approved Anti-virus before and during use.
✓ All web traffic must be routed through a proxy which logs and monitors internet access. This reduces the chance of malicious sites infecting end user devices. The proxy is configured in agreement with the Security Team. Email must also be routed through email scanning services. Direct Internet access should only be configured for update services, and by exception only.
✓ Allow the installation of applications only from approved stores.
✓ Systems must be able to be updated and must be kept up-to-date with OS and application upgrades and patches. Where possible, software updates should be configured to update automatically. Refer to the Vulnerability Scanning and Patch Management Guide for further information.
✓ A formal process must be developed and documented to ensure all firewall configuration changes are approved before being implemented.
✓ Be aware of the risks of 'watering hole attacks' that use GitHub or other open source code repositories. These attacks place malware into popular sites. Avoid trusting code, components, or other resources from popular sites. Refer to the Access Control Guide for further information.
✓ When developing a new system. ensure that it's properly scoped to understand what, if any, appropriate anti-malware software is required. You must also ensure that if the eventual system has anti-malware software, that it is configured to minimise the impact of scans on system or application performance. Contact the Security Team for further information on how to do this.
✓ Ensure that if you are responsible for patching or installing security updates of an in-house developed system or application follow the processes and requirements set out in the Vulnerability Scanning and Patch Management Guide. The success of these updates should be validated using automated vulnerability scanning services.
✓ Use hardened devices including approved and assured Gold Builds. Further information can be found in the Technical Controls guidance; contact the Security Team for help with this.

Don't
✖ Allow externally obtained (from outside the) executable software to run. This includes auto-running macros.
✖ Try to circumvent any security controls such as safe browsing lists or removable media controls; they are in place to protect the from malware.
✖ Connect any devices not procured and/or managed by the to trusted networks. Devices connected to trusted networks must be under management.

Malware Protection Guide: Defensive Layer 2
Introduction

This guide explains the types of controls that need to be implemented to form the second of three layers of defence. This guide is a sub-page to the Malware Protection Guide.

Who is this for?

This Malware Protection information is mainly intended for in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the , will also find this information helpful.

Defensive Layer 2: Preventing malicious code from being executed

Layer 1 might not always prevent malware from reaching the network. Assume that malware can and will reach devices at some point. The next layer of protection prevents malicious code from taking effect. The following tables outline ways in which you can help prevent malicious code from executing.

Do
✓ Ensure that all systems and endpoints are scanned by anti-malware software. Refer to Note 1 for more details.
✓ Ensure that if you are developing a new Microsoft Windows based system, that the 's Windows Defender enterprise anti-malware software for Microsoft environments is configured to regularly scan it. Contact the Security Team for further information on how to do this.
✓ Ensure that if you require additional anti-malware scanning functionality because of a higher malware risk, or you have non-Microsoft Windows systems, then other anti-malware vendors can be considered. You must discuss your selection with the Security Team . Refer to Note 2 for more details.
✓ If you are designing or developing a system which you expect to be at high risk of malware, you should ensure it is built with sandboxing capability in order to minimise the impact of malicious code executing on endpoints.
✓ Use hardened devices including approved and assured Gold Builds. Further information can be found in the Technical Controls guide. Contact the Security Team for more information.
✓ If you are developing or modifying networks, you should consider what protective monitoring is required. Contact the Security Team for details. Protective monitoring required can include Intrusion Prevention Systems (IPS) & Intrusion Detection Systems (IDS) to monitor, alert and block suspicious activity. These systems should feed monitoring data to the 's central monitoring capability. Contact the Security Team for more information.
✓ When developing new systems and services, or updating or maintaining them, ensure that you refer to the security requirements detailed in the Software Development Lifecycle (SDLC) guidance. Contact the Security Team for more information.
✓ Ensure production environments are segregated from other systems. Prior to going live, ensure this environment is assessed against the relevant top 20 Center for Internet Security Controls.
✓ If you are configuring host-based or network firewalls, ensure inbound connections are configured as `deny by default`. Outbound connections should also be denied by default on network devices such as firewalls, to prevent viruses avoiding proxies when leaving the 's systems. You should review these rules at least once every three months, to ensure they allow only necessary traffic.
✓ Ensure that all systems have agreed maintenance windows for patching. These maintenance windows must meet the Service Level Agreement timescales outlined in the Vulnerability Scanning and Patch Management Guide.
✓ Where possible, you should enable automatic updates for operating systems, applications, and firmware.
✓ Use versions of operating systems and applications which receive wide general support. This means they can take advantage of up-to-date security features, and so reduce vulnerabilities.
✓ Use automated code scanning services to help identify malicious and vulnerable code, including for open source applications or services. Refer to the Secure Development Lifecycle guidance for further information.

Don't
✖ Enable macros if you are using productivity suites unless there is an approved business case for doing so. For help on this point, contact the Security Team. Macros should be disabled by default.
✖ Design systems to use multiple consecutive firewalls for systems processing information. The exception is where the firewalls act as a contract enforcement point between two entities that are connecting to each other. In this case, the firewalls are structural devices that help define the boundary of responsibility rather than providing security. Refer to the NCSC guidance for further information.
✖ Delay implementing security patches on infrastructure when possible. Refer to the Vulnerability Scanning and Patch Management Guide for further information.

Note 1

Important: Those who manage anti-malware software must ensure that:

- it is in a working state
- it is set to receive updates at the highest possible frequency
- it is updated automatically with the latest virus definitions and updates
- scans are scheduled regularly or as external devices are added
- any findings are reviewed, and
- any anti-malware alerts are reported to the #unique_852 and the Security Team.

Note 2

Important: Anti-malware tools must:

- scan at least daily
- provide regular software updates
- have a Self-Protect Mode enabled
- have Clean/Quarantine capabilities
- provide regular reports and alerting to administrators
- prevent anti-malware services from being shut down without authorisation
- have defined responsibilities for maintaining, updating and reviewing the solution
- have defined test response and recovery plans to outbreaks

Malware Protection Guide: Defensive Layer 3 Introduction

This guide explains the types of controls that need to be implemented to form the third of three layers of defence. Layer 3 helps reduce the impact of malware infection in two ways:

- reducing the ability for malware to move across networks
- ensuring that data is backed up

This guide is a sub-page to the Malware Protection Guide.

Who is this for?

This Malware Protection information is mainly intended for in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the , will also find this information helpful.

Defensive Layer 3: Resilience and Rapid Response

Even with the controls created by defensive layers 1 and 2, it is still possible that malware might reside and execute on the networks. The following controls can help to build resilience, ensure a rapid response to infection, and reduce the impact of a successful malware intrusion:

Do

✓ Ensure that applications, services or systems are segregated from the rest of the network as soon as they are no longer supported by the vendor or by teams. The NCSC provides guidance on how to implement segregation of unsupported platforms.

✓ If you are designing a system, ensure that it can make regular, reliable backups of data. This is to limit the amount of data corrupted, encrypted or lost if an application, service or system is infected with malware.

✓ Ensure that backups meet all the criteria in Note 1. The NCSC provides further guidance on data backups stored in public cloud environments.

✓ Make sure that user permissions are regularly reviewed. Access to systems or drives no longer required by users must be removed. This is especially important for administrator accounts. Refer to the Access Control Guide for further information.

✓ When managing a system, ensure that backups are conducted in line with the system requirements outlined in the Information Risk Assessment Report (IRAR).

✓ Prioritise patches and updates of devices that perform security-related functions on the network. This includes firewalls and any device on the network boundary. Refer to the Vulnerability Scanning and Patch Management Guide for further details.

✓ Conduct regular audits of the software and data held on systems which support critical business processes. Check if they have been modified by malicious code.

✓ Isolate critical environments from the wider network as much as possible. This is to avoid significant business impact that might occur if the wider network is compromised by malware.

Don't
✖ Use the same browser to conduct administrative activities that you use for general user activities. An example admin activity is changing access privileges. An example general user activity is searching the internet. Separating browsers for different activities can reduce the impact of malware attacks.
✖ Delay implementing security patches on infrastructure. Refer to the Vulnerability Scanning and Patch Management Guide for further information.
✖ Delay if you suspect a malware incident has occurred. Make sure you contact the #unique_856 immediately.

Note 1

Important: Ensure that backups:

- Can be recovered. Some cloud providers allow data restoration from a point in time. This can be helpful if malware affects the cloud backup.
- Have an offline copy held in a separate location to the primary data storage. These are called cold backups and should be unaffected if an incident affects the primary environment.
- Are updated and tested regularly. The regularity of backups should be outlined in the system's Information Risk Assessment Report (IRAR).

Preventing and Detecting Lateral Movement

One of the most important ways of limiting the spread of malware on the network is to reduce lateral movement. This is where a malware problem 'jumps across' from system to system. The main ways to prevent lateral movement are covered in the following tables.

Do
✓ Make sure user credentials are protected. Do this using strong passwords which are stored securely. Refer to the Password Manager Guide for further information.
✓ Ensure that effective access controls are designed and implemented in systems. Use Multi-Factor Authentication (MFA) wherever possible. Refer to the Access Control Guide for further information.
✓ Make sure you protect highly privileged accounts, by applying the principle of least privilege. Refer to the Access Control Guide for further information.
✓ Ensure that any system or application running on the 's networks can collect and share system logs with the central monitoring function. This allows the to detect lateral movement by malware.
✓ Use tools for monitoring account activity, and look for indicators of account compromise. Examples include using Conditional Access to manage access to the network, and detecting impossible geographical travel scenarios. Configure the tools to respond promptly by raising security alerts and so helping prevent a breach.

Do
✓ In the exceptional circumstances where Bring your Own Device (BYOD) is permitted to access information, make sure your device runs anti-malware software and follows the requirements in BYOD guidance. Also ensure that users can only access emails through approved applications.
✓ If you are designing or modifying networks, ensure there is network segregation for systems and data that do not need to interact. This segregation can be achieved using physical or logical separation. Access between network domains is allowed, but must be controlled at the perimeter using a gateway such as a firewall.

Don't
✖ Access emails through third party applications which have not been approved by the .
✖ Allow access to information on devices, by default. Restrict access on devices to need to know.
✖ Use your administrator account for any non-administrative functions. Access should only be elevated for the specific tasks required, and only while the task is performed. Refer to the Privileged User guidance for further details.

The NCSC provides helpful guidance on preventing lateral movement across networks.

Ransomware

Ransomware is a type of malicious software created or used by cyber criminals. It prevents people or businesses from accessing their own data. The software takes hold of the data, holding it "hostage", until a ransom payment is made to release it.

Preventing Ransomware from taking hold of information

- Store all your information in official systems. This is general best practice, and also minimises the risk of the data being accessed by the hackers.
- Use a secure antivirus and firewall software. All official systems have these installed as standard.
- Use a trustworthy VPN when accessing public networks through wifi, for example when working remotely in a coffee shop. All official systems have a suitable VPN installed as standard.
- Ensure your laptop computer is updated regularly. All official systems do this for you automatically, as standard.
- Use multi-factor authentication (MFA) methods. Most systems support MFA, but you might have to enable it yourself.
- Do not provide any personal information to unknown contacts.
- Avoid insecure apps or websites.

Things to look out for if you suspect you have become victim to a ransomware attack

- Unable to open documents.
- Suspicious file names. Files encrypted by ransomware tend to end with `.crypted` or `.cryptor`, rather than the more typical names such as `.docx`, `.pdf`, or `.jpeg`.
- An unrecognised pop-up screen prevents access to your computer.

What to do if you think a ransomware attack is affecting your system

In the event of a ransomware attack, or if you have suspicions one may be taking place, the first thing to do is to contact your local .

With your help, the IT team attempt to determine which systems have been impacted, and can isolate them immediately. You might be asked to disconnect all your devices from the network or wifi connection, to prevent a further spread of attacks throughout the business.

Backup

System Backup Guidance

Related information

System Backup Policy on page 182
System Backup Standard on page 183

Backing up information

Backing up is an essential part of protecting Information and Communication Technology (IT) resources. This guide document provides an overview of backup concepts, and why backup is important for the .

It is not normally necessary for you as an individual user to do anything about backing up. Most of the time, it is sufficient for you to know that backups take place, and that it is normally possible to request recovery or restoration of data for a system.

What is backing up?

IT systems fail, or stop working, for many reasons. If you are unlucky, the failure results in the loss of your work. For example, if you are working with a spreadsheet on your desktop computer when the power fails, you lose all the work you have done. Similar problems affect bigger computer systems - servers - too.

Backing up is the process of making a copy of the current information held on the computer system. The copying process usually happens automatically, at regular intervals, often at night. Or it happens when you request it.

The copy of the information is the backup of the data.

A backup lets you recover or restore the data up to the moment the backup was taken, whenever it is needed. Without a proper backup, you have probably lost all your recent work.

A backup helps protect you from the consequences of hardware or software failure, or from accidental or malicious changes to the files and data.

Mirrored or load balanced systems - where the data or services are available from more that one system, and you don't need to know or care which actual system is being used - are not considered to be forms of backup.

What is data recovery or restoration?

These terms usually mean the thing: data is brought back to be the same as it was at a specific moment in time, or as it was before an event such as accidental deletion.

Why is backing up important?

A backup helps protect you and the from accidental or deliberate changes to information, for example when data are deleted or IT hardware fails.

Depending on the system used, backups can also provide a history of who made changes to data, and when.

Backups are especially important for record retention requirements. Backups for this purpose are often called archival copies, because each is kept for an extended period of time.

Protecting backups is important. The CESG Information Assurance Maturity Model (IAMM) describes the minimum level of information assurance that all Government departments should provide. For example, access control is a basic assurance requirement. The backup policy and standard both comply with access control assurance.

More information about how the backup policy meets the Security Policy Framework mandatory requirement is provided within the IT Security - Technical Controls Policy.

What systems are backed up?

Backup capability is required for all IT systems, including systems hosted by third party suppliers for the .

To decide if backup is required for a specific system, ask the question: "how long can the tolerate the system being unavailable?" If there is any time limit, then backup is probably required.

The Information Asset Owner makes the final decision about whether backup is required for an system, and what backup schedule should be followed. This is documented within the System Operating Process.

How often does a backup take place?

It depends on many factors, such as the amount of data, the sensitivity of the data, how often it changes, how often you want to restore the data, and how quickly you want it restored.

For example, if some data only changes once a month, backing up the data every day is probably excessive. Similarly, if the data changes every hour, then a daily backup is not enough.

A backup should be taken sufficiently often so that the time required to restore a system to full working state is less than the time for which the can tolerate the system being unavailable.

Where does a backup go?

Backups are stored in many different places, and on many different media types. Valuable data has many backups, stored in several different places.

Traditionally, backups are stored on one or more of the following backup media:

- an external drive or USB memory stick
- a CD or a DVD
- magnetic tape

More recently, backups are stored on services specifically intended for backups. These services have different performance and availability characteristics to ordinary data processing services. For example, the data might be stored in a different data centre.

Another reason for using backup services is that some systems have so much data that trying to backup to physical media is impractical.

Archival backup media is stored off-line for a defined amount of time. This is for reasons of contract, statutory obligation, or other formal records retention.

Backup media such as tapes should be stored off-site, and only returned on-site when required for data restoration purposes. Storage must be in a secure location that matches the sensitivity of the data. The precise requirements for storing media are outlined in the system Business Continuity Plan (BCP).

What is in a backup?

A backup contains one of:

- All data, in other words a complete copy of the information on the server. This is called a full backup. It contains all the data needed to restore the system completely, for example after a total system failure.
- Only data that has been added or changed since the last backup. This is called an incremental backup. But it requires an earlier full backup and previous incremental backups to restore a system completely.

Some backups contain data that is sensitive. Evaluate the data that is to be backed up to decide if it should have extra protection, for example by encrypting the backup.

How long is a backup kept?

Keeping all backups forever on physical media is not practical or desirable. It is usually necessary to delete data and any backups after a defined period of time.

System Backup Policy

Backing up is an essential part of protecting Information and Communication Technology (ICT or IT) resources. Backing up provides a means of recovering a system or data to a known state, or point in time. In other words,

backups enable you to restore a system or data to be effectively indistinguishable from how it was on a particular date and time.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.SBP.xxx**, where **xxx** is a unique ID number.

Note: Use of the word in this document complies with the usage defined in .

Related information

System Backup Guidance on page 181
System Backup Standard on page 183
Technical Controls Policy on page 30
Technical Controls Policy on page 30

System recovery

POL.SBP.001: All systems comply with the Security Policy.

POL.SBP.002: All IT systems conform to the IT Security - System Backup Standard.

POL.SBP.003: All IT systems be evaluated to determine if a backup schedule is required. This depends on the data stored, and on legal or other regulatory requirements. The evaluation and resulting decision regarding backup requirement be documented for the system.

The IT Security - System Backup Standard provides details of the tasks, configurations, and processes required for an IT system backup to comply with this policy.

Technical controls

To address these requirements, these statements from the Technical Controls Policy apply:

POL.TCP.108: All IT systems have back-up procedures to maintain the integrity and availability of all Information Assets held. This must align to the Recovery Point Objective which may be expressed in the Business Impact Assessment (BIA).

POL.TCP.109: All IT systems maintain a log of all back-ups taken.

POL.TCP.110: Back-up data be stored and handled in a manner appropriate to the protective marking of the Information Assets stored.

POL.TCP.111: All IT systems check all historic back-ups regularly to ensure that they can be relied upon. This includes the testing of back-up media such as tape or hard disks.

POL.TCP.112: All IT systems have a back-up restoration procedure which is tested regularly. Ideally, the testing takes place automatically.

POL.TCP.113: The retention period for historic back-ups align to the retention period of the Information Assets held.

System Backup Standard

Related information

System Backup Guidance on page 181
System Backup Policy on page 182

Backing up information

Backing up is one of the most important methods of system recovery. It protects Information and Communication Technology (ICT or IT) resources.

The IT Security - System Backup Policy describes the mandatory requirements that system backup meets.

This document provides standards and details of the tasks, configurations, and processes required for an IT system backup to comply with the policy, including:

- how backups are managed

- the process for backing up

For an overview of backup concepts, and why backup is important for the , refer to the IT Security - System Backup Guide.

For details of what backups must do, refer to the System backup requirements section.

For details of how backups are implemented, refer to the System backup procedures section.

Foundation

Each system requires:

- a backup schedule that describes the frequency and kind of backup for the system
- a retention schedule that describes how long a backup must be kept, to enable system recovery
- an archive schedule that describes how long a particular backup should be kept after it is no longer required for recovery purposes, but is still retained to comply with the Data Retention requirements or other legal needs
- a process for deleting or disposing of a backup if it is no longer required for recovery or retention purposes
- a process for recovering or restoring some or all data or other backed-up information to a known point-in-time
- information so that users understand how data can be restored for the system, if required
- a process for users to request data recovery or restoration, subject to business requirements

System backup requirements

This section of the standard describes the main requirements for system backups. It must be possible to:

- take backups
- test backups
- retain and restore backups as required
- maintain a library of backup archives

General requirements

Systems backups should be:

- proportionate to the need
- taken on a regular basis
- tested regularly to help guarantee reliable restoration of any required data
- stored safely and ready for restoration when required, for example during a disaster event
- recorded in a log, detailing what data was backed up, and when

The amount of data backed up from the system is the 'extent', and how often the data is backed up is the 'frequency'. The extent and frequency of backups must be such that the is able to tolerate non-availability of the data if becomes unavailable and must be restored.

For any information asset, an assessment should be performed to determine if recovery is required, and if so whether using a backup is an appropriate and sufficient mechanism.

The backup schedule

The backup schedule determines what backups are taken for a system, and when. Backups typically take place at intervals based on the following table:

Frequency	Kind of backup
Daily: once every 24 hours	Incremental
Weekly: once every 7 days	Full
Monthly: once every 30 days	Full archival copy

From these defaults, the actual backup frequency for a system is calculated using the Recovery Point Objective (RPO). The RPO measure is a window of time. The loss of any data additions, changes, or deletions during the RPO

window can tolerated by the users of a system. For example, if the RPO for a system is four hours, then the loss of up to four hours worth of data transactions is tolerable because they can be recreated. Therefore, the backup frequency for the system should be such that no more than four hours-worth of data are lost.

The RPO is also dependent on the amount of data that must be recovered - the 'extent'. For example, recovery of all data is likely to take longer than recovery of a subset of the data.

When deciding to use an incremental or full backup process, a helpful indicator is the Recovery Time Objective (RTO). This is a measure of how long the organisation tolerates non-availability of a system.

The time for a complete restore of data from backup should be smaller than the RTO. If full backups are taken every time, then the restore time is simply the time to restore the most recent full backup. But if incremental backups are used, the time to restore will be the amount of time to restore the most recent full backup, plus the time to restore all the necessary subsequent incremental backups.

The RPO and RTO values for a specific system are determined in the system's Business Impact Assessment (BIA) and Business Continuity Plan (BCP).

System backup schedule checklist:

1. Determine the extent of data that must be backed up.
2. Determine the RPO for the system.
3. Determine the RTO for the system.
4. Calculate backup frequency using the RPO value. The time between backups must be less than the RPO value.
5. Decide the configuration of full and incremental backups. The configuration should be such that the time required for a complete recovery is less than the RTO. Remember to allow time for deciding to do a restore, and retrieving off-site backups if required.
6. Confirm that the schedule includes backups suitable for archiving purposes.
7. For each of the types of backup testing required, include process details.
8. Identify storage requirements for backups and archives, and processes for storing and retrieving them.
9. Identify the process for logging details of each and every backup.

In summary, the backup schedule for the system provides the following details:

- the extent and frequency of backup
- testing processes, including their frequency and record keeping
- storage details, including logging, specifications and processes

Retention schedules

Backups must be stored and kept available to restore the data when required. The length of time that backups are kept for recovery purposes is called the 'retention period'. The retention schedule defines the retention period for backups.

Normally, when backup data is no longer required for recovery purposes, it is deleted, to comply with data protection requirements. Sometimes, the data must be retained for a longer time.

For example, a 'Legal Hold' might be placed on all or some of the backup media. A hold supersedes the existing schedule for destroying, deleting, or overwriting the media. The revised schedule remains in place until the hold is removed.

Backup data that is held for longer than the retention period is considered archive data, and is managed using the archive schedules. It is not normally used for recovery purposes.

Creating a retention schedule

All system backups must have a defined retention schedule.

The retention period is determined by several factors, such as a financial or regulatory requirement to keep data for a specific period of time, but no longer.

The retention schedule ensures that all necessary system backups are kept. For example, if a system is fully backed up twice a day, and the retention period is one year, then backup data equivalent to the `365 x 2 = 720` distinct backups must be retained.

When a data backup eventually falls outside the retention period specified in the retention schedule, it must be archived or destroyed.

If an information asset held in a backup has a defined retention period, that should be used as the basis of the retention schedule for that asset.

For other information assets that do not have an existing defined retention period, the following table provides a generic period.

Kind of data in backup	Default retention schedule	Disposal of backup media
High impact (RTO is one day or less)	8 weeks	Within 4 weeks after the end of the retention period.
Low impact (RTO is more than one day)	4 weeks	Within 4 weeks after the end of the retention period.
Email	2 weeks	Within 4 weeks after the end of the retention period.

The actual data retention schedule for an system is agreed between the business and the Departmental Library and Records Management Service: .

The Departmental Records Officer has responsibility for the records, and signs off the schedules which the business follows.

The backup retention period should never be shorter than the schedule requires. If the available technology cannot support the prescribed backup retention period, then an exception must be sought and documented in the relevant system Risk Management and Accreditation Document Set (RMADS).

Retention schedule checklist:

1. Is a retention period defined in the system BIA or BCP? If not, identify the kind of data backed up by the system. Use this to determine the default retention period based on the previous table.
2. If multiple data types are backed up, use the longest applicable retention schedule.
3. If you cannot determine or implement the retention period, seek guidance or an exception through the RMADS for the system.
4. Detail the retention period, and the process for moving backups into and out of the retention state.
5. Provide a process for testing each of the backups.
6. Provide a process for recovering a complete set of data using any retention backup.

Archive schedules

As described in the retention schedule requirement, backups might be kept beyond the retention period in order to comply with an additional retention requirement. Backups for this purpose are archive backups.

Depending on the nature of the extended retention requirement, it might be possible to satisfy the need in one of the following ways:

- keeping the existing backups unchanged
- using a combination of full and incremental backups
- condensing the existing backups into archives of full backups

A backup suitable for archive purposes has the following characteristics:

- it is already stored on physical media, or is converted accurately and without loss onto physical media
- the physical media will not degrade during the archive period
- the media is stored in an offline environment that is either on-site or off-site
- the backup contains all the data required to meet all the retention obligations

Creating an archive schedule

Any system with a backup schedule might need to archive data. The archive schedule for the system defines how a backup is moved into an archive state, depending on the specific retention requirement.

The data retention schedule for a system determines what the archive schedule is, and therefore how long an archive backup must be retained. More help on managing information is available here.

Archive schedule checklist:

1. If an archive process is defined in the system BIA or BCP, use it.
2. Detail the process for moving backups into and out of the archive state.
3. Provide a process for testing each of the backups.
4. Provide a process for recovering a complete set of data using any archive backup.

System backup procedures

System backup procedures describe the tasks that meet the system backup requirements. The general procedures outlined in this document provide the basis for the actual procedures and work instructions that apply to a specific system.

Responsibilities

The manager of a system, or their nominated deputy, is responsible for assuring that:

- all backups complete successfully
- the log files for completed backups are checked, to confirm that the correct data was backed up
- the register of system backups is updated and maintained
- any backup medium used is replaced as required for example because of failure or reaching end-of-life
- backup schedules are maintained
- any backup failures occurring twice or more in succession are recorded, investigated, and resolved
- the decision regarding when to try a failed backup again is documented: as soon as possible, or by waiting until the next scheduled backup task

Security considerations

Backup procedures are part of protecting a system. Therefore, the backup procedure for a system must be included within the Security Operating Procedures (SyOPs) for system administrators.

Some backups contain highly sensitive material. In addition to the security used to protect the backup media, think about encrypting the backup data itself. This should be assessed for each instance during the system accreditation process. Backup encryption is done in several ways; the method chosen and used should be described in the SyOPs.

Recovery Testing

Backups are of little value if the data cannot be restored. It is essential that regular disaster recovery testing takes place, to guarantee that system backup processes are working correctly. In particular, verify that:

- the correct data are being backed up
- backed-up data are recoverable

Testing can be done in three ways:

1. A simple read only test is performed on the backup data, to ensure that all the data can be read without error or omission. This checks that it is possible for a recovery process to have access to all the required backup data.
2. A specific server or system recovery test is performed, normally taking place on-site. The test usually requires the recovery of some or all the data to a proxy system, separate from the original server. This check ensures that the data required for a complete system recovery is available.
3. A scenario-based test is performed, normally taking place off-site. This is a more comprehensive test, where a full system restore is done using an off-site non-live environment. This approach is ideal for testing various disaster recovery scenarios such as complete loss of access to the original system that was backed up.

The testing method used, and how often it is applied, is part of the IT Disaster Recovery plan and testing regime for the system. More information is in the IT Security - IT Disaster Recovery Plan and Process Guide.

Backup schedules

The system backup configuration must be thoroughly documented in the schedule. The information describes how the backup works, how often it is done, how it is tested, and so on.

It must be possible to show that the configuration meets all the system backup requirements. Auditing confirms that any issues are resolved promptly, and that the backup process works reliably.

Looking after backup media

Physical media that contains backup data must be stored securely, either:

- onsite, where the media is stored in a secure place that is geographically close to where the backed-up system is located
- offsite, where the media is stored in a secure place that is geographically remote from the backed-up system

The storage site must meet both location and retrieval requirements of the Disaster Recovery Team.

The technical, physical and procedural security controls for storing backup media must meet or exceed the requirements for the highest protective marking of the backed up information. In other words, even if just one part of the backup data are classified as , then the entire backup medium must be protected to meet requirements.

The protective marking level for a backup is determined during the BIA process, and is described in the Accreditation Framework (this document). The precise selection of security controls for a system backup is established as part of the system risk assessment.

The handling and transportation of backup media among system and storage sites must also be in line with the highest protective marking. More information about handling protectively marked information is in the IT Security - Data Handling and Information Sharing Guide. The sharing guide provides details on the procedures and approvals that are required before any movement of any protectively marked information takes place.

Identification and tracking

Backups, and the media each one is stored on, must be identifiable for tracking and reporting purposes. This means that each media item that holds backup data must have a unique media and job ID, and a formal indication of the information held; the Protective Marking, for example .

If a single backup medium, such as a solid-state storage device, is used to hold several backups, each unique media and job ID must be recorded and associated with the hardware device in the relevant configuration management database (CMDB).

All of the following details must be recorded in the system backup register, for each unique media and job ID:

- System name and any server names
- Protective Marking for the media
- Creation date, or date last written, using the format `DD-MM-YYYY`
- End date for retaining or archiving the data, using the format `DD-MM-YYYY`
- Name of the system manager
- Name of the Information Asset Owner (IAO)
- Backup status, summarising the schedule details and kind of backup, for example Daily Incremental, Weekly Full, or Archive Full
- Outcome status, set to `Yes` indicating that the backup was successful, or `No` if the backup failed

Disposal of backup media

When a backup is no longer required for retention or archival purposes, it is normally deleted. If all the backups stored on a physical medium have been deleted, the medium itself is checked to determine if it is suitable to use again.

If the medium is reusable, it must be securely erased in accordance with NCSC guidance on secure sanitisation of storage media, then placed back into stock for re-use.

If the medium is not reusable, it must be taken out of stock and marked with a `To Be Decommissioned` status in the system backup register until secure disposal takes place. The status is also updated in the CMDB.

Disposing of any medium must be in accordance with the relevant disposal plan.

Logging and monitoring

Accounting

The base principle

Any access, and subsequent activity, to any system or data **must** employ adequate accounting techniques to ensure events can be attributed to the authenticated entity.

Accounting information must be stored in a way that it cannot be readily manipulated, particularly by the authenticated entity.

Log data security & governance

Log data can include Personal Data or inadvertent sensitive data (when an application or system is unexpectedly verbose) and must be adequately protected and governed in a comparable way to the original system's data.

Security-related log data retention

Log data created and processed for information security purposes should be retained for no longer than 2 (two) years by default (this is subject to any legislative or regulative compliance requirements) but for a minimum of 6 months.

These times are general as a guide, and require contextual analysis particularly where Personal Data is involved.

Commercial off-the-shelf applications

We have developed a series of logging requirements for Commercial off-the-shelf (COTS) applications, such as Software-as-a-Service (SaaS) solutions or where applications are not so customised that they can reasonably be considered bespoke/custom for the .

Baseline Maturity Tier
1. User directory services

Log Collection Principle(s): 1, 2

User directory services, or interactions with them, must create and forward Authentication and Authorisation events.

User directories within application environments can be rich and diverse, such technologies include:

- Active Directory (AD)
- Azure Active Directory
- OpenLDAP
- Amazon Web Services (Accounts and Incognito)
- Okta
- Auth0
- github.com (acting as an identity provider)
- (acting as an identity provider)
- Oracle identity stores
- Local user stores within operating systems leveraged by tenant applications

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)

8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Authenticated user activity events

Log Collection Principle(s): 6

Applications should create viable user activity audit information for authenticated users to reasonably identify which authenticated user took which action.

1. User/group identifier(s)
2. Action/query
3. Response size
4. Response time

Enhanced Maturity Tier

1. Data store events

Log Collection Principle(s): 6

Temporary data stores (such as intermediate queues) and permanent data store (such as databases) are key data locations and all interactions should be highly auditable.

1. Data store identifier(s)
2. Credential identifier(s)
3. Query
4. Query response size
5. Query response time

2. Unauthenticated user activity events

Log Collection Principle(s): 6

Where unauthenticated users interact with applications (for example, a document available on the general Internet through relaxed access controls), associated audit information must be created.

1. End-client identifier(s)
2. Query metadata:
    a. Destination identifier (such as target hostname, TCP/UDP port and/or full URI)
    b. Query type (for example, `HTTP GET` or `HTTP POST`)
    c. Query size
3. Response size
4. Response time

Custom Applications

We have developed a series of logging requirements for custom applications, such as digital services, applications materially customised that they can reasonably be considered bespoke/custom for the and line of business applications at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

Baseline Maturity Tier

1. User directory services

Log Collection Principle(s): 1, 2

User directory services, or interactions with them, must create and forward Authentication and Authorisation events.

User directories within application environments can be rich and diverse, such technologies include:

- Active Directory (AD)
- Azure Active Directory
- OpenLDAP
- Amazon Web Services (Accounts and Incognito)
- Okta
- Auth0
- Github.com (acting as an identity provider)
- (acting as an identity provider)
- Oracle identity stores
- Local user stores within operating systems leveraged by tenant applications

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Authenticated user activity events

Log Collection Principle(s): 6

Applications should create viable user activity audit information for authenticated users so it is reasonably possible to understand retrospectively which actions the user took or attempted.

1. User/group identifier(s)
2. Action/query
3. Response size
4. Response time

3. Unauthenticated user activity events

Log Collection Principle(s): 6

Where unauthenticated users interact with applications (for example, a digital service published and available on the general Internet), associated audit information must be created.

1. End-client identifier(s)
2. Query metadata:
    a. Destination identifier (such as target hostname, TCP/UDP port and/or full URI)
    b. Query type (for example, `HTTP GET` or `HTTP POST`)
    c. Query size
3. Response size

4. Response time

Enhanced Maturity Tier

1. Pipeline events

Log Collection Principle(s): 1, 2, 3, 6

Continuous integration and continuous deployment pipelines obey instructions to manage applications and are a privileged position to oversee all associated resources, they must be highly auditable to clarify activity and attribute the same.

1. Source identifier(s)
    a. User(s)
    b. Repository
2. Activity events
    a. Resource creation
    b. Resource destruction
    c. Target environment

2. Data store events

Log Collection Principle(s): 6

Temporary data stores (such as intermediate queues) and permanent data store (such as databases) are key data locations and all interactions should be highly auditable.

1. Data store identifier(s)
2. Credential identifier(s)
3. Query
4. Query response size
5. Query response time

Logging and monitoring

The monitors the use of services, by recording (logging) event information.

This is permitted under data protection legislation, to help defend services against cyber security attacks, and misuse (such as fraud). General Data Protection Regulation (GDPR) Recital 49 notes that the processing of personal data (to the extent that is strictly necessary and proportionate) to ensure the security of a system which forms the underlying lawful basis for why the processes this type of data for this purpose.

This is why the can log and monitor external interactions with its services, looking for evidence of cyber security attacks. It also allows the to act to protect those services. For example, the can block an IP address associated with known malware, or which is trying to perform a denial of service attack.

At the same time, the is careful not to "over-retain" log information, or to share it with those who do not need to access it, without lawful justification. The must always act in a proportionate way with this data.

The Chief Information Security Officer (CISO) is ultimately responsible for all logging and monitoring systems which have been implemented for cyber security purposes. This means that the CISO is also the Information Asset Owner for all logging and monitoring data.

Related information

Online identifiers in security logging and monitoring on page 193
Privileged User Logging and Protective Monitoring Guide on page 106
Security Log Collection on page 209

Log retention

A distinction is drawn between web-facing services (available to anyone on the public Internet) and internal-facing services (available only to people who are authenticated by an or Government means of identification, for example an email address or login ID).

Application logs be kept for the same period as those for other services. The reason is that they might contain relevant information if evidence of an intrusion is found.

Logs for external services

Logs for all services that can be accessed from the public Web be kept for a minimum of 90 days.

Logs for internal services

Logs for all services that are accessed using an or Government identity or login be kept for a minimum of 13 months.

Maximum retention period

Logs be retained for longer than 2 years without specific approval from the CISO. However, aggregate data from logging systems, such as the number of particular types of events or the total numbers of visits to sites, be retained indefinitely, so long as care is taken to remove potentially unique or personally identifying information from the retained information set.

Variations and exceptions

These requirements are defined and required by legislation, regulation such as the Law Enforcement Directive, or certification compliance such as PCI-DSS. Variations or exceptions be created without the specific documented permission of the CISO

Protecting log files and log data

Default permissions must be set on logging and monitoring systems such that only ops staff for that service, and the 's Security team (), have access to the data in them. All access to the raw logging and monitoring data must also be logged.

Bulk exporting from such logging systems is prohibited by default. Where analysis is required using sensitive logs, it must be performed "in-situ". Bulk exporting should be prevented by default, using technical or other access controls where possible. If a bulk extract from a logging system is required, for example, into a more complex analytical system or as part of a wider migration, this requires the prior approval of the CISO.

Online identifiers in security logging and monitoring

Related information

Logging and monitoring on page 192

Overview

It can sometimes be counter-intuitive to think of IP addresses, cookies, and log data as personal data. However there are good reasons why it is important fort he during design, implementation, and operation of online services. Put simply, it is easiest for the to assume that any information captured and processed through public-facing services might contain personal information, and to protect this information accordingly.

What are online identifiers?

Online identifiers are anything that could be used to track someone as they interact with online services. This can include, for example:

- IP addresses.
- Cookies that the or authorised 3rd parties set on devices.
- Information placed into local storage on devices.
- Usernames or other IDs associated with services.
- Third-party authentication tokens.

Online identifiers could also include metadata captured about a device interacting with services if this information is sufficiently different to allow devices to be reliably identified.

Why are online identifiers treated as personal data?

If there is any way to tie an online identifier to an individual, then that identifier needs to be treated as though it is personal data.

The way this mapping might be achieved is unimportant.

It could be because the user later provides personal data to the as part of using a service, and in doing so provides a link between all of the activities that their IP or session cookie has done with their identity.

There might also be a legal route available to the to determine the identity behind an identifier. For example, by making a lawful request to an ISP to uncover the person associated with a dynamic IP address at a particular time.

For more information on this, refer to the Information Commissioner's Office (ICO) key definitions, and "Recital 30" from the Article 29 Working Group. There is also an informative article here.

What does this mean for services?

It is important to think carefully about:

- What metadata is captured during a user's interaction with services.
- How long information is retained.
- Who has access to the information.

privacy notices on services must be clear about the information captured as part of a user's interaction. This includes "anonymous" interactions, such as simple browsing information about the services. Metadata like this must be included in the scope of privacy impact assessments for services.

Note: Theoretically, privacy notices are only mandatory for externally-facing services. They are not required for internal services. However, it is undoubtedly good practice - and highly recommended - to apply the same approach, for consistency.

Protective Monitoring Guide

Related information

Technical Controls Policy on page 30

About this document

Note: This is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon. Please contact us before using this on a new project:

This policy applies to all staff and contractors who work for the .

This document is the IT Security – Protective Monitoring Guide. It is designed to help protect ICT systems by providing implementation guidance for a protective monitoring solution.

How to use this document

The purpose of this document is to provide guidance on developing a protective monitoring schema for a ICT system. It must be read in conjunction with CESG Good Practice Guide No.13 - Protective Monitoring for HMG ICT Systems.

Note: This document is a supplement to CESG Good Practice Guide No.13 - Protective Monitoring for HMG ICT Systems, not a replacement.

Overview
Introduction

Protective Monitoring is a set of business processes, with essential support technology, that oversees how ICT systems are used and to assure user accountability for their use of ICT facilities. Protective monitoring places mechanisms for collecting ICT log information to provide an audit trail of defined security relevant events which can be used for reporting and alerting.

HMG Security Policy Framework (SPF) Mandatory Requirement 9 states that:

> Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

In order to meet that requirement, the SPF stipulates that ICT systems must:

> Put in place a proportionate risk based suite of technical policies and controls including: ... IV. Protective Monitoring;

Policy statements on protective monitoring are covered in IT Security – Technical Controls Policy, while this document sets out the guidance for its implementation.

Scope

This guide applies to all ICT systems including ICT systems hosted by third party suppliers on behalf of the .

Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. Protective monitoring is captured as a basic requirement in Level 1 of this model, which the will need to demonstrate compliance with in their IAMM return to the Cabinet Office.

Basics of protective monitoring
Accounting and Auditing

Protective monitoring as described in CESG Good Practice Guide (GPG) No.13 centres on the concepts of Account and Auditing.

Accounting is defined as 'the process of collecting and recording information about events', whilst Auditing is defined as 'the systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled'.

An organisation can choose to account for almost every transaction that takes place on the system, but then audit almost none of them. When deciding on what approach to take with accounting and auditing it is necessary to first identify what types of information should be recorded then decide what information should be examined and how regularly that examination should be carried out.

Accreditation and protective monitoring

The audit criteria and the decision on what information is collected and alerted upon must be derived from a risk assessment conducted against the ICT system. This decision making process for the selection of protective monitoring controls forms part of the Accreditation process where the resultant protective monitoring solution **must be** documented in the Risk Management and Accreditation Document Set (RMADS). This document provides guidance on the selection of those controls, the key questions to be applied to that selection and a template for documenting it.

Further details on the Accreditation process can be found in the Accreditation Framework.

Note: The Accreditor will assess any protective monitoring solution against CESG GPG No.13, the policy statement in the IT Security – Technical Controls Policy and this guide.

Accounting

The decision on how much information needs to be recorded in an accounting log requires a comprehensive assessment and must be consummate with the risks identified. Recording too much information can be as great a problem as recording too little. If too much information is recorded it can become extremely difficult to review and can cause performance and capacity problems for an ICT system. If too little information is recorded it may be impossible to investigate a security incident effectively.

A good method of analysing this problem is to have a structured approach whereby the different types of information which could be captured are analysed at the different levels of an ICT system (e.g. network, system and application), building a picture of the inter-relationships between the different accounting logs (at those different levels). For example, accounting may take place at the following levels:

- Network accounting (e.g. logs created by network components, such as firewalls or domain controller);

- System accounting (e.g. logs created by individual host systems, such as Windows server security logs);
- Application accounting (e.g. logs created by individual applications).

The network/systems logs can be used to record the following security events:

- All actions taken by the Administrators;
- All actions taken whilst using the database administrators' accounts;
- All updates to operating system files;
- All workstation time-outs;
- Any attempts to copy the password file;
- All updates to the application software;
- Use of the system out of normal hours.

The application logs tend to record almost all the actions that take place whilst an application is being used. These tend include:

- All failed log-on attempts;
- All successful log-ins;
- All log-offs;
- All updates to a record;
- Each time a record is viewed.

Auditing

The types of auditable event mainly fall into two categories.

Firstly, there are events which need to be checked on a regular basis because they could indicate that someone is actively trying to breach the security of the system. An example of this is unauthorised log-on attempts or copying of the password file.

Secondly, when a breach of security is detected (or reported), the work which was being conducted on the system at that time in order to identify:

- How the breach of security occurred;
- Who was responsible for the breach;
- The amount of damage caused by the breach.

To support an investigation into a security incident, it is important to have a range of flexible reporting tools which allow the investigator to sort through the accounting information collected in a variety of different ways, and allows interconnections to be made between data derived from different sources.

Note: When considering what types of information which should be captured and what auditing should be implemented, it is important to ensure that the relevant IT Security Incident Management Plan is factored into the decision making process. This is to ensure that any protective monitoring solution supports the identification, alerting and investigation of security incidents. Further information can be found in the IT Security Incident Response Plan and Process Guide.

Developing a protective monitoring schema

For the purposes of this guide, a protective monitoring schema sets out all the controls points which will be implemented in an ICT system.

Development stages

The business process for protective monitoring is captured in Figure 1 of CESG GPG No.13. This section covers the stages which should be followed when developing a protective monitoring schema:

- The key questions which must be applied which selecting protective monitoring control items;
- The minimum protective monitoring requirement;
- Selecting minimum control objectives;
- Setting the minimum audit requirement;
- Reporting and service validation.

Key questions

The following key questions cover items which should be thought about when selecting protective monitoring controls:

- What is being audited and monitored? In terms of:
  - Usage scenarios - what users are allowed to do and which actions need to be accounted for;
  - Exceptions and how they will be detected - what users are not allowed to do or what would constitute suspicious activity;
  - The complexity in terms of the different types of connectivity to support these interactions (e.g. air-gapped systems, electronic exchanges, remote access, wireless, Internet services, etc.).
- What information will be collected to support the accounting, audit and monitoring of these activities?
- How the information gathered will be used (including both a list of permitted purposes and a list of prohibited purposes)?
- Who will access the protective monitoring data and their associated responsibilities?
- How the information will be protected, stored, retained and disposed of?
- How notification of monitoring is achieved and how user consent is obtained, or otherwise?

Minimum protective monitoring requirement

The minimum level of protective monitoring which need to be implemented is set out in CESG GPG No.13; Table 1 following reproduces part of GPG13 which sets the baseline requirement to achieve a minimum level of protective monitoring.

Protective Monitoring Control	Objective
PMC1: Accurate time in logs.	To provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components.
PMC2: Recording relating to business traffic crossing a boundary.	To provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.
PMC3: Recording relating to suspicious activity at a boundary.	To provide reports, monitoring, recording and analysis of network traffic crossing a boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach an ICT system boundary or other deviation from normal business behaviour.
PMC4: Recording of workstation, server or device status.	To detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of Trojan software or so called "rootkits"). It will also record indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes).

Protective Monitoring Control	Objective
PMC5: Recording relating to suspicious internal network activity.	To monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated the internal network.
PMC6: Recording relating to network connections.	To monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.
PMC7: Recording of session activity by user and workstation.	To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.
PMC8: Recording of data backup status.	To provide a means by which previous known working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised.
PMC9: Alerting critical events.	To allow critical classes of events to be notified in as close to real-time as is achievable.
PMC10: Reporting on the status of the audit system.	To support means by which the integrity status of the collected accounting data can be verified.
PMC11: Production of sanitised and statistical management reports.	To provide management feedback on the performance of the Protective Monitoring system in regard of audit, detection and investigation of information security incidents.
PMC12: Providing a legal framework for Protective Monitoring activities.	To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.

Table 1 - Minimum audit requirements

Additional control objectives

Note: During the risk assessment process, additional control objectives may be identified for inclusion into the set derived from CESG GPG No.13. These additional control objectives must be recorded in the protective marking schema.

Minimum control objectives

The minimum control objectives that are to be applied are in the Protective monitoring schema template. These control objectives are provided as a template for the author of the protective marking schema to fill in, notes are provided and once completed can be used as part of the description of the protective monitoring solution presented to the system Accreditor in the RMADS.

Where a minimum control objective cannot be met (for example, due to an implementation restriction or where the risk does not justify the control) it must be recorded as an exception (a template is provided here).

Note: This is generic set of control objectives and the templates provided in section A.1 and A.2 are designed for the author of the protective marking schema to customising based on the guidance provided in this document, CESG GPG No.13, the ICT system and associated risk assessment.

Control objectives extensibility

It is important to ensure that there is a mechanism in place to review, update or extend the protective monitoring controls once an ICT system is in live operation. This will occur when an ICT system undergoes the re-accreditation process, further details of which can be found in the Accreditation Framework.

Minimum audit requirements

The minimum audit requirement is specified in CESG GPG No.13 where the following provides the audit criteria which **must be** captured in the protective monitoring schema (a template table is provided here):

- The retention period of any protective monitoring data captured;
- Details on when log checks are to be carried;
- Details on when the protective monitoring system is to be manned;
- Details on when the system is to be subject to compliance review;
- Details on the reporting structure (refer to Reporting Structure), which should be specified in terms of a weekly, monthly or annual report.

Baseline Control Set and implementation of controls objectives

Table 2 defines the minimum controls which **must be** implemented to achieve the baseline controls set out in HMG IA Standard Numbers 1 & 2 – Supplement: Technical Risk Assessment and Risk Treatment.

Control	Baseline Control	Notes
10.10.1 Audit logging	In accordance with SPF Departments must ensure that ICT systems are capable of producing records of user activity to support monitoring, incident response and investigations.	Routine user activity such as log-on and log-off, log-on failures, keyboard inactivity, password change, object permissions change, read/write access to objects, import/export, print, object save and deletion.
10.10.2 Monitoring system use	Departments must develop and implement procedures to monitor use of systems and services by users to support incident response and investigation activities.	Establish baseline activity within the environment and develop auditable events outside this baseline activity.
10.10.3 Protection of log information	Audit logs must be protected in accordance with their sensitivity or protective marking.	The BIL of log information captured must be documented in the ICT system's Business Impact Assessment (BIA).
10.10.4 Administrator and operator logs	ICT systems must be capable of generating audit logs for all system users including system administrators.	Log collection and storage.
10.10.5 Fault logging	Departments must log and review system faults at regular intervals.	System management activity.
10.10.6 Clock synchronisation	Departments must implement a reliable means to keep all server and device clocks of the ICT System in synchronisation.	Establish time server.

Control	Baseline Control	Notes
13.2.3 Collection of evidence	In accordance with Security Policy Framework MR 9 Departments must have 'a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system, that may be required for legal and management purposes'.	How is the integrity of the collected data assured? How is collected data stored to prevent unauthorised access?
15.3.1 Information system audit controls	Departments must implement plans and controls to ensure that audit and compliance checks do not adversely affect the business operation of an ICT system.	Minimum impact on services is required. Does this mean no degradation of service?
15.3.2 Protection of information system audit tools	System audit tools must be protected to prevent their use for unauthorised purposes.	Installed and controlled in a physically separate environment with protected network connectivity.

Table 2 - Baseline controls to achieve protective monitoring

With Table 2 in mind CESG GPG No.13 outlines a number of options which should be consider when translating the identified control objectives into a protective monitoring solution which can be implemented in an ICT system.

The following provides the typical list of components which can be put together to deliver a protective monitoring solution:

- Security Information and Event Management (SIEM) system, which includes:
  - Log collection;
  - Log analysers;
  - Filtering, query and pattern matching tools;
  - Reporting tools;
  - Computer forensic tools;
  - Network management system;
- Intrusion Detection and Prevention System (IDS/IPS);
- Network Intrusion Detection System (NIDS);
- Host Intrusion Detection System (HIDS);
- Wireless Intrusion Detection System (WIDS).

A template is provided here to capture all the accounting items to be collected and where those items are collected.

Reporting Structure

Protective monitoring is only effective if there is a clear and effective reporting structure is in place to ensure that any alerts generated by the protective monitoring solution are escalated to the relevant people.

Note: The protective monitoring solution must fit into the overall IT Security Incident Management plan; refer to the IT Security Incident Response Plan and Process Guide for further details.

Service Validation

Once the protective monitoring schema has been generated and approved by the system Accreditor, the next step in delivering an effective protective monitoring solution is ensuring that the service provided is working as planned and that it is effectively gathering the data. This part of the protective monitoring solution must be document and should contain the following:

- Details on the initial operational capability and the start date;
- A defined series of service review points, specifically identifying the review of the control sets and the validation of data gathered;

- A defined criteria for spurious or unnecessary data that should be identified during the validation period and removed from the log reporting/alerting mechanism;
- Details on the full operational capability and the start date. At the point the protective monitoring service is fully operational, no changes may be made to the service without the approval of the system Accreditor.

Protective monitoring schema template
Minimum control objective

This section of the template captures the implementation details and compliance evidence for each protective monitoring control (PMC) specified in CESG GPG No.13. A minimum control object for each PMC is entered and is intended to provide an initial starting position.

Minimum control objective for PMC 1

For PMC 1 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Accurate time in logs.	[Insert additional notes/test as required.]		
Control Description			
Provide a means of providing accurate time in logs and synchronisation between system components to facilitate collation of events between those components. The error margin for time accuracy is to be specified.	[Use any of the following: Providing a master clock system component which is synchronised to an approved time source (e.g. GSi time source); Updating device clocks from the master clock using the Network Time Protocol (NTP); Record time in logs in a consistent format (Universal Co-ordinated Time (UTC) is recommended)]		
Objective			
Provide a centralised, single time reference for all components that are subject to monitoring.	Any of the previous mechanisms may be used and an existing clock source within the support environment should be used where possible.		
Risk Level			
VERY LOW/LOW/ MEDIUM	[Insert Risk level]		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 2

For PMC 2 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Recording of business traffic crossing a boundary.	[Insert additional notes/test as required.]

Control Description			
Provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.	[Insert additional notes/test as required.]		
Objective			
Ensure only authorised traffic is passed into and out of the PM environment.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	Insert Risk level		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 3

For PMC 3 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Recording relating to suspicious activity at the boundary.	[Insert additional notes/test as required.]
Control Description	
Provide reports, monitoring, recording and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour.	[Insert additional notes/test as required.]

Objective			
Identify potential or actual attempts to access the ICT System environment by an unauthorised individual who is external to the environment	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*[Insert Risk level]*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 4

For PMC 4 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording on internal workstation, server or device status.	[Insert additional notes/test as required.]		
Control Description			
Detect changes to device status and configuration.	[Insert additional notes/test as required.]		
Objective			
Identify and report authorised and unauthorised changes to the configuration of devices in the environment.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 5

For PMC 5 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording relating to suspicious internal network activity.	[Insert additional notes/test as required.]		
Control Description			
Monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated to the internal network.	[Insert additional notes/test as required.]		
Objective			
Identify internal and external attacks on the environment network.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 6

For PMC 6 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Recording relating to network connections.	[Insert additional notes/test as required.]
Control Description	
Monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.	[Insert additional notes/test as required.]
Objective	

Identify, monitor and audit temporary connections to the environment.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 7

For PMC 7 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording on session activity by user and workstation.	[Insert additional notes/test as required.]		
Control Description			
Monitor user activity and access to ensure they can be made accountable for their actions.	[Insert additional notes/test as required.]		
Objective			
Detect unauthorised activity and access that is either suspicious or is in violation of security policy.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 8

For PMC 8 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	

Recording on data backup status.	[Insert additional notes/test as required.]		
Control Description			
Provide for a previously known working state of information assets to be identified and recovered.	[Insert additional notes/test as required.]		
Objective			
Implement and audit backup and recovery procedures.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 9

For PMC 9 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Reporting on the status of the audit system.	[Insert additional notes/test as required.]		
Control Description			
Event reporting.	[Insert additional notes/test as required.]		
Objective			
Provide a mechanism for reporting in near real-time.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 10

For PMC 10 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Alerting critical events.	[Insert additional notes/test as required.]		
Control Description			
Maintain status of the protective monitoring system and its collected accounting data.	[Insert additional notes/test as required.]		
Objective			
Ensure the integrity and proper management of the protective monitoring system.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 11

For PMC 11 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Alerting critical events.	[Insert additional notes/test as required.]		
Control Description			
Maintain status of the protective monitoring system and its collected accounting data.	[Insert additional notes/test as required.]		
Objective			
Ensure the integrity and proper management of the protective monitoring system.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation

[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 12

For PMC 12 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Providing a legal framework for Protective Monitoring activities.	[Insert additional notes/test as required.]		
Control Description			
Ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.	[Insert additional notes/test as required.]		
Objective			
Maintain legal and statutory obligations.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Exceptions

The exceptions to the minimum baseline requirements must be recorded, based on the following template table.

Serial	Protective Monitoring Control	Control Detail	Reason for non-compliance
[Insert details of those controls that will not be implemented as a result of reviewing the protective monitoring controls for each of the defined levels to show which controls either cannot be implemented for technical reasons, or as a result of a risk management decision. Delete this row on completion of table.]			

Audit regime

The audit regime which forms part of the protective marking solution must be recorded based on the following template table:

Risk Level	Log Retention Period	Log Checks	Console Manning	Compliance Review Period	Report Production

Accounting items

The following table provides a template to capture all the accounting items to be collected in an ICT system, its source and alerting details.

PMC #	Cat	Ref	Record events	Include in report	Alert on event	Method	Notes in Environment PM policy	Accounting items (defined in GPG13)	Sources and notes	Logging application requirement	Tags	Predicate	Specific Events: Audit	Specific Events: Errors & Warnings	Specific Events: Protocol errors

Security Log Collection

Security Log Collection

systems and services must adequately create and retain event data as part of the DETECT portion of the Cabinet Office's Minimum Cyber Security Standard (MCSS).

Related information

Logging and monitoring on page 192

Cyber Security Logging Platform

The Cyber Security team operate a centralised, scalable, multi-tenant, cloud-based log collection and forwarding system for infrastructure (non-application level) log data.

The platform can receive, store, index, filter, search, alert and re-forward log data from any source (including supplier systems).

Additive technology supply chain

The security log collection principles are designed to be met through technology supply chain as opposed to each system individually.

For example, where the principles require the logging of DNS traffic, this could be achieved within a corporate device ecosystem by logging at the end user device itself, or by configuring the end user device to use a corporate DNS server that logs instead. You may decide to do both, because some DNS queries can go out without the DNS server (for example in the case of a corporate VPN that is not always on).

Where a platform exists, it should provide some assurance to all its consumers that makes clear what logging it collects and what needs to be logged by its tenants.

For example, if a cloud platform allows you to spin up arbitrary virtual machines, but guarantees that all network traffic must pass via a web proxy to go out, which logs, then the cloud platform can tell you that Principle 5: Network Events and Principle 3: Infrastructure Events are logged, but that you need to provide Principle 1. Authentication Events. The platform may even provide you with a base virtual machine which have logging for authentication events built in, meaning that you don't need to provide any logging at that level.

Principles

We have created a series of security log collection principle requirements for the . If you have any questions or comments, get in touch: .

To enable ease of referencing, but not to imply priority order, each item is assigned a reference.

1. Authentication events

- a: login successes and failures
- b: multi-factor authentication success and failures
- c: logouts
- d: session creation
- e: session timeout/expiry
- f: session close

2. Authorisation events

- a: group/role creation, modification or deletion
- b: group/role membership changes (addition or subtraction)
- c: group/role elevation (for example, if a user is able to temporarily assume a higher privilege to conduct a finite amount of work)

3. Infrastructure events

Infrastructure is defined as underlying resources, whether a logical switch, server or through to a containerised compute resource in the cloud, upon which end-user or application logic is overlaid.

- a: power/service on / off
- b: creation/registration and deletion/de-registration, including suspension/hibernation if applicable
- c: software update events/status
- e: IP address allocation/deallocation
- f: Firewall/routing rule creation, modification or deletion
- g: Network change events (for example addition or removal of virtual networks or interfaces)

4. Domain name service queries

- a: successful and unsuccessful queries
- b: recursive lookup status
- c: infrastructure node / end-user device registration / de-registration (if applicable)

5. Network traffic events

- a: successful and unsuccessful inbound service daemon connections
- b: unsuccessful outbound connections where the network traffic is *not* associated to an inbound request

6. Contextual security related events

In context and where present, technology may generate events pertinent to security and these must be captured.

For example, operating system patch state information from end-point protection detections through to encryption states within storage arrays.

7. Log transmission to the Cyber Security Logging Platform

- a: All log data must be sent to the Cyber Security owned log platform unless all principles have already been met through the deployment of a holistic locally deployed and monitored Security Information and Event Management (SIEM) solution.

Where 7(a) is true, the Cyber Security team will advise in context what information must be sent from the in-place SIEM to the Cyber Security Logging Platform.

Enterprise IT - Infrastructure

We have developed a series of logging requirements for Enterprise IT infrastructure, such as underlying networks, network services and directory services at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

Baseline Maturity Tier

1. User directory services

Log Collection Principle(s): 1, 2

User directory services (such as Active Directory (AD), Azure Active Directory or OpenLDAP must create and forward Authentication and Authorisation events from the directory service itself. (Normal authentication and authorisation events for the underlying operating system and server should be forwarded as appropriate.)

For example:

- An administrator logging onto the AD server using the local end-user device's administrator account should result in an authentication event for the machine being sent.
- A directory admin logging on to the AD service from their end-user device without logging into the local machine should generate an authentication event for the directory.

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (changes to ACL's, granting of new roles in RBAC models)
10. Privilege escalation events (use of sudo, UAC)
11. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Productivity Suite security logs

Log Collection Principle(s): 1, 2, 3, 6

Productivity suites (such as or Microsoft Office 365) must create and forward all security-related log data (as defined by the vendor), including unsuccessful Authentication and Authorisation events.

For example, within an Office 365 tenancy with Conditional Access enabled and set to require multi-factor authentication when a user device is perceived to be outside of the corporate network and such prompt is made and the outcome of that challenge.

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded.

1. Client IP address
2. Query
3. Query response content including:
    a. Returned record(s) or NXDOMAIN

   b. Authoritative nameserver
4. Query response code
5. Zone and/or view identifier (if local zone response and/or multiview)

This remains true for where nodes (for example, servers) may bypass internal DNS services.

4. Web proxy access logs

Log Collection Principle(s): 5

Where web traffic proxies exist, access logs must be created and forward and must, include the following variables:

1. Authenticated user name
2. Client IP address
3. HTTP method (for example, `CONNECT GET`)
4. Full destination/target URL
5. Connection return status code (for example, 200 or 403)
6. Size of response

5. File server authentication, authorisation and access logs

Log Collection Principle(s): 6

Where file service exist, sufficient log data must be created and forwarded, including sufficient data to satisfy the following:

1. Detect permission changes and the user who changed such
2. Detect all file/folder changes and the user who changed such
3. Detect all file/folder read/open and the user who did such

6. Security-related event logs for all server operating systems

Log Collection Principle(s): 6

Security-related event logs from all servers (whether virtualised or physical) operating in a 'server' role:

- [additional information pending]

7. Allocation of IP address leases from DHCP services

Log Collection Principle(s): 3, 5

DHCP services must be configured to create and forward the following:

1. Successful client DHCP requests, including:
   a. Requesting client MAC address
   b. DHCP scope identifier
   c. IP address leased
   d. IP address lease duration
2. Unsuccessful client DHCP requests, including:
   a. Requesting client MAC address
   b. DHCP scope identifier (if applicable for unsuccessful request)

8. VPN concentrator activity data

Log Collection Principle(s): 3, 5

Where a end-user device VPN concentrator is in use, connection-related log data must be created and forwarded:

1. Success or unsuccess status
2. User/certificate identifier
3. Client IP address
4. Concentrator identifier

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded:

1. Client IP address
2. Firewall/router identifier
3. Request response code
4. Request content, including:
   a. IP protocol (for example, ICMP)
   b. Destination/target port
   c. Destination/target IP address
   d. Destination/target hostname address (if reverse lookup performed)

2. Internal DNS namespace zone content

Log Collection Principle(s): 4

Internal domain name spaces must ultimate forward, in an RFC5936 (DNS Zone Transfer Protocol (AXFR) compatible format including all information described in the RFC.

3. DHCP scopes (and the functional segmentation of each)

Log Collection Principle(s): 5

Machine-readable DHCP scope exports (and surrounding metadata/description of the purpose of each scope) must be created and forwarded.

4. Endpoint protection security logs

Log Collection Principle(s): 6

Security log data (as defined by the vendor) must be created and forwarded.

5. Mobile device enrollment activity

Log Collection Principle(s): 1, 2, 3, 6

Where a mobile device management solution is used and end-user devices register/enrol and de-register/de-enrol with it, enrollment data should be created in and forwarded:

1. Enrolment or un-enrolment event type
2. End-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
3. End-user account name (if applicable)

Enterprise IT - Mobile Devices

We have developed a series of logging requirements for Mobile Devices (also known as End-user Devices), such as thin-clients, desktops, laptops, tablets and mobile smart phones at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

Baseline Maturity Tier

1. Device power events

Log Collection Principle(s): 1

Devices must create and forward local power events.

- a: power on (including good or bad state)
- b: power off (including if restart)
- c: disk encryption state

2. User identification activity

Log Collection Principle(s): 1, 2

Devices must create and forward local Authentication and Authorisation events.

These event types must be logged and forward:

- a: account creation
- b: account lockout
- c: account unlock
- d: account authentication failures
- e: account authentication successes after 3 or more failures
- f: account password changes
- g, group membership addition / deletion (in particular, any group that gives admin access)
- h: group creation
- i: privilege modification for users (changes to ACL's, granting of new roles in RBAC models)
- j: privilege escalation events (use of sudo, UAC)
- k: multi-factor authentication state, such as:
  - 1: enabled
  - 2: disabled
  - 3: reset/rotation
  - 4: recovery method used

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded, even where they are captively routed through central enterprise IT DNS services that forward comparable log data.

- a: device IP addresses (local and public, if known/applicable)
- b: VLAN tag for associated network interface (if known)
- d: query
- e: query response content including
  - 1: returned record(s) or NXDOMAIN
  - 2: authoritative nameserver
- e: query response code

4. Security-related operating system event data

Log Collection Principle(s): 6

Any additional security-related logs, as defined by NCSC's Logging Made Easy template, from all end-user devices operating a Microsoft Windows operating system must be created and forwarded.

Comparable events from other operating systems (for example, Apple macOS or QubesOS) to that described by NCSC's Logging Made Easy template must also be created and forwarded.

5. Security-related software event logs

Log Collection Principle(s): 6

Security-related logs from any local endpoint protection software (for example, anti-virus) should be forwarded.

- a: detection information
  - 1: process/binaries
  - 2: detection criteria (for example, malware type)
- b: reaction information (for example, quarantine)
- c: 'last scan' information

- d: signature information

6. Network information

Log Collection Principle(s): 5

Devices must create and forward sufficient data to record the network posture around the device.

- a: IP address of DHCP server
- b: IP address leased
- c: IP address subnet leased
- d: IP address lease duration
- e: Network interface identifier
- f: DHCP response instructions, for example:
  - 1: DNS servers
  - 2: Proxy servers

7. VPN dial-up activity

Log Collection Principle(s): 5

Where dial-up VPN is in use, connection-related log data must be created and forwarded.

- a: success or unsuccess status
- b: VPN concentrator domain name and IP address
- c: user/certificate identifier(s) used
- d: network interface identifier

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded.

- a: client IP address
- b: network interface identifier(s)
- c: request response code
- d: request content, including:
  - 1: IP protocol (for example, ICMP)
  - 2: destination/target port
  - 3: destination/target IP address
  - 4: destination/target hostname address (if reverse lookup performed)

2. Command/executable runtime information

Log Collection Principle(s): 6

Log data to reflect the launching and subsequent processing activity stemming from user, or user profile, triggered commands/executables.

- a: user identifier(s)
- b: device identifier(s)
- c: command executed
- d: executable launched

3. Configuration information

Log Collection Principle(s): 6

Devices must create and forward sufficient data to record the changing state of device configurations.

- a: profile or GPO changes

- b: conflict detection

Hosting Platforms

We have developed a series of logging requirements for hosting platforms, such as virtualised and/or containered compute with associated supporting services such as database and queuing services at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

Baseline Maturity Tier

1. User directory services

Log Collection Principle(s): 1, 2

User directory services must create and forward Authentication and Authorisation events from the directory service itself.

User directories within hosting environments can be rich and diverse, such technologies include:

- Active Directory (AD)
- Azure Active Directory
- OpenLDAP
- Amazon Web Services (Accounts and Incognito)
- Okta
- Auth0
- Github.com (acting as an identity provider)
- (acting as an identity provider)
- Local user stores within operating systems

These event types must be logged and forwarded:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Bastion/Jump/Action-proxy services

Log Collection Principle(s): 1, 2, 6

Bastion/jump boxes that act as a management consolidation route and should be highly auditable therefore must create and forward security-related event data:

1. SSH keypair generation/revocation, including:
    a. Public key
    b. Keypair 'friendly name' / identifier
2. Account login attempts:
    a. Public key
    b. Username

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded:

1. Client IP address
2. Query
3. Query response content including:
    a. Returned record(s) or NXDOMAIN
    b. Authoritative nameserver
4. Query response code
5. Zone and/or view identifier (if local zone response and/or multiview)

This remains true for where nodes (for example, servers) may bypass internal DNS services.

4. Web proxy access logs

Log Collection Principle(s): 5

Where web traffic proxies exist, access logs should be created and forward and must, include the following variables:

1. Authenticated user name (if applicable)
2. Client identifiers:
    a. IP address
    b. Reverse lookup client name (if applicable)
3. HTTP method (for example, CONNECT GET)
4. Where available, full destination/target URL or SNI value
5. Connection return status code (for example, 200 or 403)
6. Size of response

5. Hypervisor events

Log Collection Principle(s): 3, 6

Hypervisors manage virtualised compute resources and are entrusted to segregate the same. All instructions to hypervisors should be highly auditable.

1. Virtual machine creation (including templates)
    a. Identifier(s)
    b. Operating system image information
2. Virtual machine 'power' events:
    a. Identifier(s)
    b. 'Power' on
    c. 'Power' off (including restart flag)
3. Virtual machine deletion
    - Identifier(s)
4. Virtual machine resource modification events:
    a. CPU addition/removal
    b. RAM addition/removal
    c. Networking additional/removal
    d. Storage mount/dismount/resize

6. Orchestrator events

Log Collection Principle(s): 3, 6

Orchestrators such as Cloud Foundry and Kubernetes create and manage a variety of technology resources to facilitate an application environment.

1. Resource creation (including templates)
    a. Identifier(s)
    b. Resource type
    c. Operating system image information (if applicable)
2. Container 'power' events
    a. Identifier(s)
    b. 'Power' on
    c. 'Power' off (including restart flag)
3. Resource deletion
    - Identifier(s)
4. Resource modification events:
    - Identifier(s)

7. Allocation of IP address leases from DHCP services

Log Collection Principle(s): 3, 5

DHCP services must be configured to create and forward the following:

1. Successful client DHCP requests, including:
    a. Requesting client MAC address
    b. DHCP scope identifier
    c. IP address leased
    d. IP address lease duration
2. Unsuccessful client DHCP requests, including:
    a. Requesting client MAC address
    b. DHCP scope identifier (if applicable for unsuccessful request)

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded.

1. Client IP address
2. Firewall/router identifier
3. Request response code
4. Request content, including:
    a. IP protocol (for example, ICMP)
    b. Destination/target port
    c. Destination/target IP address
    d. Destination/target hostname address (if reverse lookup performed)

2. Internal DNS namespace zone content

Log Collection Principle(s): 4

Internal domain name spaces must ultimate forward, in an RFC5936 (DNS Zone Transfer Protocol (AXFR) compatible format including all information described in the RFC.

3. DHCP scopes (and the functional segmentation of each)

Log Collection Principle(s): 5

Machine-readable DHCP scope exports (and surrounding metadata/description of the purpose of each scope) must be created and forwarded.

4. Endpoint protection security logs

Log Collection Principle(s): 6

Security log data (as defined by the vendor) must be created and forwarded.

5. Security-related logs for all Windows-based end-user devices

Log Collection Principle(s): 6

Security-related logs, as defined by NCSC's Logging Made Easy template, from all end-user devices operating a Microsoft Windows operating system must be created and forwarded.

6. Mobile device enrollment activity

Log Collection Principle(s): 1, 2, 3, 6

Where a mobile device management solution is used and end-user devices register/enrol and de-register/de-enrol with it, enrollment data should be created in and forwarded.

1. Enrolment or un-enrolment event type
2. End-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
3. End-user account name (if applicable)

7. VPN concentrator activity data

Log Collection Principle(s): 3, 5

Where VPN services are in use, connection-related log data must be created and forwarded.

1. Success or unsuccessful status
2. User/certificate identifier
3. Client IP address
4. Concentrator identifier

8. Pipeline events

Log Collection Principle(s): 1, 2, 3, 6

Continuous integration and continuous deployment pipelines obey instructions to manage hosting environments and are a privileged position to oversee all tenant resources, they must be highly auditable to clarify activity and attribute the same.

1. Source identifier(s)
    a. User(s)
    b. Repository
2. Activity events
    a. Resource creation
    b. Resource destruction

Log entry metadata

Any security log data collected must comply with these metadata standards to ensure we are able to consistently interpret log data using other systems.

Time/date

- a: all log events must be time stamped in the common log timestamping format as defined by ISO8601 `[dd/MM/yyyy:hh:mm:ss +-hhmm]` where the fields are defined as follows:
    - 1: dd is the day of the month
    - 2: MMM is the month

    - 3: yyyy is the year
    - 4: :hh is the hour
    - 5: :mm is the minute
    - 6: :ss is the seconds
    - 7: +-hhmm is the time zone
- b: systems must use an automated time syncing protocol (such as NTP) with an external time source to ensure it is not subject to 'time drift' that may impact the accuracy of time stamping.

Formats

Only the following log file formats should be used:

- a: Apache Common Log Format
- b: NCSA (Common or Access, Combined, and Separate or 3-Log)
- c: Windows Event Log
- d: W3C Extended Log File Format
- e: W3C Extended (used by Microsoft IIS 4.0 and 5.0)
- f: SunTM ONE Web Server (iPlanet)
- g: IBM Tivoli Access Manager WebSEAL
- h: WebSphere Application Server Logs

Security Log Collection Maturity Tiers

systems and services must adequately create and retain event data as part of the DETECT portion of the Cabinet Office's Minimum Cyber Security Standard (MCSS).

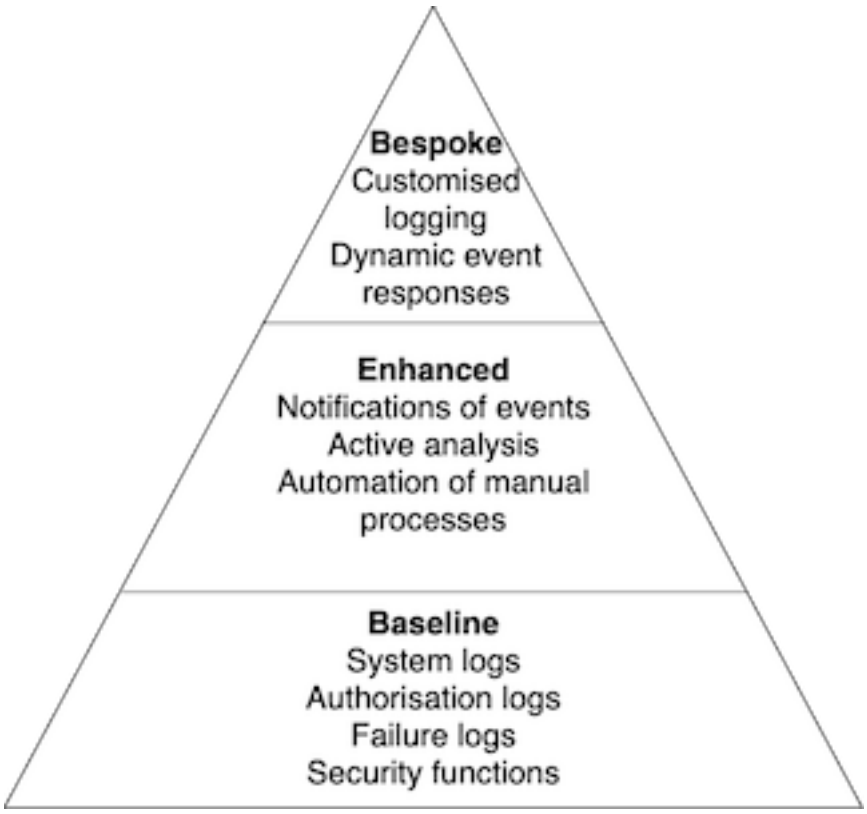
Three tiers have been developed to reflect the breadth and complexity of collecting and forwarding log data.

These three tiers represent different levels of risk profile, and concern about a system. All systems should be capable of meeting the baseline standard.

Some systems are at greater likelihood of compromise. This is due to factors such as age or public threats. Other systems would have a higher impact if compromised. This is due to the systems being sensitive or having distinctive perceived value. Such systems should be monitored to a higher standard.

The extent to which a security log collection process implements the monitoring requirement indicates the logging maturity.

Each level of monitoring - or 'tier' - has characteristics that are 'in addition' to lower level tiers. For example, a system operating at the Enhanced tier should also meet the requirements of the Baseline tier.



Baseline

The baseline tier is the generally minimum expected for event types. It includes data that should be generated, recorded, and forwarded for onward analysis. It applies to all of the systems. In most cases, this requirement may be met through the underlying platform(s) on which the systems are built.

This tier covers the broad spectrum of events that can reasonably be used to detect compromise. It allows the defensive cyber team to respond appropriately before significant impact.

Enhanced

The enhanced tier, in conjunction with the baseline event types, provides earlier notification of attempted compromise. It enables gathering of more information to detect stealthier or more capable attackers.

Bespoke

The bespoke tier concerns systems that are critical to the security, stability and statutory function of the , or that contain highly sensitive data. In this tier, systems must generate additional bespoke (customised) event types. These event types are typically agreed in context between the Cyber Security team and the associated product or service team. The objective is produce logging that reliably identifies and captures key nuance and contextual security monitoring data, based on applicable threats and risks.

Control of operational software

Guidance for using Open Internet Tools

This information applies to all staff and contractors who work for the .

This guidance gives you:

- An overview of Open Internet Tools (OIT).
- A quick checklist to help you decide if you can use an OIT.
- Reasons why you might, or might not, want to use an OIT.

- Things you must think about when using an OIT, such as data protection.
- Information on who to contact if you would like help or advice.

Note: To access some of the links in this guide you'll need to be connected to the Intranet.

Overview

Open Internet Tools (OITs) are applications or services from suppliers outside the . They often have the following characteristics:

- they are general purpose. This means they are not specific to the . Other organisations can use them
- they are accessed using the Internet, usually through a web browser. This means that if you have Internet access, you are able to connect to the tools
- they have a basic 'free-to-use' version. This means that you are able to use some or all the capabilities, but with some constraints. For example, an online word-processor might limit you to 5 documents in your account
- they have one or more 'paid for' versions. By paying for the tool, you unlock some or all the constraints

Quick checklist

To help you decide if you can use an OIT to work on an task, consider the following questions:

- is the task information subject to specific rules or requirements in your part of the ?
- is the task information classified as anything other than or?
- does the task information include any data identifiable as being about someone?
- is this the first time anyone has used the tool for business?
- does the tool need access to your account or other data you can access? For example, does it ask to use your Google or Microsoft Office account?
- does the tool install a web-browser extension?
- is the tool a plug-in for existing OITs we use, such as Slack, Confluence, or Jira?
- could there be damaging consequences if the task information you work with using the tool is:
  - lost
  - stolen
  - published in the media
- are you prevented from exporting all the data from the tool?
- are you prevented from deleting all the data from the tool when you finish working on the task?

If the answer to *any* of these questions is "Yes", you might not be able to use the OIT.

When you have all the answers, request formal approval to use the OIT from your Line Manager. Do this *before* using the OIT.

Why OITs are an opportunity

OITs offer some significant advantages for you and the , including:

- enabling you to work the way you want to, more effectively
- usually cheaper than buying or building and supporting a dedicated tool
- no need to build or support the tool
- good use of open standards, such as file formats
- reduced need to have specific hardware or software on computers
- rapid patching to address security issues
- easy updates and deployment of new features
- a large pool of help and support
- easy access, whenever you have a network connection
- increasing availability of some or all capabilities when disconnected from the network

Why OITs are a risk

OITs also pose some threats or risks, including:

- dependency on the tool and supplier
- security of access to the tool
- security of information stored within or processed by the tool
- potential difficulty of enhancing or customising the tool for -specific requirements

But as long you consider the threats or risks, and address them, OITs provide many benefits for you and the .

Summary

With careful use, OITs help you to work more effectively and efficiently. Think about them as serious and preferable options for performing tasks.

Using OITs

This guidance helps you:

- understand the conditions or constraints that apply to a tool, or a task performed using a tool
- identify and address threats or risks posed by a new tool

Privacy and personal information

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Don't use OITs for storing personal data until you have addressed the need to get consent first. Check if using the OIT might need an update to existing privacy policies or notices. Don't use OITs if unlawful disclosure of the information they process might cause damage or distress.

Data protection legislation might also limit *where* you can process personal data. An OIT should have a privacy statement that describes where it stores or processes data. Be ready to contact the OIT provider for more information about this aspect of their service.

Be sure you can fulfil your data protection responsibilities when using an OIT. It might be helpful to complete a Privacy Impact Assessment (PIA).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

Classification and security

An OIT can only store or process information classified at level.

Think about the information you work with. What would happen if you lost it, or it's stolen, or published in the media? Suppose the information was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is "No", then it's probably OK to use OITs to store or send that information.

Think also about information moving across the Internet. The data might be safe within the and in an approved OIT. But what about the connection between the two? Sending information might involve insecure networks. Be aware of the security implications. Check that enough suitable security measures are in place to protect the information. For example, check for encryption of network connections using SSL/TLS. A simple way to do this is to look for the secure connection indicator in your web browser:

You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is Principle 2 of the Government Security Classifications. The trusts you to work with information. In the same way, you're trusted to make a reasoned judgement about whether it's safe to use an OIT.

Useful help for deciding what is OK is in existing social media guidance. While it's more about how to act online, the principles are helpful for OITs.

Remember that it is impossible to delete information after it's released in public.

For more information about IT Security, look on the Intranet here.

Storage and data retention

Laws and regulations make the and its employees responsible for managing information. Some examples include:

- the Freedom of Information Act
- the Data Protection Act and General Data Protection Regulation
- the Public Records Acts

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate systems helps us, because:

- we can provide evidence about decisions
- we understand the information held, and where to find it
- we can transfer records to The National Archives

Always store information in systems. If you use an OIT, make sure the key information is also stored in an appropriate system. Guidance on what you must keep is available. At regular and convenient intervals, transfer the information to an appropriate system. Do the same when you finish the work. Don't forget to remove any redundant information from the OIT.

Most OITs let you export your data. You can then store it on an appropriate system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the Information Management Policy. There is also help on responding to requests for information.

Service and support

OITs are often intuitive and reliable. But that doesn't mean they are always available and always work as you expect. The can't provide technical support or ensure service availability for them. Always have another way of working if the OIT is not available for some reason or for any length of time. In other words, don't let an OIT become business critical.

Check the OIT usage agreement to find out more about the service and support available.

Note: The cannot provide technical support for OITs.

Common OITs

There are already many OITs used across the . Permission to use an OIT might vary, depending on where you work in the . For example, some teams must not access or use some OITs, for security or operational reasons.

Note: Check with your Line Manager if you want to use an OIT for your work, *before* you use it.

Getting help

For further help about aspects of using OITs within the , contact:

Subject	Contact
Classification and Security	Cyber Security team
Storage and Data Retention	Departmental Library & Records Management Services (DLRMS)
Information Assurance	Compliance and Information Assurance Branch
Personal Data	Disclosure Team

Technical vulnerability management

Implementing security.txt

Domains where the is primarily responsible for cyber security redirect the `/.well-known/security.txt` location to the central `security.txt` file.

This redirection be accessible from the public Internet whether or not the underlying applications or systems are. For example, `https://test.not-production.justice.gov.uk` may be a web-application requiring authentication, however `https://test.not-production.justice.gov.uk/.well-known/security.txt` still be accessible without authentication.

security.txt

`/.well-known/security.txt` `HTTP 301` (permanent redirect) to `https://security-guidance.service.justice.gov.uk/.well-known/security.txt`.

For example, `https://www.prisonvisits.service.gov.uk/.well-known/security.txt` `HTTP 301` to `https://security-guidance.service.justice.gov.uk/.well-known/security.txt`.

`/.well-known/`

We use `/.well-known/` to house `security.txt` as RFC5785 defines it as a path prefix for "well-known locations" in selected Uniform Resource Identifier (URI) schemes.

Internal-facing domains

Internal-facing domains resolvable from the public Internet (for example, `intranet.justice.gov.uk` is based on `.gov.uk` with a publicly routeable IP address) also implement `security.txt` as described previously.

Non-production domains

Non-production domains resolvable from the public Internet (for example, a demonstration deployment of a digital service or prototype) also implement `security.txt` as described previously.

Vulnerability Disclosure Policy

The Security Vulnerability Disclosure Policy is published as part of the Digital & Technology blog.

Thanks & Acknowledgements

Where security researchers have submitted qualifying vulnerability reports and have accepted our offer to be publicly thanked and acknowledged for their efforts, they will be listed on the dedicated thank you page within the Digital & Technology blog.

Feedback

If you wish to provide feedback or suggestions on the Security Vulnerability Disclosure Policy, contact our security team: cybersecurity+vulnerabilitydisclosure@digital.justice.gov.uk.

The policy will naturally evolve over time; your input is welcome and will be valued to ensure that the policy remains clear, complete, and relevant.

h/t to https://www.bbc.com/backstage/security-disclosure-policy/

Vulnerability Scanning and Patch Management Guide

Introduction

This guide is designed to ensure that all IT systems and services developed, procured or operated by or on behalf of the have regular patching and maintain secure configuration. The document will provide steps to ensure that privileged users are able to patch systems effectively and according to the Service Level Agreements in the Patch

Management guide to reduce risks to IT systems. Unpatched vulnerabilities can be a major risk factor in organisations being compromised by threat actors. This page is the first in a series of three pages about vulnerability scanning and patch management within the .

Who is this for?

This guide is aimed at two audiences:

1. The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the Event, Problem, Incident and CSI (EPIC) Team.
2. Any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the .

Related guides

Further guidance on vulnerability scanning and patch management can be found in the following guides:

- The Vulnerability Scanning Guide explains the scanning requirements for the systems.
- The Patch Management Guide explains the patching requirements for the .

The base principles

All systems and applications **must** be scanned using commodity tooling for known vulnerabilities such as, but not limited to, OWASP Top 10 application issues.

Any issues found must be proportionally considered for remediation prior to progression into production.

'In-house' applications **must** be scanned for vulnerabilities during development. Normally this scanning would be automatic rather than requiring manual invocation.

The scanning **must** include build pipelines.

It **must not** be possible to release to production without a record of a current vulnerability scan, and associated mitigations or documented exemptions.

Tools such as OWASP ZAP may be useful in enabling automated scanning of applications.

What is covered?

Vulnerability scanning is the identification of potential vulnerabilities within an organisation's network and devices including its firewalls, routers, switches, servers and applications. It is an automated process and focuses on finding potential or known vulnerabilities which could be exploited by threat actors.

Patching is the application of a vendor-supplied or in-house developed security patch or fix to a known vulnerability. Patching can also refer to other ways of achieving the same goal, for example:

- Virtual patches.
- Removal of vulnerable services or functionality.
- Disabling and preventing access.

Patching may include recompiling applications to incorporate security updates. Patch updates may also be held in third party or other code libraries so you may need to locate these and update them.

All assets must be scanned and patched. The following assets are explicitly covered by this guide:

- **Internet facing websites:** Any open internet-facing websites operated by the .
- **End user client devices:** An end user client device is one that is normally used by a single person - the user. The device does not supply services to other users. Example devices include desktop PCs, laptops, tablets and mobile phones. If an end user device provides a service (for example, running a web server on a mobile phone), then it is considered to be an infrastructure device and is therefore subject to the same security requirements as infrastructure devices.

- **Infrastructure devices**: Devices that form part of the infrastructure of systems and services. Examples include edge firewalls, routers, networking equipment, servers and printers.
- **Digital services**: Any services provided by or operated on behalf of the digital services. Many services make use of third-party software libraries and imported code.
- **Applications**: All applications hosted on servers, external servers or on a cloud platform such as database services.

If you have a query about any assets not explicitly covered in this guide, please contact the Cyber Assistance Team.

Minimum software requirements

To meet the minimum requirements of this guide, all software used by the must be:

- Fully compliant with applicable Licenses and Terms of Use.
- Supported by applicable supplier packages (but refer to the following note).
- Removed from devices when no longer licensed or supported (subject to the change management approach).
- Capable of being patched in a suitably prompt fashion when security updates are made available, according to the severity of the vulnerability. Indicative timescales for the different vulnerability levels are provided in the Patching Schedule section of the Patch Management Guide.

Note: Commercial software will normally have support packages identified and agreed as part of the purchase (acquisition) and deployment process. Open Source software would not always have associated support packages. The decision to use a given software tool in a project or service must take into account what support packages are available to ensure that the tool remains viable and secure for the lifetime of the project or service. If a support package is not available - for example with Open Source software - then a risk evaluation must be performed to understand the business implications if the tool becomes unavailable or unsafe to use.

Vulnerability Scanning Guide
Introduction

This guide explains the scanning requirements for systems.

This guide is a sub-page to the Vulnerability Scanning and Patch Management Guide.

Scanning requirements

The should conduct the following scanning activities outlined in this guidance and in line with the requirements identified in this guide.

- If you are developing a system or application, you must ensure that they are scanned for vulnerabilities prior to live deployment and as part of approval for live deployment.
- If you are managing a live service, you must ensure that the system or application is scanned at specified intervals after deployment until it is withdrawn from service.
- The scanning frequency section in this guide gives the minimum scanning requirement, however the system or application itself may need to be scanned more frequently. Any specific scanning frequencies or requirements will be outlined in the system or application Information Risk Assessment Report (IRAR).
- Scanning must be conducted through automated vulnerability scanning tools that scan web applications, from inside or outside the system, to look for security vulnerabilities.
- The scanning process should consider the licensing and support status for an infrastructure device, its operating system, or any applications hosted on the device.
- Scans which take place one year before the expiry of a license or vendor support should flag the forthcoming expiry as requiring attention and remediation such as license renewal or equipment replacement.
- Examples of known vulnerabilities which must be scanned for include cross-site scripting (XSS), SQL injection, command injection, path traversal, and insecure server configuration.
- If scans identify vulnerabilities, patches must be applied according to the schedule described in the Patch Management guide.

For assistance with identifying, evaluating, and selecting appropriate tooling for scanning, contact the Security Team.

Note: Expired or missing license or support materials for a system or service are also considered to be vulnerabilities. The reason is simple - using a system or service without the necessary license might result in financial or reputational loss. Similarly, using a system or service without the necessary support in place might result in loss of availability, performance, integrity, confidentiality, or other problems.

Point in time scanning

By default, all applications and services should be scanned automatically, on a regular basis. However, there will be occasions where extra, 'Point in time' vulnerability scans are required. These provide an assessment of the vulnerabilities at that point in time.

An example might be following a significant configuration change or application update, and it is considered advisable to check for vulnerabilities at that point in time, rather than waiting until the next, scheduled check.

Web Check

In addition to specific scanning processes, the NCSC's Web Check services must be employed for all open internet facing websites operated by the . Web Check continuously scans these websites and provides regular reports to the . If you are responsible for developing or running a website for the , you must:

- Ensure that it is added to the HQ Web Check Account. Contact the Security team to be added to the Web Check Account.
- Ensure that any vulnerabilities identified are patched according to the Patching Schedule in the Patch Management guide.

Further information on the NCSC's Web Check service can be found here.

Scanning frequency

Scanning should be undertaken in line with the following indicative schedule for each system and equipment type.

System and equipment type	Minimum scanning frequency
Internet Facing Websites and Digital Services	Every week.
Infrastructure Devices	Every week.
Server Applications	Every week.
End User Clients	Every two weeks.

The actual minimum scanning frequency for a given service or system might be determined by a separate Service Level Agreement, contract, IRAR or other formal agreement. If there is a conflict with the Scanning Frequency defined in this guide, the contract, IRAR or other formal agreement takes precedence over this guide.

You need to ensure that scanning logs and results are made available to the Security Team () for subsequent analysis and potentially forensic investigation purposes.

Vulnerability alerts

Any problems picked up during scanning must be recorded and reported as a vulnerability alert. As a minimum, the alert should be reported to:

- The system owner.
- The person responsible for risks regarding the system.
- The person responsible for risks regarding the information accessed or processed using the system.
- The Security Team.

These vulnerability alerts must contain as a minimum:

- An alert identifier.
- A cross-reference to known vulnerabilities.
- A risk rating (refer to the following Vulnerability risk ratings section).
- A description of the fix, mitigation, or workaround, where known.
- A link to patch materials, if available.

- A status which is updated as necessary.
- Where to get further information.

Vulnerability risk ratings

Vulnerabilities are designated a severity rating (1-4) based on the level of risk they pose to the . The schedules defined in the Patch Management Guide for remediation are aligned with the risk exposure the vulnerabilities create to systems. The vulnerability ratings are based on the Common Vulnerability Scoring System (CVSS) which is aligned with the Cyber Essentials Scheme. If vendors use different terminology to define Critical or High Risk vulnerabilities, the following table should be used to define the CVSS score of the vulnerability:

Rating (Severity)	Values on CVSS	Definition
Critical (4)	9.0 - 10.0	High, with compounding issues or additional circumstances. An issue that will cause extreme financial or reputational damage.
High Risk (3)	7.0 - 8.9	A serious issue that is likely to cause severe financial or reputational damage.
Medium (2)	4.0-6.9	A significant issue that may cause financial or reputational damage.
Low (1)	0.0 - 3.9	An issue that is unlikely to cause financial or reputational damage.
Info	N/A	An issue with no immediate security implications.

Roles and responsibilities

Managed service

If you are responsible for a system or a service which is managed by a vendor, or a Managed Service Provider, the vendor may be responsible for scanning and alerting you of any vulnerabilities and providing patches. Please refer to the Patch Management Guide for more information. The specific responsibilities will depend upon the services provided by the vendor and any contractual agreements between the and the vendor.

The schedules for vendors to conduct vulnerability scanning and issue vulnerability alerts to the are outlined in this guidance.

- Scanning after Scheduled Patch Releases: Scan to take place within two business days from the implementation of the patch as required by the Patching Schedule Service Level Agreement in the Patch Management Guide. The must be alerted of any vulnerabilities within 1 business day of the scan being conducted.
- Scanning after Ad Hoc / Off Cycle Patch Release: Scan to take place within three business days from the implementation of the patch as required by the Patching Service Level Agreement in the Patch Management Guide. The must be alerted of any vulnerabilities within 1 business day of the scan being conducted.

The actual scanning schedule for a given managed service or system may be determined by a separate Service Level Agreement, contract, IRAR, or other formal agreement. If there is a conflict with the requirements in this guide, the contract, IRAR or other formal agreement takes precedence over this guide.

In-house developed

If you are developing or running a system or application in-house, you must make sure that it is scanned. Where centralised scanning is not possible, the system owner is responsible for ensuring that scans are undertaken with at least the frequency defined in this document and in sufficient depth to identify vulnerabilities in libraries, code or infrastructure configuration.

Contact details

Contact the Security Team for advice on risk, scanning and patching, to report a vulnerability alert, or to add a URL to the Web Check system: .

Patch Management Guide

This guide explains the patching requirements for systems once a vulnerability has been identified.

This guide is a sub-page to the Vulnerability Scanning and Patch Management Guide

The intent is to avoid compromise of systems because of vulnerabilities.

Related information

Technical Controls Policy on page 30

Patching of systems and equipment

This guidance must be followed for all systems and services developed or procured by the . It applies to all asset types including, but not limited to:

- Internet facing websites and digital services.
- End user client devices, such as Desktop PCs, laptops, tablets, and mobile phones.
- Infrastructure devices, such as networking equipment, servers, and printers.
- Applications.
- Internet-of-Things (IoT) devices.

In general, there are three options for patching:

1. The problem is serious or urgent, and must be mitigated as soon as possible.
2. The problem is important but not urgent; mitigation can wait until the next scheduled patching cycle.
3. The problem does not require mitigation in advance of changes introduced as part of normal system upgrades.

Note: The nature of the patching cycle will depend on what is agreed during development, deployment, and subsequent maintenance of the system or service.

Patching is the application of a vendor-supplied security patch. It can also refer to other ways of achieving the same goal. Examples include:

- Virtual patches.
- Removal of vulnerable services or functionality.
- Disabling and preventing access.

Patching might include recompiling applications to incorporate security updates. The updates might be in third party libraries or other code.

Always apply patches as soon as possible. Where this guidance mentions a time limit, you should apply patches no later than the time given. Some important or sensitive systems might need more urgent patching. For example, a system might need you to apply 'critical' or 'high risk' patches within 7 days.

Where patching or other mitigation is required, it must be applied in compliance with the Patching Schedule in this guide.

Operating systems and applications installed on systems must be:

- Licensed and supported.
- Removed from devices when no longer licensed or supported.
- Patched as soon as possible.
- Patched within no more than 14 days of an update being released, where the fix is for a 'critical' or 'high risk' vulnerability.

To ensure that patches are implemented on systems, you must either:

- Enable and use any vendor-provided automatic patch deployment mechanisms for the system.

- If automatic patch deployment is not available, apply patches manually according to the schedule outlined in this guide.

If a system or service, or a component it depends on, can no longer be licensed or supported, it should be reviewed within the timescale of the vulnerability scanning lifecycle, to determine what action to take. If the required license or support cannot be obtained, the system or service should be replaced by an alternative, or removed. If the system or service cannot be removed, then the issue should be raised through the patching exemptions process outlined in the Patching Exemptions section in this guide.

In summary:

- It must be possible to patch or mitigate an system or service. A clear, documented process must exist explaining how to patch or mitigate.
- Wherever possible, patching should be automated, or at least have minimum possible dependency on manual intervention.
- If a patch is not available, or cannot be deployed, then a suitable risk mitigation might be acceptable.
- Patching or mitigating a system or service might impact or be affected by other systemic components. These must be identified and addressed as part of the patch or mitigation process.

Digital services

For systems or services developed by the , it must be possible to patch or mitigate in order to address any vulnerabilities. To ensure this is possible:

- The Beta development stage must include a mechanism or process for a new or updated service to track and apply patches.
- Sufficient logs must be available from the new or updated service, so that security problems can be tracked from identification through to rectification.
- The patching process must also describe how to triage and action any problems.

Patching Schedule

The following Patching Schedule defines the indicative severity ratings and consequent timescales. All vulnerabilities must be remediated or patched in line with this schedule. By agreement and formal approval, alternative timescales for system patching, on a case-by-case basis, can be operated.

Note: The default is for patches to be applied as soon as possible. You should not normally delay patching because of concerns about possible issues with the patches themselves.

Patches and updates for security related devices must be treated as High Risk (3) at least, and implemented in accordance with this rating.

For ratings of High Risk (3) or Critical (4), the Risk Advisor team (contact through email) must evaluate the probability and impact, and use this to guide a 'tolerance' period, at the end of which a patch must be applied.

Where the rating is Medium (2) or lower, the patch can be deferred to the next scheduled maintenance or patching activity.

This schedule outline is considered a baseline. Some systems might require different patching schedules. These different schedules must be identified in the system's Information Risk Assessment Report (IRAR).

Table 3: Patching Schedule

Rating (Severity)	Infrastructure Devices; Server Applications; Digital Services	End User Client Devices	Web Check Reporting
Critical (4)	3-7 days after vulnerability alert released.	14 days after vulnerability alert released.	**Urgent:** Serious configuration problems that you should fix without delay and no later than 28 days after the vulnerability alert is released.
High Risk (3)	3-7 days after vulnerability alert released.	14 days after vulnerability alert released.	**Advisory:** Configuration problems that leave the site vulnerable. Patches should be implemented no later than 28 days after the vulnerability alert is released.
Medium (2)	28 days after vulnerability alert released.	28 days after vulnerability alert released.	**Informational:** Configurations that you could optimise, or information that you may find useful.
Low (1)	Next scheduled system upgrade (not to exceed 90 days).	Next scheduled system upgrade (not to exceed 90 days).	**N/A**
Positive (0)	N/A	N/A	**Positive:** Site configurations that conform to best practices.

Patch management processes

There are two patching and change management approaches in the .

Infrastructure and services provided by a Managed Service Provider (MSP)

Where services and infrastructure are provided by MSPs, the vendor is normally responsible for developing and implementing patches to identified vulnerabilities. Patches or a workaround must be provided by vendors to ensure the is able to meet the schedule for implementing patches.

If this is not possible, vendors must provide a firm statement that the patch or workaround cannot be made available within the timescale mandated for addressing the vulnerability. The vulnerability alert must then be escalated to the Risk Advisor team (contact through email) for help with acceptance, transfer, mitigation or avoidance.

Any patches to be deployed must go through the normal change management and approval process, and the changes recorded in the Service Management Tool.

Services and applications developed by in-house project teams

Where services and applications are developed by in-house project teams, patching and change management is addressed on a project-by-project basis. Changes are identified through awareness channels and scanning activities. These identify operational and security issues. A change management ticket must be created, detailing the change required. The project manager follows the change management process to determine how and when to implement the change, based on the security risk rating.

The patch review and approval is normally managed within the project team. If assistance is required, contact the Security Team.

If changes are urgent because a major security risk has been identified, the product, system, or service owner should ask a competent developer to investigate, and if possible create and implement a patch quickly. If the issue is more complex, Technical Architects, Security Architects and the Security Team might need to assist in the development of appropriate remediation plans.

Patches must be implemented according to the schedule in this guide. If this is not possible, the project team must provide an indication that the patch or workaround cannot be implemented within the timescale mandated for addressing the vulnerability. This delay must be escalated to the Risk Advisor team (contact through email) for help with acceptance, transfer, mitigation or avoidance.

Removal of equipment

If a system or service vulnerability cannot be patched or mitigated, it might be necessary to remove that system or service.

Before the removal of any system or service, a fresh Business Impact Assessment must be conducted and the business process owner consulted. The removal of a system or service is likely to come under the emergency and major change process.

Patching exemptions

In exceptional cases where patching of systems is not possible, other mitigations (such as logical separation) must be identified and evaluated for efficacy prior to enablement. The circumstances must be discussed with the affected Information Asset Owners (IAO) and System Owners. If the IAOs agree with the deviation, System Owners must request formal approval by the Senior Information Risk Owner (SIRO) for the exemption. Approval must be sought and obtained within a comparable timescale to applying a patch. If a critical patch cannot be applied, the approval to be exempt must be obtained within the same number of days allowed for applying a critical patch.

Contact details

Contact the Security Team for advice on risk, scanning and patching, to report a vulnerability alert, or to add a URL to the Web Check system: .

Communications security

Network security management

Code of connection standard

This standard is designed to help protect IT systems by providing a standard for the connection of a 3rd party IT system to a MoJ IT system.

Related information

Technical Controls Policy on page 30

Overview

Introduction

A Code of Connection (CoCo) is designed to provide a mechanism to record a formal agreement between a 3rd party organisation and the on the security measures to be applied by that 3rd party prior to and during any electronic connection with a IT system, for example, to facilitate the exchange of data between two case management systems.

HMG Security Policy Framework (SPF) mandatory requirements state that:

> Departments and Agencies must put in place an appropriate range of technical controls for all IT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

In order to meet these requirements, the SPF stipulates that IT systems must:

Comply with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which they are signatories (e.g. Government Secure Intranet).

Policy statements on connecting 3rd party IT systems and the requirements for a CoCo are covered in IT Security – Technical Controls Policy, while this document sets out the standard for its implementation.

Scope

This guide applies to all IT systems including IT systems hosted by third party suppliers on behalf of the where there is a valid business requirement to connect to a 3rd party system.

Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. Maintaining secure connections is captured as a basic requirement in Level 1 of this model, which the will need to demonstrate compliance with in their IAMM return to the Cabinet Office.

Code of Connection
Context

A Code of Connection (CoCo) is designed to provide evidence to the that a connecting 3rd party understands the security controls and procedures required to connect to a IT system and that those controls and procedures have been implemented. The aim here is to ensure that the risks associated with connecting IT systems together are sufficiently mitigated in the technical solution and managed on an ongoing basis during live operation.

Note: This standard is based on connecting a RESTRICTED-IL3 IT system with an Accredited 3rd party RESTRICTED-IL3 IT system where all electronic communication is over an Accredited RESTRICTED-IL3 network/s and/or RESTRICTED-IL3 communications channel. Where this is not the case, advice must be sort from the IT Security Officer (ITSO) and system Accreditor.

A generic CoCo (based on the previous note) is provided in Appendix A; it is split into two sections:

- basic requirement (refer to section A.1) – The section outlines the base set of CoCo requirement which need to be met by the connecting 3rd party
- supporting compliance statement (refer to section A.2) – This section contains a series of compliance statements based on ISO 27001 and the IAS 1&2 Baseline Controls Set (BCS). It is designed to provide a mechanism for a connecting 3rd party to supply compliance evidence to the system Accreditor. Section 3.2 provides details on how this compliance statement should be applied.

Note: A signed CoCo between the and the connecting 3rd party is required before the connection can go into live operation.

Managing the risk of connectivity

In order to ensure that the connectivity and sharing of electronic data between a IT system and a 3rd party IT system does not cause undue risk from one participating organisation to another, each organisation must reasonably comply with the code of connection to ensure any risks are managed effectively.

The need for a CoCo and its application will be determined by the system Accreditor who will consider the risks involved, this may require the production of a technical risk assessment and/or RMADS for the connection (further details on RMADS can be found in the Accreditation Framework).

The CoCo condition and compliance statement contained within the generic CoCo document (refer to A.1.3) provide a good platform to judge whether the assurance level of the connecting 3rd party IT system is sufficient rather than just relying on its accreditation status. A risk based approach must be taken to the application of security controls associated with the connection. The generic CoCo (refer to Appendix A) provides a baseline by which a 3rd party IT system's connection to a IT system will be assessed. The system Accreditor will provide a steer as to how this should be applied, where the default steer is that the guidance provided in IAS 1&2 Baseline Controls Set (BCS) at the DETER level should be applied.

It is highly likely that the connection between the two systems will be over the GSi. If so, the 3rd party organisation is likely to have completed the GSi Code of Connection for that system connection. The information requested in the generic CoCo is similar to that required for the GSi CoCo and as such should be readily available.

Note: Depending on the protocols being used, the GSi authority may need to be contacted.

Completing a Code of Connection

The IT System Manager and/or ITSO for the connecting 3rd party organisation must review CoCo and submit the supporting compliance statement to the system Accreditor along with any supporting documentation.

In completing the CoCo statement, the connecting 3rd party organisation confirms that they have implemented all the controls required, it should be noted that the adoption of these controls will not totally mitigate all the risks involved whether to the 3rd party's own IT system or to the connecting IT system.

Where the connecting 3rd party IT system does not comply with the controls outlined in the CoCo, the IT System Manager and/or ITSO must provide supporting comments including a high-level plan that outlines the expected timeline to meet them.

An approval from the system Accreditor is required prior to the connection going into live operation.

Appendix A - Generic Code of Connection

NOTE: *This appendix contains a generic Code of Connection, it is based on connecting a RESTRICTED-IL3 IT system with an Accredited 3rd party RESTRICTED-IL3 IT system where all electronic communication is over an Accredited RESTRICTED-IL3 network/s and/or RESTRICTED-IL3 communication channel. Where this is not the case, advice must be sort from the IT Security Officer (ITSO) and system Accreditor.*

It may need to be customised based on the relevant risk assessment and business context.

A.1 Code of Connection – Basic requirement

A.1.1 Applicable policies

This Code of Connection (CoCo) covers the connection of the "NAME OF IT SYSTEM" to "NAME of 3rd PARTY IT SYSTEM".

The services to be provided by this connection are defined in section A.1.2.1.

The IT Security Policy and the IT Security Policy for the "ORGANISATION NAME FOR 3rd PARTY IT SYSTEM" are the primary policies which apply to this CoCo.

Any 3rd party IT system connecting to a IT system must have a current and relevant IT Security Policy which is accepted by the ITSO and system Accreditor. If any aspects of the data to be exchanged require special handling measures or are particularly sensitive, the system Accreditor must be informed an approach to handling that data must be agreed by both connecting parties in advance.

A.1.2 Connectivity

A.1.2.1 Data flows, service and protocols

This section must contain details on all the data flows and service facilitated by this connection (including the protocols used); where appropriate this information can be contained within a referenced document with a summary contained in the CoCo. It must also contain details on all onward connections from the 3rd party IT System.

A.1.2.2 Connection

The "NAME of 3rd PARTY IT SYSTEM" must provide a gateway at the edge of their system to facilitate the connection to the "NAME OF IT SYSTEM" which is Accredited to RESTRICTED-IL3 and exhibits the following properties:

- Only permit the data traffic flows and protocols identified in A.1.2.1;
- This gateway must be managed by authorised service personnel with SC security clearance as a minimum;
- The gateway must maintain its own audit logs which are included as part of the "ORGANISATION NAME FOR 3rd PARTY IT SYSTEM" protective monitoring system;
- Have front-end firewall(s) to be a minimum of EAL4 certified or CAPS approved;
- Provide a minimum of EAL4 separation on front-end firewall(s) between the port used for connection to the NAME OF IT SYSTEM] and ports used for other connections.

A.1.3 Conditions

Condition	Description
CoCo-1	The minimum standards applicable to the "NAME of 3rd PARTY IT SYSTEM" shall be the equivalent to application of the IAS 1&2 Baseline Controls Set (BCS) at the DETER level and ISO27001. The supporting compliance statement (refer to A.2) has been derived from IAS 1&2 Baseline Controls Set (BCS) and ISO27001 and provides a check list that "ORGANISATION NAME FOR 3rd PARTY IT SYSTEM" should use to document their compliance to this CoCo. The completed compliance statement will allow the to determine whether the "NAME of 3rd PARTY IT SYSTEM"'s level of compliance is sufficient to meet the requirements outlined in this CoCo.
CoCo-2	The system Accreditor must be advised of any proposed changes (including configuration changes) to be made to the "NAME of 3rd PARTY IT SYSTEM" which will have an effect on its connection to the "NAME OF IT SYSTEM".
CoCo-3	All existing and planned onward connections to or from the "NAME of 3rd PARTY IT SYSTEM" must be brought to the attention of the system Accreditor prior to any live connection to the "NAME of 3rd PARTY IT SYSTEM" as this may represent a risk to the "NAME OF IT SYSTEM" and its onward connections. All such connections must be identified in this document (refer to A.1.2.1). The information provided will be kept confidential and only used for the purpose of assuring the security of this connection.
CoCo-4	No data Protectively Marked higher than RESTRICTED should be exchanged over this connection.
CoCo-5	All points of connection to the "NAME OF IT SYSTEM" shall be within a secure IL3 environment.
CoCo-6	All users (including administrative users) who connect to the "NAME of 3rd PARTY IT SYSTEM" have been subject to a formal user registration process (section A.11.2.1 in the compliance statement, refer to A.2) and all have individual unique user accounts.
CoCo-7	All security incidents concerning the "NAME of 3rd PARTY IT SYSTEM" which have (or may have in the future) involve the connection between the "NAME of 3rd PARTY IT SYSTEM" and "NAME OF IT SYSTEM" must be reported to ITSO and system Accreditor.
CoCo-8	Data may only be exchanged over this connection using the permitted types of business connection defined in relevant Interchange Sharing Agreement and/or Risk Management & Accreditation Document Set (RMADS) and is limited to the protocols defined in this document (refer to A.1.2.1).

Condition	Description
CoCo-9	The "NAME of 3rd PARTY IT SYSTEM" is protected by either a hardware Firewall or software Firewall which is either EAL 4 certified or CAPS approved.
CoCo-10	The "NAME of 3rd PARTY IT SYSTEM" has an anti-virus application installed and it is subject to regular anti-virus signature updates, with the maximum period between updates being 4 hours.
CoCo-11	The "NAME of 3rd PARTY IT SYSTEM" is subject to an operating system and hosted application security patch regime.
CoCo-12	The "NAME of 3rd PARTY IT SYSTEM" is administered by dedicated and trained IT staff to a recognised standard such as ISO2000 (ITIL) and/or recognised professional IT qualifications such as MCSE.
CoCo-13	The "NAME of 3rd PARTY IT SYSTEM" must be hosted, operated and supported from within the UK.

A.1.4 Assumptions

The connecting 3rd party IT system may make the following assumptions about the security provided by the "NAME OF IT SYSTEM":

- The "NAME OF IT SYSTEM" is Accredited by the to process data up to and including RESTRICTED-IL3 for Confidentiality, Integrity and Availability;
- The security regime within the "NAME OF IT SYSTEM" ensures the confidentiality and integrity of data originating from the "NAME of 3rd PARTY IT SYSTEM" once it enters the boundary of the "NAME OF IT SYSTEM".

A.1.5 Administration

This document must be reviewed annually or following a major change to the "NAME of 3rd PARTY IT SYSTEM" or the "NAME OF IT SYSTEM" to ensure no additional security measures are required.

Note: A major change is defined as:

- Software – A significant change in the functionality of any software used to support the connection;
- Hardware - A significant change to the physical hardware supporting the connection;
- Design/Architecture - A change in the connectivity of the "NAME of 3rd PARTY IT SYSTEM" to the "NAME OF IT SYSTEM" or any other IT system it connects to, the security controls protecting those connections or the re-configuration of any services used to support the connection.

A.1.6 Authorisation for connection

On the basis of the information made available to them, and to the best of their knowledge, the undersigned confirms that the connecting "NAME of 3rd PARTY IT SYSTEM" complies with the requirements outlined in this CoCo and that the information provided in the supporting compliance statement is accurate.

Note: Any major change (as defined in A.1.5) to the connecting "NAME of 3rd PARTY IT SYSTEM" may invalidate this CoCo and a new submission may be required.

NAME	Signature
JOB TITLE	
NAME OF 3rd PARTY CONNECTING ORGANISATION	Date

NAME OF INFORMATION ASSET OWNER	Signature
Information Asset Owner	
	Date
NAME OF SYSTEM ACCREDITOR	Signature
System Accreditor	Date

A.2 Supporting compliance statement

This compliance statement provides a check list which will enable the to assess the "NAME of 3rd PARTY IT SYSTEM" compliance against this CoCo and the pertinent security controls from HMG IAS 1&2 Baseline Controls Set (BCS) at the DETER level and ISO27001. The system Accreditor will determine whether or not the "NAME of 3rd PARTY IT SYSTEM" presents an unacceptable risk to the "NAME OF IT SYSTEM".

Guidance on completion:

- Under the 'Control' column are a number of security controls which should be read and responded to in subsequent columns;
- Under the 'Compliance' column, answer **Yes**, if the control is fully met, **No**, if it is not fully met, **Partial**, if part of the control has been implemented or **N/A** if the control does not apply;
- Under the 'Process Owner/References' column, the name of an individual or group who is responsible for managing that control must be entered and any associated documents referenced;
- Under the 'Solution/Comments' column, enter a brief statement outlining how that control is met, why it is not met, only partially met or why it does not apply.

Note: The notes (in blue and italics) under the “Solution/Comments” column are for guidance only. These notes must be removed upon completion.

Ref.	**Control**	**Compliance (Applicability) Y/N/ P/N/A**	**Process Owner/ Reference**	**Solution/Comments**
A.5	**Security Policy**			
A.5.1	**Information Security Policy (ISMS Policy)**			
A.5.1.1	**Information Security Policy document** - Does the "ORGANISATION NAME FOR 3rd PARTY" have an Information Security policy document, approved by management, and published and communicated to all employees and relevant external parties?			*State clearly what the document title is. Describe how/when this document is communicated to all staff and contractors. Provide a copy of the policy with this statement if possible.*
A.6	**Security Organisation**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.6.1	**Information Security Infrastructure**			
A.6.1.1	**Management commitment to Information Security** - Does "ORGANISATION NAME FOR 3rd PARTY" management actively support security within the organisation through the establishment of a forum where security issues are discussed and security responsibilities are acknowledged?			*Is information security a standing agenda item at a regular management meeting and/or has a separate working group been set-up to discuss and address security concerns? Who attends this meeting and what is the frequency. Provide terms of reference for the meeting/group where possible.*
A.6.1.3	**Allocation of Information Security Responsibilities** - Are "ORGANISATION NAME FOR 3rd PARTY" information security responsibilities allocated and documented?			*Have information security responsibilities been documented and communicated to all staff? If so, how?*
A.6.1.5	**Confidentiality Agreements** - Does the "ORGANISATION NAME FOR 3rd PARTY" have any confidentiality or non-disclosure agreements in place for staff, contracted bodies and other 3rd parties?			*Do confidentiality agreements state your requirements for security? Provide a copy of your agreement with this statement if possible.*

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.6.1.8	**Independent Review of Information Security** - Is the "ORGANISATION NAME FOR 3rd PARTY" subject to external audit? Do any of these audits look at security issues?			*The approach to managing information security and how it is implemented should be reviewed regularly, i.e. processes, procedures, policies, etc. When was the last one conducted, by whom and how regularly is it normally reviewed. If the system is included in the scope of a certified Information Security Management System, details should be provided.*
A.6.2	**External Parties**			
A.6.2.1	**Identification of Risks relating to External Parties** - Has the "ORGANISATION NAME FOR 3rd PARTY" conducted any form of risk assessment related to their IT systems and the data held on them? Has the outcome of the risk assessment (e.g. risk treatment plan) been implemented?			*How do you assess risk to your organisation caused by the provision of access to a 3rd party? Does it also take into account physical & logical access controls, etc*

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.6.2.2	**Addressing Security when dealing with Customers** - Has the "ORGANISATION NAME FOR 3rd PARTY" identified security requirements which need to be adhered by other entities or organisations connecting into "NAME of 3rd PARTY IT SYSTEM" before they are given access?			*Need to provide detail of any security requirements?*
A.6.2.3	**Addressing security in 3rd Party Agreements** - Does the "ORGANISATION NAME FOR 3rd PARTY" include security requirements in contracts with third parties that involve accessing, processing, communicating or managing the organisation's information or information processing facilities?			*Do the 3rd party agreements include terms that assist meet the identified security requirements? Examples of these terms or a copy of the 3rd party agreement should be provided.*
A.7	**Asset Classification and Control**			
A.7.1	**Responsibility for Assets**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.7.1.3	**Acceptable use of Assets** - Does the "ORGANISATION NAME FOR 3rd PARTY" have any documented policies on the acceptable use of information and assets associated with information processing, i.e. personal use, use of email, Internet access etc?			*Are there rules for the use of assets within the organisation, e.g. Acceptable use policies or “Do and Don't” lists for Email & Internet, mobile devices, etc. If so, details should be provided.
A.7.2	**Information Classification**			
A.7.2.1	**Classification Guidelines** - Does the "ORGANISATION NAME FOR 3rd PARTY" use a data classification scheme (e.g. the Government Protective Marking Scheme) with defined protective controls for each classification or sensitive personal data?			*State the classification scheme applied and associated controls to protect personal data (if applicable). Has this been documented and communicated to all staff? Provide a copy of the guidance provided if possible.*
A.8	**Human Resources Security**			
A.8.1	**Prior to Employment**			
A.8.1.1	**Roles and Responsibilities** - Does the "ORGANISATION NAME FOR 3rd PARTY" identify security roles and responsibilities of employees, contractors and 3rd party users? Are such roles/responsibilities documented?			*Are there defined, documented and communicated security roles and responsibilities? State what these are at a high-level and provide documentation where possible to support this. E.g. role/function terms of reference.*
A.8.2	**During Employment**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.8.2.1	**Management Responsibilities** - Does "ORGANISATION NAME FOR 3rd PARTY" management ensure security requirements are enforced by employees, contractors and 3rd party users? How is this achieved?			*How do management ensure that staff and contractors are aware and comply with their responsibilities for security?*
A.8.2.2	**Information Security Awareness, Education and Training** - Do "ORGANISATION NAME FOR 3rd PARTY" employees and, where relevant, contractors and 3rd party users receive appropriate security awareness training and regular updates in "ORGANISATION NAME FOR 3rd PARTY" security policies and procedures, as relevant for their job function?			*Do all employees and contractors undergo security awareness training? How frequently is this awareness training conducted? What does the security awareness training cover at a high-level. How do you assess employees' understanding of that training?*
A.8.3	**Termination or Change of Employment**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.8.3.3	**Removal of Access Rights** - Does the "ORGANISATION NAME FOR 3rd PARTY" remove access rights of all employees, contractors and 3rd party users to information and information processing facilities upon termination of their employment, contract or agreement? How is this done?			*Details should be provided on the process for removing access rights on termination of employment.*
A.9	**Physical and Environmental Security**			
A.9.1	**Secure Areas**			
A.9.1.1	**Physical Security Perimeters** - Does the "ORGANISATION NAME FOR 3rd PARTY" have a defined, effective, security perimeter to protect areas that contain information-processing facilities?			*Describe the physical security barriers, e.g. walls, alarm systems, doors/gates, fencing, etc, where applicable.*
A.9.1.2	**Physical Entry Controls** - Are there secure areas within the "ORGANISATION NAME FOR 3rd PARTY" premises, protected by appropriate entry controls to ensure that only authorised personnel are allowed access?			*Describe any designated secure areas in the building. Where will the servers/workstations/ gateway used to support this connection be located? What security controls are in place to limit access to those with a need-to-know?*

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.9.1.6	**Public Access Delivery & Loading Areas** - Are access points such as delivery and loading areas and other points where unauthorised persons may enter the "ORGANISATION NAME FOR 3rd PARTY" premises controlled and, if possible, isolated from information processing facilities to avoid unauthorised access?			*Describe the controls limiting access from public access, delivery and loading areas to the areas housing the IT services used to support this connection.*
A.9.2	**Equipment Security**			
A.10	**Communications and Operations Management**			
A.10.1	**Operational Procedures and Responsibilities**			
A.10.1.1	**Document Operating Procedures** - Does the "ORGANISATION NAME FOR 3rd PARTY" have operating procedures for the system connecting to "NAME OF IT SYSTEM"?			*Are operating procedures documented? A copy of the document or Table of Contents will suffice.*
A.10.1.2	**Change Management** - Does the "ORGANISATION NAME FOR 3rd PARTY" have a Change Management process which covers the system connecting to the "NAME OF IT SYSTEM"?			*Describe the change management process.

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.10.2	**3rd Party Service Delivery Management**			
A.10.2.1	**Service Delivery** - If the "ORGANISATION NAME FOR 3rd PARTY" use a 3rd party service provider for its IT Service , does the "ORGANISATION NAME FOR 3rd PARTY" ensure that the security controls, service definitions and delivery levels included in the 3rd party service delivery agreement are implemented, operated and maintained by that 3rd party?			*Do you use a 3rd party supplier to support IT used in this connection? Are security requirements stated within the agreement? How do you check the effectiveness of the security controls stated in the 3rd party agreement?*
A.10.3	**System Planning & Acceptance**			
A.10.4	**Protection against Malicious and Mobile Code**			
A.10.4.1	**Controls against Malicious Code** - Has the "NAME of 3rd PARTY IT SYSTEM" implemented controls to detect and protect against malicious code and that appropriate user awareness procedures is provided? What AV application is installed and how often is the AV library updated?			*What measures are in place to control against malicious software/code? Describe the process for detection and removal of malware if detected.*
A.10.5	**Backup**			
A.10.6	**Network Management**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.10.6.1	**Network Controls** - Is the system connected to the "NAME of 3rd PARTY IT SYSTEM" segregated from other "ORGANISATION NAME FOR 3rd PARTY" systems? Note: It is understood that this may not be possible in all cases.			*How is the connecting system protected against network intrusions? Describe any segregation of other networks and provide a high-level logical network diagram if possible.*
A.10.7	**Media Handling and Security**			
A.10.7.3	**Information Handling Procedures** - What procedures are in place for the handling and storage of information in order to protect such information from unauthorised disclosure or misuse?			*Describe your information handling procedures. How does this map to A.7.2.1 (Information Classification).
A.10.7.4	**Security of System Documentation** - What security procedures are in place to secure the system documentation concerning this connection so it is protected from unauthorised access?			*How is the system documentation prevented from unauthorised access?*
A.10.8	**Exchange of Information**			
A.10.8.5	**Business Information Systems** - Are there any policies and procedures to protect information shared over this connection?			*Please provide any policies or an Information Sharing Agreement.*
A.10.9	**Electronic Commerce Services**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.10.10	**Monitoring**			
A.11	**Access Control**			
A.11.1	**Business requirement for Access Control**			
A.11.2	**User Access Management**			
A.11.2.1	**User Registration** - Does the "NAME of 3rd PARTY IT SYSTEM" have a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services?			*Describe the registration and deregistration process. Are the user registration procedures documented?*
A.11.2.2	**Privilege Management** - Does the "NAME of 3rd PARTY IT SYSTEM" restrict the allocation and use of privileges?			*Who has (or will be given) privileged access to the IT System – roles will suffice? How will this access be restricted to just those named roles?*
A.11.2.3	**User Password Management** - What process is in place to allocate passwords to users? Is a password policy enforced and what technical controls are in place to support that enforcement?			*Describe the process for allocating new passwords, the password policy and any control used to enforce it?*
A.11.2.4	**Review of User Access Rights** - Is there a review process that covers users' access rights on the "NAME of 3rd PARTY IT SYSTEM"?			*Describe the process for regularly reviewing access rights*
A.11.3	**User responsibilities**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.11.3.1	**Password Use** - Do users follow good security practices in the selection and use of passwords?			*State the password policy. What controls are in place to prevent users from selecting weak passwords?
A.11.3.2	**Unattended User Equipment** - Is there a user timeout set on the "NAME of 3rd PARTY IT SYSTEM"?			*What is the timeout process?*
A.11.4	**Network Access Control**			
A.11.4.1	**Policy on use of Network Services** - How does "NAME of 3rd PARTY IT SYSTEM" ensure that users only have direct access to the services that they have been specifically authorised to use?			*Describe how users are limited to those services that they are only authorised to use. Is there a policy covering access to network services?*
A.11.4.2	**User Authentication for External Connections** - Does "NAME of 3rd PARTY IT SYSTEM" ensure any remote access is subject to authentication of the same standard as for normal users? Refer to Control A.11.2.3.			*What security safeguards are in place to control access by remote users?*
A.11.5	**Operating System Access Control**			
A.11.5.1	**Secure Log-on Procedures** - Is access to the "NAME of 3rd PARTY IT SYSTEM" only attainable via a secure log-on process?			*Provide an overview of the secure log-on process.*

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.11.5.2	**User Identification and Authentication** - Do all users of the "NAME of 3rd PARTY IT SYSTEM" have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual?			*State clearly whether users have a unique User ID associated with their use of the IT system and additionally that this unique identifier can be used uniquely/ unequivocally to identify the activities of that user.*
A.11.5.4	**Use of System Utilities** - A confirmation is required that the use of system utility programs on the "NAME of 3rd PARTY IT SYSTEM" is restricted and tightly controlled?			*What procedures do you have in place to restrict access to system utility programs?*
A.11.6	**Application Access Control**			
A.11.7	**Mobile computing and Teleworking**			
A12	**Information Systems Acquisition, Development and Maintenance**			
A12.1	**Security Requirements of Information Systems**			
A.12.2	**Correct Processing in Applications**			
A.12.3	**Cryptographic controls**			
A.12.3.1	**Policy on the Use of Cryptographic Controls**			*Check with the system Accreditor on whether any cryptographic controls are required in this connection.*

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.12.4	**Security of System Files**			
A.12.4.1	**Control of Operational Software** - Is there a process to control the implementation of software on the "NAME of 3rd PARTY IT SYSTEM"?			*Provide details on the controls put in place on the implementation of operational software.*
12.5	**Security in development and support processes**			
A.12.5.1	**Change Control Procedures** - All changes to the "NAME of 3rd PARTY IT SYSTEM" should be examined and any major changes reported to system Accreditor.			*Is there a documented Change Control procedure? Details should be provided.*
A.12.5.4	**Information Leakage** - Are there controls in place to reduce the likelihood of information leakage (compromise of)?			*What controls are in place to detect, deter or prevent information leakage?*
A.12.6	**Technical Vulnerability Management**			
A.13	**Information Security Incident Management**			
A.13.1	**Reporting Information Security Events and Weaknesses**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.13.1.1	**Reporting Information Security Events** - Is there a documented process to ensure information security events affecting the "NAME of 3rd PARTY IT SYSTEM" are reported to ITSO and system Accreditor as soon as possible?			*Describe the Incident Management process applicable to the connecting system or supply documentation to support this. It must include reporting of security incidents to the .*
A.13.2	**Management of Information Security Incidents & Improvements**			
A.13.2.1	**Responsibilities & Procedures** - Have assigned responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents been implemented? This needs to include the requirement to report incidents associated with the "NAME of 3rd PARTY IT SYSTEM" to .			*All IT Security incidents should be reported to Operational Security Team.*
A.14	**Business Continuity Management**			
A.14.1	**Aspects of business continuity management**			
A.15	**Compliance**			
A.15.1	**Compliance with legal requirements**			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
A.15.1.4	**Data Protection and Privacy of Personal Information** - Does the "ORGANISATION NAME FOR 3rd PARTY" have documented procedures covering data protection and privacy of personal information?			*Reference relevant documentation that details the procedures for adhering to privacy and protection of personal information. Provide documentation to support this if available.*
A.15.2	**Reviews of Security Policy and Technical compliance**			
A.15.2.1	**Compliance with Security Policies & Standards** - Does the "ORGANISATION NAME FOR 3rd PARTY" conduct compliance audits to achieve compliance with security policies and standards, including the CoCo for this connection?			*What is the process to conduct a compliance audit against the processes and procedures employed to support this connection? When was the last one conducted? Were any gaps identified, if so is there a remediation plan in place?*
A.15.2.2	**Technical Compliance Checking**			*Is the connecting system subject to a technical assessment (penetration test / ITHC? When was the last one done? Were any vulnerabilities identified and if so have these been addressed/fixed?*
A.15.3	**System Audit Consideration**			

Defensive domain registrations

The and associated organisations (Executive agencies, non-departmental public bodies and so on) maintain varying levels of 'online presence' using domain registrations. This are a fundamental part of the organisation's identity on the public internet. An example is the `justice.gov.uk` email domain used for contacting other government organisations, partners and members of the public.

Each organisation **must** identify a core set of internet domains it considers critical to its internet identity. Each organisation must then defensively register a small number of obvious variations (for example, `justice.gov.uk` may justify `justicegov.uk`, `justice.co.uk` and `justice.uk` where already not used for legitimate purposes).

These registrations will help protect the organisation, as well as its partners and members of the public, from illegitimate parties pretending to be the organisation when they are not. Failing to register these domains can cause problems, such as phishing emails using what seem to be plausible domains.

Limiting the permutations to register

Domain permutations for defensive registration should be limited to the organisation's core identity, as opposed to tertiary campaigns/identities, in order to keep costs and management overheads down.

Some domain registrars have methods to detect malicious registrations of overtly government-associated domains through the use of misspellings and so on. Unless there are strong justifications as to why misspellings must be covered, organisations should only defensively register `.uk` and `.co.uk` top-level domain variants and visual manipulations. For example, the removal of one dot from justice.gov.uk leads to justicegov.uk which could be a registerable domain and one that looks a lot like justice.gov.uk during a casual inspection.

Mandatory features for defensively registered domains

The following features are required when registering a defensive domain:

Functional nameservers

The defensively registered domain must have a functional nameserver configuration.

Sender Policy Framework (SPF)

There must be an SPF record which uses *strict* configurations to indicate whether the domain is expected by the owner to send emails, or not.

Example 'no permitted sender' record:

```
v=spf1 -all
```

Additional SPF implementation guidance is available on GOV.UK.

Domain-based Message Authentication, Reporting and Conformance (DMARC)

There must be a DMARC record configured in line with published DMARC guidance on GOV.UK.

Example 'reject' policy record:

```
v=DMARC1;p=reject;rua=mailto:<example dmarc email address>;
```

Mail Exchanger (MX)

There must be a nullified MX record in order to ensure any attempt to send emails to the defensive domain to instantly failed.

Example nullified record:

MX priority `0` with host name `.`

DomainKeys Identified Mail (DKIM)

There must be a nullified DKIM record in explicitly highlight that any outbound email attempts are likely invalid.

Example nullified record:

```
v=DKIM1; p=
```

DNS Certification Authority Authorization (CAA)

There must be a DNS CAA record(s) to indicate restrictions so that certificate authorities that certificates should not be issued for these domains.

Example nullified record:

```
issue ";"
```

Example iodef notification record:

```
iodef "mailto:certificates@digital.justice.gov.uk"
```

Automated renewals

Defensively registered domains should be configured to automatically renew by default.

Web services/redirects

Web services/redirects must **not** be functional or available for defensively registered domains.

The `www.` should *not* be created. The apex `@` record, if required and created, should not respond to TCP/80 (HTTP) or TCP/443 (HTTPS).

Mail services/redirects

Mail services/redirects must **not** be functional or available for defensively registered domains.

Registering and maintaining a defensive domain

organisations should contact domains@digital.justice.gov.uk for assistance with defensive domain registrations and operations.

Decommissioning a domain

When a service is no longer provided or required, any domain name used to access that service is no longer required. This means that the domain can be decommissioned. Technically, decommissioning a domain is easy: simply cancel the registration.

But it's important to check whether the domain is still required, even when the service is no longer provided.

How long should a domain be kept?

The answer depends on how the original domain was used in practice.

For example, if the domain was only used internally within the , and all references to it have already been updated to point to the new or replacement service, then the old domain name probably does not need to be kept for more than 12 months.

However, there are circumstances where it is important to keep a domain for longer periods of time. For example:

- The domain was heavily used internally, and there might be old emails or documents referring to it.
- The domain was used externally.
- The domain would be attractive for 'domain squatting'.

In general, unless there is a good case for saying that a domain name does not need to be kept for defensive purposes:

- A domain associated with a decommissioned service **must** be maintained for *at least* five years after the corresponding service is decommissioned.
- The domain registration **must** be reviewed again *not less than* 12 months before it is due to expire, to determine if the registration should still be maintained.

Domain names and Domain Name System (DNS) security policy

Introduction

This policy gives an overview of domain name registration and monitoring principles and responsibilities within the and summarises the 's related compliance policies and guides.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.DOM.xxx**, where **xxx** is a unique ID number.

Who is it for?

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, Service Owners and the EPICK Team.
Service providers	Defined as any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for or on behalf of the .
General users	All other staff working for the .

'All users' refers to General users, Technical users and Service Providers as defined previously.

Policy sections

This policy aligns to industry standards and frameworks and is divided into two categories (and subsections describing the controls) addressing:

- Principles.
- Policy statements.

Note: If any of the controls within this policy cannot be applied, they are considered an exception to be assessed for inclusion within a risk register.

Principles

Effective domain name registration encompasses the following five principles, which include:

- **POL.DOM.001:** The secure domain name management aligning this to its Cyber security guidance, specifically multi-factor authentication (MFA), least privilege and review of user access rights.
- **POL.DOM.002:** The manage domain name portfolio growth, that is, their inherent value, before assessing their expiration.
- **POL.DOM.003:** The ensure non-core or defensively registered domains point to relevant content.
- **POL.DOM.004:** The ensure all "Technical users" and "Service Providers" are reminded of the processes for requesting new registrations, auto-renewal, and decommissioning domains.
- **POL.DOM.005:** The apply domain name specific technologies such as (list not exhaustive):
  - Domain Name System Security Extensions (DNSSEC), which protects against cache poisoning.
  - Domain-based Message Authentication, Reporting and Conformance (DMARC), which protects against email spoofing.

Domain name registration statements

This policy's statement elements are outlined as follows:

Standards, guidance and technology

- **POL.DOM.006:** To improve clarity and security hardening, all domain name registrations and usage adhere to the 's domain naming standards and system hardening standards.
- **POL.DOM.007:** This policy's related security guidance clearly describe why defensive domain registration is essential and why not doing it creates cyber risk.
- **POL.DOM.008:** This policy's related guidance on How to get, register or manage a domain name clearly describes defensive domain names solutions.

Domain Operations: Operations Engineering team

- **POL.DOM.009:** The team manage the registration of all domain names, including defensive domain names.
- **POL.DOM.010:** Departmental teams and ALBs be directed to the team to carry out domain registration on the user or department's behalf.

- **POL.DOM.011:** All departments and ALBs ensure that they transfer ownership of non-GOV.UK domains to the team, with a list of transfers and registration managed by the team.

Domain monitoring

- **POL.DOM.012:** The Threat Vulnerability Management team (TVM) be responsible for identifying, detecting, reporting, and helping prioritise domain monitoring issues, including squatting or hijacking.
- **POL.DOM.013:** The TVM team also be responsible for detecting and reporting on external domain name hijackings.
- **POL.DOM.014:** The team and TVM team be responsible for resolving domain issues raised by the TVM team, domain owners and teams, by implementing any required changes.
- **POL.DOM.015:** The follow when a domain is hijacked or used maliciously.
- **POL.DOM.016:** departments, ALBs and third parties report domain variants and domains used within the but which are not owned by the . Refer to the contact details.

Note: Contact the TVM team through the .

Note: Security contacts in the event of an incident are located on the Intranet.

Decommissioning domains

- **POL.DOM.017:** Any decommissioned domain be transferred to the team. Contact them at on behalf of departmental teams or ALBs, and providing appropriate HTTP redirections to a suitable URL, for example, `301` or `302`.
- **POL.DOM.018:** Domains registered pre-policy be moved to the team.
- **POL.DOM.019:** The allow decommissioned domains to expire if there is no risk to the via "Domain Squatting" or "Phishing" attacks, or value in registering them defensively.
- **POL.DOM.020:** Any decommissioned domains be added and managed in a risk register.

Enforcement

- **POL.DOM.021:** domains discovered that do not abide by the statements set out in this policy be treated as suspicious, reported to NCSC, and blocked automatically.
- This policy is enforced by lower-level policies, standards, procedures and guidance.
- Non-conformance with this policy could result in disciplinary action taken as per the department's disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the department always cooperates with the relevant authorities and provides appropriate evidence.

Contact details

organisations should contact for assistance with domain registrations, defensive domain registrations, transfers and operations.

Internet -v- PSN

The internet is 'ok'

The prefers the use of public commodity networks (such as the Internet) over the use of dedicated or private network links.

Networks are bearers

The consider networks, whether private or public, to be bearers for information transfer, in and of themselves they should not be considered as the mechanism to identify and confer trust or privilege.

IP addresses, DNS information & architecture documentation

OFFICIAL-SENSITIVE? Not by default

The does **not** consider its IP address, DNS or architectural information to be (a handling caveat within the information classification) *by default*.

In some contexts, this information may be considered sensitive (usually when combined with other information), for example, "Server X on IP address x.x.x.x has not been security patched for 5 years and there are known vulnerabilities which are unmitigated and thus could actively be exploited in this moment."

IP addresses of connecting clients (for example, the IP address of the computer of a general member of the public accessing a public digital service) *may* be Personal Data.

RFC1918 addresses

Private network IP addresses cannot be directly accessed from public networks so require multiple faults or compromises to be useful as part of an exploit.

Information via email

IP addresses, DNS information & architecture documentation can generally be sent via email services that enforce adequate in-transit integrity/encryption without any additional security protections such as the use of ZIP files.

Multiple consecutive (back-to-back) firewalls

At the does **not** require or prefer the use of two or more firewalls in a 'back-to-back' fashion unless they are reasonably required due to segregated role or trust management (for example, interconnecting two networks which are managed independently).

Same rules, same management, different vendor

There is a myth that the use of multiple back-to-back firewalls from different vendors (with the exact same rulesets) is better for security as vulnerabilities that exist in one firewall will not exist in the other however any value of this perceived security benefit (which is likely limited in meaningful benefit anyway) is dwarfed by additional cost, complexity, and maintenance overheads.

Two networks, two managers

When interconnecting two networks that have different purposes or trust requirements (and when they are potentially managed by different parties) back-to-back firewalls can be used to enforce segregation and ensure managed integration and change control.

Networks are just bearers

The base principle

IP networks **must** be considered commodity bearers for technical connectivity to facilitate the movement of data.

Network characteristics (such as hardware port, VLAN tag or IP address) should not be solely relied upon as part of authorisation to confer trust or privilege.

h/t https://medium.com/@joelgsamuel/ip-address-access-control-lists-are-not-as-great-as-you-think-they-are-4176b7d68f20

Information transfer

Bluetooth

This guidance helps you use Bluetooth enabled devices and peripheral devices.

Related information

Personal devices on page 46

Overview

Bluetooth is a very short range wifi technology. In everyday terms, Bluetooth devices can 'talk to each other' if they are very close, for example in the same room. This makes Bluetooth really good for wireless devices, for example a telephone headset, or a mouse or keyboard.

Bluetooth works by 'pairing' devices. This makes it quick and simple to use. The problem is that Bluetooth, and the pairing process, is not very secure. This means that attackers might get unauthenticated access to devices. As an example, an attacker 'listening' to the Bluetooth connection between a computer and a keyboard could possibly intercept passwords or other sensitive information as the details are typed on the keyboard.

This guidance tells you more about the view of Bluetooth, from a security perspective. It also gives you hints and tips on how to use Bluetooth more safely.

The aim is to help you maintain the Confidentiality, Integrity and Availability of data, applications and services. The results should be that:

- the information you access is not compromised
- you can connect devices using Bluetooth, safely
- you are aware of the problems around Bluetooth, and can take the necessary safety precautions

Note: Remember that there might be local rules that apply regarding the use of Bluetooth devices. A good example is in Prisons, where use of Bluetooth would not be available by default. Ensure that you check with local requirements.

Accessibility

Some types of Bluetooth devices are not allowed, by default. However, where there is a good reason for requiring a Bluetooth device, such as for Accessibility reasons, then a request for an exception to use the device will be treated sympathetically and permitted wherever possible.

Bluetooth devices and risks

Examples of Bluetooth devices, and whether they might be used for business purposes, are as follows:

Bluetooth device	Suitable for work purposes (Y/N)
Keyboards	Y
Mouse	Y
Telephone headsets	Y
Headphones	Y
Earbuds	Y
Trackpads	N - but exception possible for Accessibility reasons
External speakers	Y - but be aware of other people or devices nearby that might be listening
Gaming joysticks and controllers	N - but exception possible for Accessibility reasons
Laptops	Y - for -issued devices
Hearing aids	Y
Watches and Fitness bands	N
Smart TVs	N - requires authorisation
Storage devices (similar to USB 'thumb' drives)	N
Internet-of-things 'Smart speakers'	N

Bluetooth device	Suitable for work purposes (Y/N)
Connected vehicles	N - Connected vehicles are effectively Bluetooth-connected storage devices.

A Bluetooth device might be at risk from any of the following:

- Eavesdropping
- Unauthorised access
- Message modification
- Denial of service
- Data exfiltration
- Insecure data transmission
- Phishing

An example of a Bluetooth problem is 'Bluetooth marketing'. As you walk around with your mobile phone, it is continuously looking for Bluetooth devices and wifi access points. It does this to help with accurate location tracking. But other devices can also find your mobile phone. These devices might report tracking information about where you were at any time. This guidance will help you understand more about the problem, and suggest things you can do to reduce the risks.

Connected vehicles

Connected vehicles are effectively Bluetooth-connected storage devices. They are considered personal devices for the purposes of this guidance, regardless of whether they are owned, leased or rented.

Automatic transfer of contact information and calendar events might happen during the pairing process. The resulting transferred data is accessible to any third party who subsequently pairs their mobile device to the vehicle.

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, devices be paired with Bluetooth-enabled vehicles.

Best practices for using Bluetooth

Before using a Bluetooth device in a work context, consider the following:

- What is the business case for using the Bluetooth device?
- What data might be or will be access through, or using, the Bluetooth device?
- Does the Bluetooth device have the latest patches and fixes applied - where possible?
- Was the Bluetooth device purchased from a reputable vendor?
- Does the Bluetooth device require a PIN code or similar before connecting?
- Are the Bluetooth devices 'discoverable'?
- Have you connected to any other 'public' Bluetooth devices?
- Are all the devices password protected?
- Might someone be able to find out what Bluetooth devices you are using?
- Is the material you are working with or higher?

The best way to ensure your Bluetooth device is as up-to-date as possible is to apply all patches and fixes for all hardware devices as soon as you can.

Bluetooth is a very cheap and simple technology. This means that it is often included in extremely cheap devices; often these use old versions of technology or are not provided with patches and fixes. The best thing is to obtain any Bluetooth devices from reputable vendors, so that it is more likely the device will be supported and maintained correctly.

Many Bluetooth devices try and make connection as easy as possible by enabling 'Direct Connection'. This often means that you only need to 'find' a Bluetooth device on your 'phone or laptop, then click once for a connection to be established. While very easy, this is not safe, because those same direct connections can also happen automatically,

'behind the scenes', without you being aware. If possible, ensure that a Bluetooth connection is allowed only when a PIN or password is supplied. This reduces the risk of 'hidden' Bluetooth connections.

Some Bluetooth devices allow you to choose whether they are 'discoverable'. For example, on Android 'phones, you can go to the `Settings -> Connected devices -> Connection preferences -> Bluetooth visibility` or similar. The best advice is to change the Bluetooth settings to not discoverable if you can. Only make the device discoverable when you need to connect to a trusted device.

At regular intervals, check to find out what Bluetooth devices are 'known' to your devices. Remove any you don't recognise.

When in public places, make sure you only connect to known devices. Always ensure you are in a secure and safe location such as home, office, or a known isolated place before switching on your Bluetooth.

If someone can find what Bluetooth devices you have, or are using, they might try and use one of their device to intercept or monitor the connection. Try to keep Bluetooth devices out of sight so that no-one knows which ones you might actually be using. Even the bright blue light Bluetooth devices illuminate when they are connected might draw unwanted attention.

Generally speaking, Bluetooth devices do not present extra problems when working with material. However, the whole point of Bluetooth is to enable and simplify communications, so you need to be extra careful when using Bluetooth devices while working on or higher material.

Criminal Justice Secure Mail

The operates the CJSM service to enable those people working in the Justice system who do not have access to a suitable email service to exchange information in a safer way.

The does **not** require the use of CJSM where other suitably secure and efficient means can be used. It is considered a safe option to enable communication but it is only an option.

Government secure email policy

Email services that are materially aligned to the UK government secure email policy are suitable for the movement of data, including where the handling caveat has been applied.

Data sovereignty

The Senior Security Adviser, Chief Information Security Officer (CISO), Chief Technical Officer (CTO) and Data Protection Officer (DPO) have issued this guidance for business units and third-party partners across the supported by Digital & Technology and/or within scope of the Data Protection Officer (DPO) to explain the 's position on 'data sovereignty' (where the processing of data, including personal data, may take place).

Summary

At level, subject to adequate, proportionate and standard information security controls, the Department is content to process, and allow third-party partners to process, data (including personal data) outside the UK.

This statement includes the (marked as) handling caveat advising that additional care may be required; it is not a separate classification and any data / information is subject to the same rules as .

The does not by default or routine require 'UK only hosting' or 'UK only services' for data privacy, data protection or information security reasons.

Data sovereignty questions

- Where is the data located (i.e. servers and storage), including any off-site backup locations?

Even if located in the UK can it be viewed, modified, copied or deleted remotely from another country?

- Who is managing the service (n.b. administrators may be based anywhere in the world)?

For example, Microsoft Azure's data centre is in the UK but the system administrators can be located in Brazil, New Zealand, US and etc.

- Where are all of these entities legally instantiated and located?

For example, Amazon Web Services has UK data centres but is nevertheless is a US company with global support staff.

The 'where' data is processed is the combination of the answers to the previous questions, and is much more than just where the servers and hard drives are physically located (data hosting).

As part of routine due diligence, including fulfilling legal obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act (2018), where data is processed in other legal jurisdictions the is to ensure that adequate safeguards, including where relevant Data Protection Impact Assessments (DPIAs), are in place to ensure data is secure and that the rights and freedoms of any Data Subjects are maintained.

UK and the European Union

The departure of the UK from the European Union will not lead to a change in the 's position.

The has no plans to inshore data (i.e. limiting and / or returning data to the UK) for privacy or security reasons, nor is the asking its partners (for example, commercial suppliers) to do so.

Where to get help

In the first instance, contact the 's Data Protection Officer - .

Email

Overview

This document provides you with guidance for safe and secure use of email within the .

In general, always use email in an acceptable way.

In particular:

- Never circulate messages or material that contains obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), and disruptive, or otherwise offensive language.
- Don't use email or other messaging systems for trivial debates or exchanges with an individual or group of people.
- Don't use email or other messaging systems for anything other than appropriate business purposes.
- Don't make statements that defame, slander or lower the reputation of the , any person or organisation.
- Don't forward email chain letters to your contacts. Instead, report them to .
- Be aware of unsuitable attachments, for example video clips, images, or executable files. email automatically filters many unapproved attachment types, particularly those that can contain executable files. Emails containing those attachments are likely to be quarantined and not delivered.
- Avoid excessive use of email, and sending email to large numbers of recipients. Ask yourself if it really makes sense to "Reply All"?
- Any recipients in the "To" or "Cc" fields can retrieve the addresses of all other recipients in those fields. If you are sending an email to a list of people outside , where privacy of individuals might be relevant, place your list of recipients in the "Bcc" field and set the "To" field to your own address. This ensures that none of the recipients can retrieve the identities of the other recipients.
- Keep your operating systems up to date to prevent susceptibility to viruses.
- Scan email attachments to detect viruses and other malware.

Be aware that the monitors the use of electronic communications and web-browsing. Your manager can request reports detailing your activity if they suspect inappropriate use of email or web-browsing facilities.

Ask if you want further information.

Monitoring

The monitors all email for security purposes.

Specifically, communications may be monitored without notice and on a continual basis for a number of reasons including compliance with legal obligations, effective maintenance of IT systems, preventing or detecting

unauthorised use or criminal activities (including cyber-intrusion), monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

In general, the monitors telephone usage, network, email and Internet traffic data (including sender, receiver, subject, attachments to an email, numbers called, duration of calls, domain names of websites visited, duration of visits, and files uploaded or downloaded from the Internet) at a network level.

Email threats

Although email is a powerful business tool, it has problems. In this guidance, we describe some of the problems, and how you can avoid them.

Email threats often use familiar email addresses to disguise attacks, or to pose as valid emails. Email threats are becoming more frequent and pose one of the biggest problems for systems and services.

There are many possible threats, including:

- Viruses: These can be spread between computers in emails or their attachments. They can make PCs, software or documents unusable.
- Spam: This is unsolicited mail sent in bulk. Clicking on links in spam email may send users to phishing websites or sites hosting malware. Often email spam mimics the addresses of people you know.
- Phishing: These are emails disguised to look like a legitimate company or bank to illegitimately obtain personal information. They usually ask you to verify your personal information or account details. Often links will direct you to a fake website, made to look like the real thing.
- Social engineering: In the context of security, social engineering refers to manipulating people to do something or divulge confidential information. For example, you might get a call from someone pretending to be from a software supplier, claiming that a virus has been found on your PC; they demand personal details before they can remove the virus.
- Spoofing: A spoofed email is where the sender (in this case, a criminal) purposely alters part of the email to make it look as though it was from someone else. Commonly, the sender's name/address and the body of the message are made to look as though it was from a legitimate source. It is commonly used to trick the recipient into providing confidential information such as passwords, or to market an online service dishonestly, or to sell a bogus product. Check the real sender of any email you receive if you ever have any doubt or uncertainty. If the sending address is one you don't recognise, do not click on any link contained within the email.

The scans approximately 14 million messages a month for threats (figures from November 2020). Of these, we might expect to find 1.4 million "spam" messages, 150,000 "phishing" messages, and about 1,000 malware messages (including viruses). Unfortunately, not every virus or spam email will be identified and blocked. The good news is that there are some simple steps you can take to reduce the threat:

- If you are not expecting the email, do not reply to it.
- If you are at all suspicious, do not divulge your details or any sensitive information.
- Avoid opening potential scam emails.
- Don't open unexpected attachments or click on strange links in emails, even if the email appears to be from someone you know. Check the style and content; if it isn't consistent with previous emails, it could be a scam.
- Do not reveal personal or other sensitive information in response to automatic email requests.
- Avoid sharing your business email address on the internet. These might be collected and used by automatic 'harvesting' software programs.
- Never use your email address to register for non-work related sites.

If you think you've received a scam email, or a virus, report it immediately. Do not click on any link or forward it to anyone. Only delete it from your inbox when you have been told to do so.

Further reading from the NCSC

Email security and anti-spoofing

Other email problems

Auto-forward

Auto-forwarding is where you get your email system to send emails automatically to another account. This might seem very useful, especially if for some reason you can't access your normal business email account, for example while you are away on holiday.

But auto-forwarding is very risky.

You can't be certain that the forwarded emails are safe to send to the new account. For example, the new account might have weaker technical security, making it easier for a hacker to break in and read your email.

You might also be auto-forwarding emails sent to you from outside the ; perhaps from another government department or commercial organisation.

When an email is sent to you, you are responsible for ensuring that everything in the email is handled correctly. This means looking after it to the standard required for that information. You mustn't send that information to another email address, where the required security standards might not be met.

Never use auto-forwarding to forward emails from your business email address to another non- email address. In particular, never forward email from your business email address to a personal email address.

There might be occasions when you have a genuine business need to auto-forward email to another email account, where the new address has the same or higher security standards. An example is forwarding from an business email address to another business email address. If you have business need for this, ask for help.

Chain letters

These are letters sent to several people who are asked to send copies to several others. They sometimes threaten that bad things will happen if the letter is not forwarded. Chain letters are a hoax.

Chain letters usually do not have the name and contact information of the original sender so it is impossible to check on their authenticity.

Legitimate warnings and solicitations will always have complete contact information from the person sending the message.

Newer chain letters may have a name and contact information but that person either does not exist or is not responsible for the hoax message.

Warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist, are probably hoaxes.

Don't circulate warnings yourself; real warnings about viruses and other network problems are issued for everyone by technical services.

Note: When in doubt, don't send it out.

Scams

Scams are "get rich quick" schemes. They make claims such as promising your bank account will soon be stuffed full of cash if follow the detailed instructions in the letter or email. In reality, it is an illegal plan for making money.

A typical scam includes the names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then remove that name and add yours to the bottom.

You are then supposed to mail copies of the letter or email to a few more individuals who will hopefully repeat the entire process. The letter promises that if they follow the same procedure, your name will gradually move to the top of the list and you'll receive money.

Other high-tech scams using IT also exist. They might be sent over the internet, or may require the copying and mailing of computer disks rather than paper. Regardless of the technology used to advance the scheme, the end result is still the same.

Scams are a bad investment. You certainly won't get rich. You will receive little or no money. The few pounds you may get will probably not be as much as you spend making and mailing copies of the letter if hard copy.

By their very nature, scams are harassing. Sending such mails using facilities is prohibited. The misuse of computer resources to harass other individuals or groups is unacceptable. Any person tempted to forward an email scam should familiarise themselves with the HR intranet pages, particularly the section regarding disciplinary action and electronic communications.

Note: Scams also clog up the system and reduce the efficiency of our servers.

How to recognise a scam

From the older printed letters, to the newer electronic kind, scams follow a similar pattern, with three recognisable parts:

- A hook: this to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl is dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
- A threat: when you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. Others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.
- A request: some older chain letters ask you to send money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to "Distribute this letter to as many people as possible." They never mention clogging the internet or the fact that the message is a fake; they only want you to pass it on to others.

If it sounds too good to be true, then it is!

Bogus calls

There are a range of scams that can target you at home or at work. Callers usually say they are from IT Support, and tell you that they have detected a virus on your machine that needs to be removed. The bogus caller will then either:

- Direct you to a website, in the hope you will download malicious software.
- Try and obtain details from you about your computer, or the network.

In all genuine situations, the will provide you with an incident reference number if there is a real problem with your machine.

If you receive a call from someone claiming to be from the , always ensure you ask them for the incident reference number. Then disconnect the call, and call the yourself, directly. If the original call was genuine, when you provide the incident reference number, they will be able to help you.

In general:

- Treat all unsolicited calls as suspicious.
- If possible, note the details and incoming telephone number of the caller.
- Do not go to any external site if directed from an unsolicited call.
- Never give any information about your computer to the caller.
- Check if the call is genuine with your . Report the call as a security incident if it is not. Use a different phone from that used to take the original call.

Hoaxes

Hoax letters are designed to trick you into believing, or accepting as genuine, something false and often preposterous: the messages they contain are usually untrue.

Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people. Who wouldn't want to warn there friends about some terrible virus that is destroying people's systems? Or help this poor little girl who is about to die from cancer?.

Chain letters and hoax messages have the same purpose but use a slightly different method of coercing you into passing them on. Chain letters, like their printed ancestors, generally offer luck or money if you send them on (scams). They play on your fear of bad luck and the knowledge that it is easy for you to send them on. Scams play on people's greed and are illegal no matter what they say in the letter.

The risk and cost of hoaxes

The cost and risk associated with hoaxes may not seem to be that high. If, however, you consider the cost of everyone within the receiving one hoax message, spending two minutes reading it and another two minutes forwarding it on or discarding it, the cost can be significant.

Handling these messages may also make our mail servers slow down to a crawl or crash.

Spammers (bulk mailers of unsolicited mail) may harvest email addresses from hoaxes and chain letters. Many of these letters contain hundreds of legitimate addresses, which is what the spammers want. There are also rumours that spammers are deliberately starting hoaxes and chain letters to gather email addresses.

How to recognise a hoax

A request to "send this to everyone you know" (or some variant) should raise a red flag. The warning is probably a hoax. It's unlikely a real warning message from a credible source will tell you to send it to everyone you know.

If the warning uses technical language, most people, including technologically savvy individuals, tend to believe the warning is real.

There may be credibility by association. If the janitor at a large technological organisation sends a warning to someone outside of that organisation, people on the outside tend to believe the warning because the company should know about those things. Even though the person sending the warning may not have a clue what he is talking about, the prestige of the company backs the warning, making it appear real.

These make it very difficult to be certain a warning is a hoax. Check if the claims are real, and if the person sending out the warning is a real person. Ask yourself if they are someone who would know what they are talking about.

Type of hoaxes

Scam chains

Mail messages that appear to be from a legitimate company but that are scams and cons, for example Advance fee scams.

Giveaways

Stories about giveaways by large companies. If you only send this on, some big company will send you a lot of money, clothes, a free vacation, etc., etc. You would have to wait forever for any of these to pay off.

Malicious warnings (virus hoaxes)

These are warnings about Trojans, viruses, and other malicious code, that have no basis in fact.

Virus hoaxes have flooded the internet with thousands of viruses worldwide. Paranoia in the internet community fuels such hoaxes. An example of this is the "Good Times" virus hoax, which started in 1994 and is still circulating the internet today. Instead of spreading from one computer to another by itself, Good Times relies on people to pass it along.

Sympathy letters and requests to help someone

Requests for help or sympathy for someone who has had a problem or accident.

Urban myths

Warnings and stories about bad things happening to people and animals that never really happened.

Inconsequential warnings

Out of date warnings and warnings about real things that are not really much of a problem.

True legends

Real stories and messages that are not hoaxes but are still making the rounds of the internet.

Traditional chain letters

Traditional chain letters that threaten bad luck if you don't send them on or request that you send money to the top "x" people on the list before sending it on.

Threat chains

Mail that threatens to hurt you, your computer, or someone else if you do not pass on the message.

Scare chains

Mail messages that warn you about terrible things that happen to people (especially women).

Jokes

Warning messages that it's hard to imagine anyone would believe.

Email and storing information

Data held by the should be managed in such a way that employees who require the data, for business reasons, can gain access to it. Managers should ensure that data is stored in an area that is easily accessible to those who require access. This includes information exchanged using email.

If you need further assistance or information about this process, ask for help.

Accessing emails or information in an absent employee's email account

Staff absences do occur and these can cause disruption to business where colleagues have no access to relevant departmental information. Staff are away for events such as annual leave, secondment or maternity leave, but they don't make provision for colleagues to access departmental information.

When an absence occurs, there is no right to be able to access another employee's account to obtain information. This is true, regardless of whether the absence is expected or unexpected, for example annual leave or illness.

Accessing another employee's account, without their permission, might contravene data protection legislation.

Data protection legislation protects personal information which relates to identifiable, living individuals held on computers. It specifies that appropriate security measures must be in place to protect against unauthorised access to, loss or destruction of personal data. If you breach this principle you could render the liable to enforcement action by the Information Commissioner.

Avoiding the problem

If you know you're going to be away for any significant amount of time, you can make life easier for everyone, including yourself, by following these simple steps:

1. Make provision for someone to have access to your work email account during your absence. If you don't know how to do this, contact your .
2. Create a "handover" package, containing information about the tasks that will, or might, need attention during your absence.
3. Make sure the package has contact details for everyone who might need to help progress or update the status of the tasks.
4. Create an "Out Of Office" notification in your email system; include clear details of who to contact in your absence.

Authorised access to user email accounts

You must not access the email accounts of any other users, unless you are authorised to do so as required by your role. Access is authorised on a case by case basis only, and will typically be aligned to the following circumstances:

- During a criminal investigation by a law enforcement agency.
- During an employee investigation relating to misconduct or a security incident, for example IT misuse.
- Upon the death or unexpected exit of an employee, for example for the retrieval of key information and closing down an account.

Ideally, access will have been organised in advance of an absence. But this is not always the case; sometimes there are unexpected or unusual circumstances. Gaining access in such situations will require substantial escalation to management and Data Privacy and Security teams.

Anyone needing access to someone else's email account should read the Privileged Account Management Guide, then get in touch for further assistance.

Contacts for getting help

In practice, all sorts of things can go wrong with email from time-to-time. Don't be afraid to report a problem or ask for help; you'll be creating a better and safer work environment.

For general assistance on security matters, email .

Suppliers to the should primarily contact your usual points of contact.

Email Authentication Guide

This guide identifies the security controls that or be implemented at the domain layer to verify sender's domains and mitigate spoofing attacks.

It is policy to follow and comply with HMG Email Security policy.

This means that the implements a number of controls for email systems:

- Sender Policy Framework
- Domain Keys Identified Mail
- Domain-based Message Authentication, Reporting and Conformance
- Mail Transfer Agent Strict Transport Security
- TLS Reporting

Related information

Email Security Guide on page 277

Sender Policy Framework

Sender Policy Framework (SPF) be implemented for email domains. SPF enables organisations to publish a Domain Name System (DNS) record of all the domains and IP addresses which are trusted for sending and receiving email.

SPF is verified by checking a specific `TXT` DNS entry in emails. Emails are flagged if they are not sent from the domains and IP addresses published in the DNS record.

The enforces SPF controls to help users spot spoofed or unknown email addresses. Suspicious emails are sent directly to the "spam" folder, instead of to the user's inbox.

When creating an SPF record in the public DNS, use all the IP addresses or address ranges from which an email might be sent. You can use both IPv4 and IPv6 addresses. An SPF record might look like the following:

- An example of a basic SPF record to be added to an organisation's public DNS, where it uses Google, might be:

```
v=spf1 include:spf.google.com ~all
```

- An SPF record including Google's IP ranges and a sending service with an IP address range, might be:

```
v=spf1 include:spf.google.com ip4:80.88.21.0/20 ~all
```

- An example of a more complex record, with additional services and some dedicated IP addresses, might be:

```
v=spf1 include:spf.protection.outlook.com include:mail.zendesk.com
ip6:2001:db8::/32 ip4:203.0.113.6 ~all
```

In the previous examples, `v=spf1` is an SPF record, `include:` means email can only come from these sources, `~all` considers any other email as a soft fail, and `-all` considers any other email as a hard fail.

Note: A hard fail be used when a domain is being forged by spam.

To correct SPF failures, add the sending systems you use to your SPF record. Do this using either the IP address or by reference to another SPF record. These previous examples are unique, so check the actual domain or IP range of the email sending service. Also check with the supplier on setting up SPF records.

Domain Keys Identified Mail

Domain Keys Identified Mail (DKIM) be enabled for all email domains. DKIM enables automatic filtering or rejection of emails that fail DKIM verification.

- DKIM can verify a sender domain by looking up the sender's public key published in the DNS. You can then determine if an email has been tampered with during transit, for example during a "Man-In-The-Middle" attack.
- A valid digital signature provides assurance that the hashed content has not been modified since the signature was affixed to the email message.
- The enforces DKIM controls to help users identify communication tampering attacks by sending the messages directly to the spam folder, instead of to the user Inbox.
- DKIM be used across the , including by executive agencies and ALBs.

Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication standard that be used with SPF and DKIM to:

- Confirm a sender's email addresses.
- Flag any emails that have been spoofed or otherwise tampered with.

By using DMARC:

- emails are more likely to reach the recipients' inboxes (suppliers, partners and public users), rather than getting filtered out as spam.
- There is full visibility of all the domains and IP addresses used to send emails.
- There are warnings if a mail sender fails SPF, DKIM, or DMARC authentication.
- It is possible to detect any unauthorised use of the domain.

When developing a new service with email sending or receiving capability, a DMARC policy be published. The policy be set to the highest level:

```
'p=reject'
```

This policy indicates that mailbox providers reject all emails that fail DMARC.

If the DMARC policy cannot be set to `'p=reject'`, publish a record using `'p=none'` to override the default DMARC policy. This means that the mailbox provider won't take any actions with emails that fail DMARC.

Publish a DMARC record to the DNS for the domain to tell the email receiver how to handle emails that fail DMARC authentication, and where to send DMARC reports.

DMARC Profiles	Benefits	Risks
`p=none`	Allows you to review incoming email to determine legitimacy while implementing DMARC for the first time.	Easier for phishers and spammers to take advantage.
`P=quarantine`	Malicious email is filtered out. Recipients decide what they want to do with quarantined email.	Legitimate emails might be missed if incorrectly quarantined and filtered
`P=reject`	All malicious email is stopped. The intended recipient of malicious email is not aware of the email, as it won't be sent to a spam or quarantine folder.	Legitimate emails might fail authentication and be rejected without the recipient being aware.

`DMARC TXT` records be available for creation or iteration across the . This is to comply with the GOV.UK DMARC configuration guide page.

Mail Transfer Agent Strict Transport Security

Mail Transfer Agent Strict Transport Security (MTA-STS) is a protocol which tells services that are sending email to your organisation that your domain supports Transport Layer Security (TLS) 1.2 or higher. This protocol makes email less vulnerable to middle-person attacks, and allows the receiving email service to enforce encryption, without the risk of delivery failing.

The implement and use MTA-STS for email systems.

To 'enable' MTA-STS, publish a text file containing the MTA-STS policy. Before sending an email to the , the sending email service checks the Domain Name System (DNS) record of the email service for an MTA-STS policy.

It is policy to follow HMG Email Security policy for MTA-STS. The deploy an MTA-STS policy with `enforce` mode specified.

For more information on UK Government configuration and use of MTA-STS, refer to the published guidance.

TLS Reporting

TLS Reporting (TLS-RPT) is a protocol that allows a domain to advertise a destination for sending email services to report the success or failure of encryption in transit.

The implement and use TLS-RPT for email systems.

To 'enable' TLS-RPT, publish a DNS record telling mail sender tools where to send TLS-RPT reports. A sending email service checks for the record, and if one exists it is used to send a report to the address provided.

For more information on UK Government configuration and use of TLS-RPT, refer to the published guidance.

Making changes to the domain name system

Changes be made to DNS records when implementing SPF, DKIM, DMARC, MTA-STS, and TLS-RPT controls. When requesting changes, specific information be included for each record. If given the option, set a short time to live (TTL) in DNS records to monitor changes quickly, and fix any issues.

DKIM example

Record type: `TXT`

Host or record name: `selector.`*`domainkey`*

Put your selector, or the selector provided by your service provider, in place of selector in the host or record name.

Record value: `v=DKIM1; k=rsa; p=<your DKIM key>`

Paste your DKIM key from your key generator in place of `<your DKIM key>`.

Some providers might use a `CNAME` record instead of a `TXT` record. Follow the guidance from your provider.

GSI is no longer used, but the following addresses still route through to `@justice.gov.uk`. The following table shows the authorised users you can contact to request DNS changes:

Record Type	Contact
`*.gsi.gov.uk`, `*.gsx.gov.uk`, `*.gse.gov.uk`, `*.gcsx.gov.uk`, `*.x.gsi.gov.uk`	Vodafone Contact GDS
`*.gov.uk` or any other domains	Your registrar, DNS provider or Internal System Admin
`*.cjsm.net`	Egress via

DMARC example

Record type: `TXT`

Host or record name: `dmarc`

Record value: `v=DMARC1;p=none;fo=1;rua=mailto:<example dmarc email address>,mailto:dmarc@<yourdomain.gov.uk>`

Create the email address and put your domain in place of `<yourdomain.gov.uk>`.

SPF example

Record type: `TXT` or `CNAME` (check guidance for your service on which to use).

Host or record name: `@` (if required)

Record value: `v=spf1 include:<your email server domain> ip4:<your email service IP> ~all`

Put your email server domains or email sending IP ranges in place of the < > sections. You do not need to include both. In many cases you might only need `include:`.

DNS contact details

For DNS changes and associated advice, contact the Platforms and Architecture team: domains@digital.justice.gov.uk

Email blocking policy

This document outlines the policy for blocking emails, and deleting emails through administrative processes across email services across the estate. It specifically highlights the reasons for active inclusion on an email blocklist and removal from mailboxes.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.EBL.xxx**, where **xxx** is a unique ID number.

Related information

Acceptable use of Information Technology at work on page 50
Data Security and Privacy on page 351
Email blocking process on page 273
Malware Protection Guide - Overview on page 174
Data Handling and Information Sharing Guide on page 59
Email Security Guide on page 277

Scope

This policy applies to all email domains and gateways managed by the , across all the applicable email services. Specifically, this policy applies to both email traffic inbound (before it reaches the), and outbound (before it leaves the).

Blocklist definition

A blocklist is a real-time list, consisting of elements such as IP addresses, network ranges, domain names, email addresses, URLs, and other email characteristics. The common characteristic of the elements is that the sender is suspected of delivering spam.

The blocklist primary purpose is to prevent emails from entering or leaving the email services. Blocking emails is part of the overall cyber security strategy, providing defence-in-depth on managed email platforms.

Email types considered for blocking or removal include:

- Malicious emails.
- Phishing emails, including derivatives such as vishing, spearfishing, and whaling attacks.
- Spoofed or impersonation emails.
- Emails that cause disruption to the availability of an email service.
- Other harmful or threatening emails.

Blocking policy

POL.EBL.001: All email services used by the have the ability to add items to the blocklist. The have the appropriate permissions to update and review each email service blocklist.

POL.EBL.002: Any item added to an email service blocklist be replicated across the different services in use across the estate.

POL.EBL.003: Blocklist items added are regularly reviewed to ensure the relevance of the block. Timeframes for reviews reflect the retention policies on the individual email services. Any changes that are made as a result of a review be completed and documented under change or incident management processes.

POL.EBL.004: When establishing the criteria for adding an item to the blocklist, the go through an impact assessment to establish the impact of adding the specific item to the internal blocklist. If the impact might be substantial, for example causing widespread disruption, or where legitimate emails might be blocked, then the blocking object be reconsidered or rescoped.

POL.EBL.005: As part the review process, or as a result of a user reported issue such as an incident reported through a user's local IT Team, a legitimate email might become blocked because it is now on a blocklist. This might be where the email address was added to the blocklist manually, or incorrectly flagged by automated tools in the email system. In this scenario, the promptly unblock affected emails, and re-evaluate the blocking rule responsible, in line with this policy. This unblock happen through the incident management process. All users are encouraged to speak with their Local IT team about concerns with email delivery, or email blocking.

POL.EBL.006: In the event that a legitimate email is blocked by an automatic vendor driven process, or included as an "indicator of compromise" through a threat intelligence product, the request that the object be reviewed or reclassified.

POL.EBL.007: Before adding any object to the blocklist, or automatically removing it from an mailbox, impact analysis be carried out and documented through the change/incident management process.

Deletion of existing emails in scope for blocking

POL.EBL.008: As part of the blocking procedure, the have the ability to delete or purge emails across the estate which match the blocking criteria listed in the blocklist. This is an optional step, done at the discretion of the .

POL.EBL.009: Purging of existing emails which have been added to the blocklist be done under peer review. Peer review be completed by an independent member of the team who is not involved directly in the analysis or investigation of the email. Peer review takes place only if there is a further threat of users interacting with the newly classified email.

POL.EBL.010: If deletion of emails takes place, then details of the criteria be included as part of the documentation process recorded as part of change or incident management.

POL.EBL.011: Where appropriate, users are encouraged to delete for themselves any emails confirmed to be in scope for blocking or deletion. Deletion of emails by the take place only where there is a significant number of users who received the newly classified email.

POL.EBL.012: Removing emails from recipient mailboxes is a viable alternative to adding emails to an email blocklist. This be the preferred option to prevent users from interacting with emails considered for blocking or removal.

POL.EBL.013: Deletion of emails be done in such a way that the email could be recovered if required. If this is not possible, the email be moved to the users 'junk' folder rather than simply being deleted.

POL.EBL.014: Users be made aware of the deletion of emails. However, this is not mandatory.

POL.EBL.015: The has no responsibility to delete emails from unmanaged mailboxes.

POL.EBL.016: Automatic deletion of emails for users be done through automated processes. The minimise access to the mailbox from which unwanted emails are purged.

Automated blocking tools

POL.EBL.017: email services come with inbuilt vendor managed blocking facilities based on known Indicators of Compromise (IOC's) to prevent emails entering or leaving the email environments. This vendor managed list either be done through general lists of IOCs, or heuristic scanning.

POL.EBL.018: The email service vendor provide the with the ability to reclassify incorrectly classified emails. This reclassification process be accessible to the Cyber Security team, as well as email administrators.

The Cyber Security Team encourages the integration with 3rd party threat intelligence feeds from trusted providers as part of the in-depth defence strategy.

Blocking or deleting received emails

POL.EBL.019: Any user who receives an email suspected to be one of the types described previously request that the email be blocked, preventing future similar emails from being received. On receipt of this, the reviews the evidence and determines if addition to a blocklist is appropriate. Further actions taken follow the policy statements in this guidance.

POL.EBL.020: Addition of emails to the blocklist is completed by either the local email service management team, or by the . If the former, then approval be obtained from the .

POL.EBL.021: In the event that an email is causing widespread disruptions or impacting business, then the individual email administration team responsible for the email platforms delete emails or place blocks on emails without prior approval. This be done under change and incident management, with notifications sent to the .

POL.EBL.022: The provide a way for users to request emails for review by the relevant teams.

Preemptive blocking

POL.EBL.023: If security receives intelligence about a credible threat to the confidentiality, integrity, or availability of an managed email service, then those emails be added to the blocklist. Before blocking according to this policy statement, the intelligence go through an impact analysis.

POL.EBL.024: All blocks remain in place until the threat is no longer a credible threat to the .

POL.EBL.025: Email from previously known or blocked items be re-added to the list if there is credible information or grounds to do so.

Automatic blocking of emails based on attachments

POL.EBL.026: The be able to restrict the delivery or sending of emails with certain malicious file attachment types.

POL.EBL.027: A complete list of email attachments blocked be kept and managed by the individual email administrators, and be consistent across different email services in use across the estate.

Email blocking process

The manages a number of different mail platforms, including infrastructure in , as well as Microsoft Exchange (on-premise) and Microsoft Cloud platforms.

There are numerous reasons that email might be blocked. An email matching the criteria on a blocklist is only one reason.

If you have any concerns about email delivery, contact your email service provider or Infrastructure exchange team.

Related information

Email blocking policy on page 271
Email Security Guide on page 277

Definitions

Within this guidance, 'email' might refer to individual user mailboxes, shared or group mailboxes, or distribution lists and mailing lists.

More specifically, a recipient or mailbox is any functional email account, for example .

Throughout this guidance, references to malicious emails include the following specific threats:

- Emails which contain malware.
- Phishing emails.
- Spoofed or impersonal emails.
- Harmful emails.
- General spam emails.

There are a number of different email threats that exist in information technology. Each threat varies in complexity, and the impact it might have on the and its employees.

Spam	Spam emails, also called junk emails, involve the sending of nearly identical messages to numerous recipients. They are high volume, unsolicited messages.
Malicious or malware	These emails are specifically designed to damage operational systems or disrupt business operations. While the email itself may not be malicious, it might contain URLs or file attachments which are malicious.
Phishing	This is an email-based attempt to acquire sensitive information such as credentials including IDs and passwords for malicious purposes. Phishing emails typically masquerade as a trustworthy person supposedly taking part in electronic communications.
Spoofed or impersonation emails	These emails are from a forged sender address. At first glance, the email seems to be from a respected or reputable email sender, or an individual you know or trust.
Harmful emails	These are emails that are not necessarily classified as malicious, but might cause distress or harm to users. Examples include threatening emails, or Denial of Service (DoS) attacks.

Email blocklist

The purpose of any email blocklist is to prevent malicious emails entering or leaving the email infrastructure.

A blocklist consists of some or all of the following elements:

- IP address.
- Network range.
- Domain name.
- Email address.
- URL.
- Other email characteristics.

Each element helps identify more precisely where the sender is suspected of delivering malicious emails.

Throughout this document, any item on the email blocklist is referred to as a 'blocklist object'.

Each individual mail platform has its own set of objects that can be added to the blocklist. These objects vary from product to product.

Note: Users interact with any unsolicited or unwanted emails. Instead, follow email spam handling processes. For more information on this, contact your local .

All email platforms in use by the have the ability to add items to the blocklist. The security team have appropriate permissions to update and review items on this list.

Internal blocklist

There are two specific types of blocklists:

- Individual mailbox blocklist.
- Global blocklist.

Each mail platform that the manages has its own internal blocklist. Any object added to an internal blocklist is blocked from reaching mailboxes or recipients in that mail platform. Where possible, when a specific object is added to an internal blocklist in one platform, it be replicated to other email environments.

The criteria for adding items to the internal blocklist are outlined in this policy.

Note: Individual mailboxes might have their own internal blocklist. This is a preferred route for requests to add domains to the global blocklist. Owners of individual mailboxes are responsible for managing their own individual mailbox blocklists.

If a user has multiple email addresses spanning different email platforms, then it's the users responsibility to keep their personal blocklists synchronised between the platforms.

External blockList

The Security team use a number of commercial products which provide estate-wide or 'global' blocking, rather than individual blocking.

By default, external email blocklists are applied at the global level, meaning that they are applied to all mailboxes in an email environment.

Auditing

All emails that are received into the email platforms have AntiVirus scanning in place. The scanning includes automatic detection, classification, and responding to suspicious emails.

Be aware that email filtering and blocking can not be 100% effective. This means any suspicious or unsolicited emails always be treated with caution. Similarly, an e-mail might be incorrectly marked as infected or "spam". This might result in some emails being blocked unnecessarily.

Freedom of Information (FOI) requests

The is a public sector organisation. This means that any member of the public has the right to make an request for information about any item of public interest. General information about FOI is available on the Intranet. Security-specific considerations are outlined in the Data Handling and Information Sharing Guide.

The Security team applies vendor processes to remove an object or item from the external blocklist, where appropriate.

Note: The Security team cannot assist with troubleshooting generic email delivery issues.

Requests to remove objects from a blocklist

If you have concerns about the use of a blocklist, you need to provide relevant information about the problem, such as:

- Sending IP address.
- Time and date, including timezone information.
- Error messages, such as undeliverable mail notifications.

You might also be asked to provide other information to help determine the specific reason why the email has not been delivered. In response, the reviews internal and external blocklists, and determines if the email was indeed blocked by an object on the blocklist.

If you believe that you cannot access justice services due to a blocklist, then you can request that a review of blocklist by the .

Requests for review are assessed on an individual basis, working with the information disclosure team, to determine resolution steps.

Impact assessment

Any blocklist object be defined so as to not result in widespread email failures. For example, it would not be helpful to block the whole of `@gmail.com`. Each blocklist object be examined, taking into account the characteristics of the specific blocklist, and relevant intelligence sources.

Senders that have an established history of clean or legitimate emails, but have recently been sending emails of concern, be added automatically or instantly to the blocklist. Instead, the sender be 'quarantined' by the affected email system.

Avoiding the use of blocklists

Requests are sometimes made to block individual senders based on repeat, vexatious, or otherwise undesirable content. Take care when determining whether the sender truly has malicious intent, or whether they are a simply a member of the public with a genuine grievance but lacking the skills to air their concerns more constructively. Consider the risk of 'denying access to the criminal justice system' to an individual. If in doubt, refer to the .

Documentation for internal blocklists

Use the incident management and change management process to add emails to internal blocklists. This includes documenting expected impact, and other relevant information.

As part of the documentation steps, the assessment and justifications for blocking specific objects be included. Ensure the information is brief but contains sufficient relevant information. The relevant information include:

- The specific items to be added to the internal blocklist.
- The classification of the email, and justification for blocking.
- Summary outcomes from the impact assessment.
- Summary actions taken to triage and resolve the incident, before resorting to blocking.

One ticket might contain multiple different blocking objects.

If an item is blocked without a corresponding ticket and justification as described in this guidance, then that object be removed from the internal blocklist with immediate effect.

Review of existing blocks

The review items manually added to the internal blocklist, on a regular basis, to determine if they are relevant or not. Regular means at least every quarter. Any item included in the list and which is considered irrelevant be removed. An irrelevant item is one that blocks legitimate emails from entering the email system.

A review of internal blocklist also be done frequently, in line with the time for which blocked email messages are kept. This ensures the is able to recover incorrectly-blocked emails, and avoid them being deleted automatically.

Spam emails

The ICO website provides general information about spam, and gives advice about the steps to reduce spam.

A spam email does not necessarily require automatic and instant inclusion on the internal blocklist, although it might be included as part of the external blocklists, as highlighted in this policy.

Blocklist listing policies

The email platforms have the ability to deploy automatic blocking of traffic. This includes blocking the following email classifications:

- Spam traffic.
- Malware traffic.
- Open proxy or open relays.
- Shared cyber threat intelligence.
- Spoofed domains.

Reporting incidents to external companies

The reserves the right to forward any email suspected of being added to the blocklist to external organisations for verification.

Organisation that are trusted by the for this purpose include:

- Google.
- ICO
- Microsoft.
- Netcraft.
- NCSC.

In such cases, after forwarding, the delete email messages from affected mailboxes.

Email Security Guide

This guide sets out the requirements for implementing and maintaining email security across the .

Related information

Email Authentication Guide on page 268
Email blocking policy on page 271
Email blocking process on page 273
Secure Email Transfer Guide on page 291
Spam and Phishing Guide on page 297

Who is this for?

This guide is aimed at two audiences:

- The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
- Any other business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, and storing data) for, or on behalf of, the .

These audiences are referred to as "technical users".

Roles and responsibilities

All technical users are responsible for maintaining and using the 's email communications securely, in line with the requirements set out in this guide. In particular:

- Where possible, automate checks of the sender's authenticity by implementing the controls in the Email Authentication Guide.
- Ensure all email communications are protected according to the classification of the information held within them. There is more information in the the Information Classification Handling and Security Guide.
- Discourage people from downloading data to mobile devices. Instead, encourage and enable the use of cloud services such as Office 365.
- Make it easy for people to send suspected or actual phishing emails to the , so that the emails can be handled safely.
- Keep operating systems up-to-date, to prevent susceptibility to viruses.
- Scan email attachments to detect viruses and other malware.
- Ensure email services are appropriately authenticated. Refer to the Email Authentication Guide for more information.
- Ensure secure email messaging services, and, where necessary, encryption tools, are used to transfer sensitive information and system secrets. Refer to the Secure Email Transfer Guide for further information.

- Ensure that email configuration is secure, and that all necessary technical controls, including those set out in the Malware Protection Guide, are implemented and kept up to date.

Note: Suppliers use their own email services if agreed by the but, as a minimum, they must meet the security requirements.

Authorised access to user accounts

By default, users access the email accounts of any other users, unless they are authorised to do so as required by their role. Access is authorised on a case-by-case basis only, and is normally aligned to the following circumstances:

- After a criminal investigation has been opened by a law enforcement agency.
- After an employee investigation has been opened relating to misconduct or a security incident, for example IT misuse.
- Upon the death or unexpected exit of an employee, for example to enable retrieval of business information or closing down an account.
- For long-term archiving of information no longer in current use.

Anyone required to enable or carry out authorised access to a user account should follow the guidance in the Privileged User Guide.

Monitoring

The does monitor Email services for security purposes.

Delegate access

Ensure that standard end users do not by default have the permissions necessary to provide another user with delegate access to their account. There will, however, be occasions when an IT user might need to give another user access to their email account.

Examples would be where a mailbox owner has a legitimate requirement for another user to:

- Read, send, or delete messages on their behalf.
- Manage their calendar.

In this situation, the user first seek permission from their line manager. When permission is granted, technical users ensure secure delegation by:

- Enforcing mailbox owners to limit delegate access to pre-defined periods of time.
- Enabling mailbox owners to manage and revoke access themselves.
- Prevent federated sharing, where users in one organisation can share free or busy calendar information with recipients in other organisations.
- Preventing auto-forwards to external email services, including personal email accounts.
- Preventing delegate access to unauthorised users, such as people outside the), by enforcing Role Based Access Control (RBAC).
- Implementing Access Control Policy, in particular regarding access to email as a result of forwarding or delegation.

For individual accounts, the can configure delegate access. Administrators of group inboxes can also configure delegate access to those inboxes.

For further details, refer to the Privileged User Guide.

Phishing or spoofing of users

staff, contractors, suppliers or other partner organisations deliberately send phishing or spoof emails, or similar malware communications, to any users for any purpose.

If there is a valid business need to send a fake message, for example to test the resilience of an end-to-end business process against an attack, then prior approval for the fake message be obtained from the . Do this by contacting .

General app guidance

When working, you need to communicate with colleagues and use business tools ('apps'). You'll also need to work with people outside the . There are various tools you might use, besides the standard email and telephone tools. This document tells you about the tools you can, and cannot, use for business purposes. This guidance applies to all staff and contractors who work for the .

Some ALBs, Agencies, or other large groups within the might have their own, specific guidance regarding how to use certain apps for different purposes.

Access to tools

You can access tools that are provided through your provided devices by downloading from:

- The Software Centre application on your device (for Dom1 equipment).
- The Self Service application on your Mac (for managed MacBook laptops).

Currently, access to the tools mentioned in this document is not available from Quantum devices.

For other provided devices, seek help from your Line Manager in the first instance.

Corporate, work and personal accounts

- A corporate account is for making official statements and providing official views. Only a small number of authorised people can use it.
- A work account is your normal account, that you use every day for business as usual. Only you have access to your work account.
- A personal account is your own personal account on gmail, hotmail, yahoo, and so on. You should never use a personal account for business purposes. To be clear: never send your work material to your personal device or your personal email account.

Some of the applications listed make a distinction between general use with a work account, and use with a corporate account. Using a tool with a corporate account means you are providing views or statements on behalf of the . Never use a personal account for business purposes with any tool.

Remember that if you are authorised to use a corporate account, you are speaking and acting for the whole of the . When working with a personal account, you are speaking and acting as an employee and a civil servant.

Always follow all policies and guidelines regarding public information, including social media. To access this information you'll need to be connected to the Intranet.

In particular, follow the Civil Service Code of Conduct.

Video conference hardware

There are specific security concerns when using video conferencing hardware. The hardware might need extra permissions, involving access to the network, or involving personally identifiable information.

Video conferencing hardware might also be in a 'constant listening state'. This means that anything said within hearing distance, at any time, is 'heard' by the device. Similarly, anything in the line of sight might be 'seen' by the device. Some video conferencing hardware might record and even store the audio or video data outside the .

Video conferencing hardware for use within the meet the required security standards of the . Any devices that do not meet the security standards be used. The reason is that the hardware might be insecure, and therefore unsafe to use for conversations.

Using video conference tools safely

The NCSC has excellent guidance on using video conferencing services safely.

Key things to remember *before* a call include:

- Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password.
- Test the service before making (or joining) your first call.

- Understand what features are available, for example recording the call or sharing files or screen information.

Key things to remember for *every* call include:

- Do not make the calls public, for example always require a password to join the call.
- Know who is joining the call, in particular check that everyone is known and expected to be present, and that people who have dialled in have identified themselves clearly and sufficiently.
- Consider your surroundings, for example checking what can be seen behind you (forgetting to check information on a whiteboard or noticeboard is an easy mistake).

Policy and guidance and Information

information is the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

is not a classification. is a handling caveat for a small subset of information marked that requires special handling by staff. You should apply the handling caveat where you wish to control access to that information, whether in a document, email, or other form.

Privacy and personal information (Data Protection)

Some communications tools expect to have a copy of your contacts list. The list is uploaded to the tool server in order to let the tool to function correctly. Think carefully about whether this is reasonable to do. Make sure that sharing your contacts list does not impact any one else's privacy in a negative way.

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

- Email:
- Slack: `#security_privacy_and_live_service_team`
- Intranet: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/

Information Management

Many of the tools are only used for your day-to-day communication with colleagues. The information you work with is typically classified at .

Think about the information you work with when using these tools. What would happen if you lost your mobile device, or it's stolen? Suppose the voice or video call was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use the tool to communicate that information with colleagues.

You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is Principle 2 of the Government Security Classifications. The trusts you to work with information. You're trusted to make a reasoned judgement about whether it's safe to use an approved tool, or whether you should use a different -provided work tool.

Never send work material to your personal devices or email accounts.

Remember that it is impossible to delete information after it's released in public.

For more information about IT Security, look on the Intranet here.

Storage and data retention

Laws and regulations make the and its employees responsible for managing information. Some examples include:

- Freedom of Information Act.
- Data Protection Act and General Data Protection Regulation.
- Public Records Acts.

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate systems helps us, because:

- We can provide evidence about decisions.
- We understand the information held, and where to find it.
- We can transfer records to The National Archives.

Always store information in systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate system. Guidance on what you must keep is available on the Intranet here. At regular and convenient intervals, transfer the information to an appropriate system. Do the same when you finish the work. Don't forget to remove any redundant information from a tool by clearing or deleting data if it has been preserved in an system.

Many tools lets you export your data. You can then store it on an appropriate system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the Information Management section on the Intranet. There is also help on responding to requests for information.

Acceptable Use

You must use communications tools for business purposes in an acceptable way.

Be sensible when using communications tools for business purposes:

- Be extra careful with sensitive and personal information in tools.
- Try to avoid using the same tool for business and personal use - you can get confused who you're talking with.
- If the message you're about to send might cause problems, upset, offence, or embarrassment, it's not acceptable.
- Context is important - a message you might think is funny could be upsetting to someone else.
- If something goes wrong, report it.

The bottom line is:

> If there is doubt, there is no doubt - ask for help!

Approved tools

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Apple Facetime	Communication tool: Video	Avoid personal or sensitive data	Smartphone App	Internal/ External
Apple iMessage	Text messaging	Avoid personal or sensitive data	Smartphone App	Internal/ External
Google Meet (was Google Hangouts)	Communication tool: Video and/or voice	use approved for and	controlled Mac - Self service, Web browser.	Internal/ External
Microsoft Teams	Communication and collaboration tool: Video and/or voice	use approved for and	Dom1 Software centre, controlled Mac - Self service, Web browser.	Internal/ External
Miro	Collaboration tool: Whiteboarding	Avoid personal or sensitive data	Web browser.	Internal/ External
Skype for Business	Communication tool: Video and/or voice	use approved for and	Dom1 Software centre, controlled Mac - Self service, Web browser.	Internal/ External
Slack	Text messaging, Voice/ Video calls, etc.	Avoid personal or sensitive data	controlled Mac - Self service, Web browser.	Internal/ External

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Slido	Q&A tool during presentations	Avoid personal or sensitive data	Web browser.	Internal
Trello	Project management tool, 'Kanban' cards	Avoid personal or sensitive data. An enterprise-wide licence is available. Ensure you create Trello boards in the workspace. Do not use a personal Trello account.	Web browser based use. Log in using your single sign-on account, for example a Digital & Technology Google account, or a Microsoft Office 365 account.	Internal
Twitter	Text Messaging, Video transmission	Approved for Corporate account. Using a personal account to comment on work related issues is encouraged, as long as you follow the Civil Service Code of Conduct.	Web browser, Windows 10 App, Smartphone App.	Internal/ External
WhatsApp	Text messaging, Voice/ Video calls	Avoid personal or sensitive data	Dedicated app on device, also web browser.	Internal/ External
Yammer	Text messaging	Avoid personal or sensitive data	Dedicated app on device	Internal
YouTube	Video sharing tool: Video, streaming and chat	Avoid personal or sensitive data	Web browser based use.	Internal/ External
Zoom	Communication tool: Video, voice and chat	Avoid personal or sensitive data	Web browser based use, or dedicated and installed app by approval	External meetings. For Internal meetings, use Microsoft Teams.

Password managers

guidance encourages the use of password managers where possible. To establish what options are available for an -issued device, check the official software and application installation tool provided with the device, to see whether it includes a facility to install optional software and whether a password manager is among the options.

Tools for sharing information internally and externally

For secure sharing and transfer of materials within bodies or external organisations including other government departments, the installation of Microsoft Teams is approved for use with data up to and including .

For secure sharing and transfer of materials with external organisations that cannot use Teams, the Criminal Justice Secure Exchange (CJSE) and Criminal Justice Secure Messaging (CJSM) tools are the preferred solution for data up to and including .

For secure sharing and transfer of materials with external organisations where the use of Teams, CJSE, or CJSM is not practicable, the following tools are approved for data up to and including :

- Egress (NCSC certified)
- Galaxkey (NCSC certified)

For use within bodies, these products may only be installed on -issued devices. For advice on installation and configuration of these products, consult the team responsible for the supply and configuration of your devices.

For secure sharing and transfer of materials with other government bodies, where the use of Teams, CJSE, CJSM, Egress, or Galaxkey is not possible, the use of official email systems is approved for data up to and including .

Always follow the guidance in the Data Handling and Information Sharing Guide when making such transfers. This applies particularly with regard to the sharing of data classified higher than .

If you need clarification or further assistance in selecting the appropriate tool, ask for help.

Proctoring software

You install proctoring software onto equipment.

Some certification or examination organisations enable people to take assessments remotely. They do this by having 'supervision' software installed on the user's computer. This software is often referred to as 'proctoring software'. The tools make sure that the assessment is as fair as possible, by installing a variety of controls. For example, the software can take control of the camera and microphone of the device it is installed on.

The problem is that the controls give the proctoring software extensive access to the computer. This means that the tools could inspect information or other applications on the computer. In effect, the proctoring software might have uncontrolled access to information or materials on the computer. This is not acceptable.

If you need to use proctoring software, your options are:

- Install the proctoring software on a personal device.
- Contact the assessment organisation asking for alternative options.

NHS Track and Trace

The official NHS Covid-19 app was designed by the NHS. Both NCSC and Cabinet Office have been involved in the security of the system. The app provides contact tracing, local area alerts and venue check-in. It enables you to protect yourself and your loved ones. Installation is optional, but recommended.

After installing the app, you'll receive an alert if you have been in close contact with other people who have tested positive for coronavirus. You can then take action to avoid passing the virus on, for example by self-isolating.

From a security perspective, it is safe for you to use the app on your personal or issued devices. There are no extra risks for colleagues with security clearance, such as SC and DV.

If you wish to install the app, start at the NHS site.

Note: The NHS app may not work on some older devices. Installation might not be possible, for example on Quantum smartphones.

You might have both a personal and an issued device. Think about which device makes most sense to use with the app. It's best to install on the device that you carry with you and use most of the time. You could install on all your devices if you prefer.

To reduce the likelihood of false alerts on the app, turn off the app's Bluetooth mode. Do this when:

- You are working in environments with protective Covid measures in-place, for example plexiglass separators.
- You need to leave your personal or work device in a locker, for example during a sports activity or to work in a secure facility.

Other tools

Some tools, such as Facebook, Instagram and LinkedIn, are approved for specific corporate accounts to use, for corporate communications messages. General use of these tools for work purposes is not permitted.

If you wish to use a tool that is not listed in this guidance, please consult our Guidance for using Open Internet Tools and ask for help.

Other information
Government policy and guidance

GDS Social Media Playbook

NCSC

Video conferencing services: using them securely

Secure communications principles

Using third-party applications

Phishing Guide

This guide provides information about 'phishing' is. It describes what phishing is, and how it happens. It tells you what you can do to protect yourself, and to keep systems secure.

There is also information on what to do if you think you have been phished.

What is a phish?

Phishing attacks are when threat actors pretend to be legitimate parties. They do this to steal money, credentials, or sensitive information. There are a variety of phishing attacks that you might come across. Some are more sophisticated or targeted than others.

Phishes often use two techniques:

- They affect emotional states.
- They create a sense of urgency.

Urgency makes users want to do the actions requested as quickly as possible. The combination of urgency and emotional manipulation leaves users feeling panicked and worried. It might fill them with a sense of euphoria. Threat actors use emotion and deadlines to convince users to act. The user doesn't take the time to think about whether it's a sensible or valid request.

Most phishes are emails, but they can also use other technology, such as SMS texts or telephone calls.

Threat actors might use phishes to request payments. They might ask you to click links and log in to an account or change a password. They might instruct you to buy items for them. They might get you to provide some personal details before you can claim a supposed prize.

Threat actors utilise a variety of methods in phishes. They often take advantage of seasonal events to appear more legitimate. They use emotional and urgent triggers such as:

- Telling you that your tax return is overdue.
- Threatening to share access to your personal sensitive photos unless you pay.
- A request to send money urgently to a family member in trouble.
- Telling you 'good news' ,for example that you have won a big prize or are due a tax rebate.
- Providing a final demand about a very overdue invoice that, if unpaid, will see you taken to court.
- A 'last warning' about resetting your password, otherwise you will lose account access.

Beware of messages that create a sense of urgency or a heightened emotional state - good or bad. Treat such messages with suspicion. Check the message before you take any action. Unexpected messages with attachments are also common. Never open the attachment until you have done checked and verified the legitmacy.

Common types of phish

There are many different types of phish. You might recognise many of them. But the more sophisticated the phishing attack, the harder it is to spot. Checking and verifying are the best way to stop a phishing attack. They use a second, different method of communication to check the authenticity of the contact and the requested action.

Email phishing

These are emails that request actions. Examples include clicking on links to change passwords, or requesting money.

SMS phishing (smishing)

These are text messages that ask you to click links to access services or to pay for things. They often take advantage of seasonal events to appear more legitimate. Examples include Christmas delivery phishing texts, or texts around tax return time. Other recent examples use Covid news items to demand payments or personal information.

Voice phishing (vishing)

These are phone calls that ask you for sensitive information, or payments, or remote access to your devices. Threat actors might pretend to be from banks and other official organisations. Others might claim to be technology companies such as Microsoft. Another vishing example might claim to be from a jail, requesting bail money.

Spear phishing

Some phishing attacks focus on specific targets. Threat actors use OSINT to gather data about an individual. They can then create a 'custom phish'. It is interesting for the target. The target is then more likely to respond to the phish. Examples include real names or work-related jargon. These are often very sophisticated phishes. The use of personal data makes the phish more likely to succeed.

Whale phishing (whaling)

These target at high level individuals such as CEOs and Director level and above staff. Whaling uses a variety of phishing methods to contact high profile targets. The goal is to steal large sums of money, or access high level credentials, intellectual property, and sensitive information.

Business email compromise (BEC)

This type of phishing attack targets high level staff to steal money or reveal sensitive information. Threat actors pretend to be another high-level staff member. They do this by using their name or email address to seem legitimate. They often create a sense of urgency to convince junior staff to do the requested action. These emails often come from a compromised staff member's email account. This means the email system doesn't block the sender.

Watering hole attack

This is a very sophisticated supply chain attack. It uses research from an organisation's frequently used websites to identify a target. Targeted websites are then compromised and infected with malware. When users visit the websites, the malware downloads onto their systems. These are sophisticated attacks. The user is visiting an official and legitimate website. It is the website itself that has been compromised.

QR codes

Quick response codes (QR Codes) are a form of matrix (two-dimensional) barcode. They are machine-readable links. A QR code reader on a mobile device sends the user to a website or app. You don't need to click or type a link.

Some devices have QR code readers built into their camera app. Other devices need a dedicated app.

When you scan the QR code, the app asks you if you wish to go to the website or app described by the QR code.

Note: QR codes are not human readable. This means it is important to verify that the codes are legitimate and have not been tampered with.

You'll see QR codes in many situations. They give easy access to restaurant menus. They link to charity donation pages or surveys. Banks use them to link to services. They can be used to join wifi hotspots. They can be used to add contacts directly to your contacts list.

A QR code in an official context should be as safe to scan as an ordinary web link. For example, a QR code on an official notice in an building.

If the QR code is not labelled, or is from an unknown person, be suspicious. For example, a QR code stuck on a lamppost, or a QR code on a non-official flyer on a wall in a public location. These are not safe to scan.

It's possible that even a QR code in a safe, official place might be tampered with. Someone might draw over it. They might cover it with a sticker and a fresh QR code. If a QR code looks 'contaminated', don't scan it. Report it to security.

In summary, the risk associated with QR codes is currently considered low. They are simply barcode versions of web links. When deciding whether to scan a QR code or not, follow the same procedure as receiving an unexpected message .

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is a great way to reduce the risk of account compromise by a phishing attack. MFA provides an extra layer of defence for the account. If you have MFA set up, threat actors cannot access your account. It's safe, even if you accidentally reveal your credentials.

Never give MFA to codes to anyone. Genuine companies, banks, government departments, and social media sites will never contact you and ask you to tell them an MFA code. They will never offer to input it for you, or request you give the code to them over the phone. MFA codes should only ever be entered by you, directly into the account login.

MFA also provides an early warning system for credential compromise. If you ever receive an MFA code for an account that you are not actively logging into, then someone other than you is trying to access the account. This means your credentials might have been compromised, so as quickly as possible, you should:

- Report the problem to security.
- Change your password.

Check and Verify

Check and verify is an easy method to confirm the legitimacy of communications and requests. They can confirm the identity behind a message or request, and they can confirm the validity of the message or request itself. Social engineering techniques and phishing tactics take advantage of people who do not use check and verify. By checking and verifying, these sorts of attacks can be stopped very easily.

Checking and verifying is when an individual uses a different method of communication than the one the message came from. This method means that if one communication method is compromised, you quickly find out by using a different communication method to confirm validity. The likelihood of multiple communication methods for the same person or team being compromised is low.

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call – but not email – to confirm that they did indeed send the original email. If they did send the email, you can proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

Example 2: You receive a phone call from someone claiming to be your bank, or HMRC, or HMCTS. You hang up the call, and locate the official website for the company. You should be able to find multiple official contact details there. Use one of these to contact the place the caller claimed to be from. If, for example, the claim was that your bank was calling, you can call the direct number and speak to the switchboard about the reason for the initial call. They will forward you to the correct department. You can then confirm the validity of the original call, and so confirm whether the original caller was actually from your bank or not.

Example 3: Someone enters your place of work, and claims to have a meeting with a specific person. Unfortunately, there is no record of this on the expected visitor list. You can call or email the person within your place of work to confirm the visitor is legitimate. This check also works if tradespeople arrive unexpectedly, because you can contact both the relevant person within your place of work and also contact the company they claim to be from, using the company’s official website contact details.

Example 4: You receive an email requesting that you reset your password immediately. The email contains a link to perform the password reset. You have not attempted to login to that account recently. You should use an internet search for the website or type the URL directly if you know exactly what it should be. When you attempt to login, the website will let you know if you need to reset your password. If not, you know someone else has attempted to gain access to your account. That would mean the password reset request was not legitimate, and most likely a phishing attempt hoping to get your username and password through the reset link in the original email. Similarly, if you get an MFA request unexpectedly, do not confirm it unless you were indeed attempting to access that account immediately before the request came through. If you get an MFA request, but had not been trying to connect using the account, you should change the account password as soon as possible, because it might have been compromised.

When checking and verifying, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, check and verify by making a phone call. If someone calls you, check and verify by using the Internet. It is very unlikely that multiple communication channels have been compromised.

Be sure to get official contact details for companies only from their official websites. Never be afraid to hang up on someone and check their identity through another method, especially if they are asking for sensitive or personal information or credentials. Never be afraid to check the legitimacy of unusual email requests. by contacting the sender through a different communication channel.

By checking and verifying, it lets you confirm that the messages come from the person they claim to be, and that the requests are valid. This helps prevent you or your company from losing money to fake invoices, from accidentally giving up sensitive information or credentials, and from having unauthorised individuals in your place of work. Checking and verifying is fast and easy. All members of your workplace should be happy to receive such a check. It shows that you take security seriously, and that you are helping to protect them as well as yourself.

If you think you've been phished

Don't panic.

You will not be punished if you fall for a phish - it can happen to anyone. You will not be punished for reporting a phish, even if it turns out to be a false alarm.

If you think you have been phished:

1. Report it immediately.
2. If your credentials were phished, highlight that in the report.
3. Change the password for affected accounts as soon as possible. Never use the link in an email asking you to change a password. Check and verify by going directly to the website to change a password. Be cautious when following password actions requested in emails or texts.

firewalls and antivirus systems should catch the majority of malware before they can affect systems. By reporting the incident as quickly as possible, the security team will be alerted and on the lookout for any more sophisticated malware.

If your credentials have been phished, reporting it immediately and resetting your password quickly greatly reduces the risks.

Any phishing emails that get through the filters and into your inbox will be very sophisticated. This makes them much harder for you or anyone to spot. Never feel guilty or ashamed for being phished.

Reporting phishes

Reporting phishing attempts helps improve the filters that catch them before they get to your inbox. They also help protect other colleagues and the from being compromised, or having data or money stolen.

If you think you have spotted a phish, or you think you have been phished, report it as quickly as possible. If you think you have spotted a more targeted phish that claims to be from a vendor or another staff member, check and verify to determine if it is legitimate. If it is not, then please report the email as a phish.

Reporting a phishing attempt is quick and easy. Contact service desk using one of these two options:

You can also forward on all spam and phishing text messages to 7726 for free.

Protecting WhatsApp accounts

The permits the use of WhatsApp for text messaging, voice and video calls. You avoid using it for business tasks involving personal or sensitive data.

You always keep WhatsApp account details safe and secure. Accounts link with specific devices. When you register your device with a WhatsApp account, that provides some protection. Only the registered device can send or receive messages associated with you.

Unfortunately, device registration is a tempting target for attackers. It is a way for potential compromise of user data. Compromises affect backups of conversations, and contact lists.

A compromised account might also attack other people. An attacker might pretend to be a user, and so target other contacts. They might make their way to compromise a high-value target.

An example scenario might be an attack on the WhatsApp account of a family member of an employee. The attacker compromises the family member's WhatsApp account. They then pretend to be the family member. They contact the employee through the contact list. The employee trusts the message: it seems to come from the family member.

How a WhatsApp attack works

Note: This document does not provide full details of how to attack a WhatsApp account. We provide enough information to understand helpful protective steps.

Registering a device with a WhatsApp account uses an authentication code (a PIN code). The attacker tricks the victim into revealing the device registration code. They then deregister the victim's device from the WhatsApp account. Next, they register the attacker's device with the WhatsApp account.

The key point is the authentication code. It's very important to keep this secret, like a password.

Recovering and protecting your WhatsApp account

You can often recover a compromised WhatsApp account. A good way is to use your device telephone number. Use the app to ask for a 6-digit SMS verification code. When the code gets to your phone, enter it into the app. After re-authenticating your phone, the attacker is automatically disconnected. They cannot reconnect without a fresh authentication code.

While recovering an account, you might have to provide a two-step verification PIN. If you don't have this code, it suggests the attacker enabled two-step verification. Without the code, you must wait 7 days before you can sign in to WhatsApp. But the attacker is disconnected from the account immediately when the code is sent. Although you can't get into your account for a week, the attacker cannot get into your account at all.

When you reconnect into your WhatsApp account, check for any unknown devices. Do this by checking **Linked Devices** in the WhatsApp settings menu.

Always enable two-step verification on your account. Any future attempt to register a device needs a PIN to enable the app. Do this by going into the **Settings** then **Account** menu on the app. Select the **Two-step verification option**.

If there's something suspicious about your account, or the messages in the account, contact the . Ask for help as soon as possible.

Always follow policy about applications for official business or storing business-related information. Don't use unapproved applications for official business. Don't use unapproved applications for storing business-related data. Always use approved applications and storage tools.

WhatsApp account do's and dont's

Do ask for help if you think your WhatsApp account has been compromised.

Do enable two-step verification on your account. Do this by going into the **Settings** then **Account** menu on the app. Select the **Two-step verification option**.

Do tell everyone on your contact list if you think your WhatsApp account has been compromised.

Do check the list of linked devices at regular intervals. Look for unknown or unexpected devices. Do this by checking **Linked Devices** in the WhatsApp settings menu.

Do not share a WhatsApp one time passcode, password, or authentication code with anyone.

Do not use unapproved or unauthorised applications for work purposes.

Do not use personal accounts for work purposes.

Secure Data Transfer Guide

Introduction

This guide outlines the security procedures and advice for staff wanting to send or receive data securely from external sources.

This is important to the , because personal and sensitive data is regularly transmitted between departments. Legislation such as GDPR, and industry standards such as PCI DSS, affect the 's responsibility to secure this data. It is also important to recognise the damage that leaked sensitive data could cause to the vulnerable people the works to protect.

Who is this for?

This policy is aimed at three audiences:

1. **Technical users**: these are in-house Digital and Technology staff who are responsible for implementing controls during technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
2. **Service Providers**: defined as any other business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, storing data) for, or on behalf of, the .
3. **General users**: all other staff working for the .

The phrase "all users" refers to General users, Technical users, and Service Providers as defined previously.

Transfer Considerations

Anyone handling personal or sensitive data must seek consent from their line manager to authorise data transfer.

Before any data transfers are requested, consider the following:

- Is it strictly necessary for the effective running of the , and the care of the people it serves, that the data (regardless of whether the data is sensitive or not) is transferred?
- What is the nature of the information, its sensitivity, confidentiality, or possible value?
- What is the size of the data being transferred?
- What damage or distress might be caused to individuals as a result of any loss or unmanaged sharing during transfer?
- What implications would any loss or unmanaged sharing have for the ?
- What information is actually necessary for the identified purpose? For example, is the intention to send an entire document or spreadsheet, when only one section, or specific spreadsheet columns, are required?
- Has the identity and authorisation of the information recipient been established?

Any transfer technique used :

- Encrypt the data over the network (in transit), using sufficient and appropriate encryption (currently TLS 1.2 or greater).
- Require strong authentication to ensure that both the sender and recipient are who they claim to be.

These considerations apply when transmitting any data over a wireless communication network (for example wifi), or when the data will or might pass through an untrusted network.

If the is the controller of the data being transferred, the security storage requirements at the destination be considered to ensure that they comply fully with the relevant regulation, such as PCI DSS or GDPR.

If it's not clear who the data controller is, ask the for help.

When dealing with third parties, consider whether any data sharing agreements or contracts are in place that apply to the transfer of that data. Check whether there are any stipulations in place regarding the method of transfer that can or should be used.

If personal data is being transferred to a third party, then the privacy team be informed, to decide if a Data Protection Impact Assessment is required.

Data Transfer

Normally, files be transferred by email. Normally, files be transferred by secure network links using appropriate protocols such as `https`, `ssh`, or `sftp`. For large files, such as those over 5MB, transfer using a secure protocol is a practical necessity, as many recipients will not accept emails with attachments greater than 5MB.

Data Transfer by Secure link

The 's preferred method of data sharing is to use Microsoft Teams via Sharepoint. Teams has been authorised to hold information. It is configured to provide greater granular protection through tools such as Azure Information Protection (AIP). Where possible, data be transferred using Teams.

Due to the diverse nature of the 's architecture, using Teams might not always be possible. Those in the Digital and Technology team who do not have access to Microsoft Teams use to transfer data.

For more details on the actual process for a transfer, contact the .

Data Transfer by email

Where it is not possible to use Microsoft Teams or , **AND** the data to be transferred is less than 20MB, email be used, **BUT** the following requirements be met:

- Email communication be used to transfer unencrypted sensitive or personal data. Employees note that emails are not designed to attach and transfer large amounts of data. The 's email system does not support file attachments that exceed a total of 20MB.
- You consider an alternative secure method of transferring sensitive data wherever possible and practicable. If no suitable alternative is available, then apply an extra level of security. Do this by using encryption to apply a strong password to the sensitive data you wish to send. All passwords be transferred using an alternative method of communication to get to the recipient. Examples includes post, a telephone call to an agreed number, or by SMS text message.
- Email messages contain clear instructions of the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.
- Information sent , where practical, be enclosed in an encrypted attachment.
- Care be taken as to what information is placed in the subject line of the email, or in the accompanying message. Filenames or subject lines reveal the contents of attachments. Filenames or subject lines disclose any sensitive personal data.
- Emails only be sent from your work email address, as provided by the . This is to ensure that the correct privacy and security information is displayed.

CJSM email

- The Criminal Justice Secure email Service (CJSM) is provided for criminal justice agencies and practitioners to communicate with each other.
- As a general rule, it only be used for purposes relating to the criminal justice service.

Microsoft 365 Encrypted email

- This facility is available for standard individual and generic email accounts
- This method be used to send or receive files classified as . It is normally used with external partners, agencies, or individuals who cannot be contacted using CJSM email.
- The attached files on a single email exceed 25MB.

Removable storage devices

The strongly discourages the use of removable storage devices such as USB devices for data transfer. However, if all other options are not possible, then removable storage devices be used with caution.

Any data being transferred by removable media such as a USB memory stick be encrypted. Encrypted portable storage devices be password protected with a strong password. All passwords be transferred using an alternative

method of communication to get to the recipient. Examples includes post, a telephone call to an agreed number, or by SMS text message.

If you think you have no other option for copying or moving data, and have to use removable media, contact the .

Ownership of any removable media used be established. The removable media be returned to the owner on completion of the transfer. The transferred data be securely erased from the storage device after transfer.

Clear instructions of the recipient's responsibilities, and instructions on what to do if they are not the intended recipient, accompany the removable media.

Any accompanying message or filename reveal the contents of the encrypted file. The sender check, at an appropriate time, that the transfer has been successful, and obtain a receipt. An email confirming receipt is acceptable.

Report any issues to your line manager and in the case of missing or corrupt data to the immediately.

Data transfers by post or courier

Data transfers using physical media such as memory cards or USB devices only be sent using secure post. Royal Mail First or Second class be used. Royal Mail Special Delivery or Recorded Delivery be used. For non-Royal Mail services, a secure courier service be used, with a signature obtained upon delivery. The recipient be clearly stated on the parcel. The physical media be securely packaged so that it is not damaged in transit.

The recipient be told in advance that the data is being sent, so that they know when to expect the data. The recipient confirm safe receipt as soon as the data arrives. The sender responsible for sending the data is also responsible for confirming the data has arrived safely.

Hand Delivery and Collection

Hand delivery or collection of data be used where removable media is used. When arranging for an individual to collect information, the identity of the individual be established, to confirm who they claim to be. An appropriate form of identification be provided before handing over any documentation.

Telephone or Mobile Phone

Phone calls might be monitored, overheard, or intercepted. This might happen deliberately or accidentally. Take care to protect calls, as follows:

- Transferred information be kept to a minimum.
- Personal or Confidential information be transferred over the telephone, unless the identity and authorisation of the receiver has been appropriately confirmed.

Residual risks with encrypted data transfer

All users recognise that even if a system uses encrypted data transfer, there are still occasions where data might be affected by unauthorised access. Be aware of these residual risks. Line Managers include consideration of these risks in employee awareness training. Examples include:

- Some data relating to the communication might still be exposed in an unencrypted form. An example is metadata.
- Data transfer processes that rely on Public Key Infrastructure (PKI) implement strict certificate checking to maintain trust in end-points.

Secure Email Transfer Guide

This guide provides technical users with information about the services and encryption tools for transferring information securely using email. Ensure that email communication is sufficiently secured before transferring sensitive information. Examples of sensitive information include:

- classified information such as personal data.
- API and other application keys or credentials, including within containers.
- SSH keys.
- Database and other system-to-system passwords.
- Private certificates for secure communication, transmitting, or receiving data using protocols such as TLS or SSL.

- Private encryption keys.
- RSA and other single-use password information.

Related information

Email Security Guide on page 277

Transport Layer Security

Ensure that any service capable of sending and receiving email uses enforced TLS to encrypt messages:

- The always use the latest version of TLS.
- TLS always be used when sending to `gov.uk` domains.
- Any domains that do not support TLS be documented in an exceptions list, and an exception rule authorised by the DNS provider. Refer to the Email Authentication Guide for DNS provider contact details.
- Where mandatory TLS encryption is not suitable:
  - Use certificates from Certificate Authorities, making sure they are always valid and use strong encryption, algorithms, and key lengths.
  - Use Secure Multipurpose Internet Mail Extension (S/MIME), as it signs and encrypts email data before it is transmitted.
- If you operate an internet-facing email service, you buy and manage appropriate TLS certificates from the Digital Marketplace.

The Information Classification Handling and Security Guide offers further advice on encrypting email communications. This includes protecting data at rest, and data in transit.

For further guidance on TLS, refer to the Cryptography guidance.

End-to-end encryption

End-to-end email encryption ensures that only the sender and intended receiver can read email messages. Data is encrypted on the sender's system. Only the intended recipient is able to decrypt and read it. Many but not all email tools support end-to-end encryption for email communications. You might need to implement transit encryption for your users with a third party app that provides end-to-end encryption. Contact the for advice.

Secure email transfer options

Select the most suitable system for service users, and configure it appropriately. This section provides guidance on the various options available.

Note: Remember that only email systems may be used for business purposes. Personal email accounts be used for business purposes.

Secure Messaging Options	Examples
Cloud Email Solutions (securing to the Government Secure Standard)	Microsoft Office 365 (`@justice.gov.uk`) or (`@digital.justice.gov.uk`)
Supplementary Email Solutions	CJSM

Cloud email solutions

These are tools that are configured to the Government secure standard. When evaluating a tool, ensure that it provides assurance of compliance to the Government standard, and provides confidence for the secure exchange of information.

Google mail

Google mail is part of the service. It uses Transport Layer Security (TLS) to encrypt incoming and outgoing emails automatically. However, the email providers of both the sender and the recipient must always use TLS, otherwise the email transfer cannot be assured as secure. If required, S/MIME encryption might be suitable. To get help with this, contact the .

Office 365

By default, all emails in Office 365 are sent using Opportunistic TLS. If a TLS connection cannot be established, the message is sent in plain text using Simple Mail Transfer Protocol (SMTP). If TLS must be applied, contact the for help. In this configuration, certificate verification is required whenever mail is sent from a third party to the .

Outlook supports two other encryption options:

- S/MIME encryption: to use S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard. Outlook supports the S/MIME standard.
- Office 365 Message Encryption (Information Rights Management): to use Office 365 Message Encryption, the sender must have Office 365 Message Encryption configured.

Microsoft currently provides additional tools to secure information via email.

If either of these additional encryption methods is required, please contact the .

Criminal Justice Secure Mail

Criminal Justice Secure Mail (CJSM) provides a closed email service between Criminal Justice Agencies (CJAs), and Criminal Justice Practitioners (CJPs). CJSM be used from public or personal computers. CJSM be used only for legitimate business purposes relating to the Criminal Justice System.

Examples of CJAs within the GSC are:

- Police
- Prison Service
- Court Service
- CPS
- Probation

Examples of agencies or CJPs outside the GSC are:

- Youth Offending Teams
- Victim Support
- Solicitors and Barristers.

The CJSM offers two mechanisms for connection:

- A CJSM mailbox (webmail) hosts a mailbox on behalf of the user. A user accesses the mailbox using either a standard internet browser, or a POP3 email client.
- A CJSM server connection (SMTP) is deployed to act as an encryption proxy for any email traffic containing a destination address ending in `cjsm.net`. All CJSM servers require a certificate to be installed. The certificate is issued by Egress. Session keys are established for each transaction.

All users can send or receive over CJSM by adding `.CJSM.net` to the end of their email address.

CJSM only be used to share information up to and including .

CJSM be used with multi-client mail relay services such as Mailgun, Mailchimp, or AWS SES.

For further guidance contact the . Alternatively, further information is available at: https://www.cjsm.justice.gov.uk/training/index.html.

External emails

Ensure that all outgoing emails are automatically appended with a disclaimer.

If you are exchanging email with an outside organisation with which the could be bound contractually, the following text must be appended:

> I am not authorised to bind the Ministry of Justice contractually, nor to make representations or other statements which may bind the Ministry of Justice in any way via electronic means.

Auto-forward

Ensure that auto-forwarding is used responsibly, and in line with the 's Information Classification Handling and Security Guide. In particular:

- Disable auto-forward to external domains. If auto-forwarding to an external domain is required, it be controlled by creating custom Role Based Access Control (RBAC) roles.
- Advise users to only forward emails from an email address to an email address that provides the same or higher security standards.
- Do not provide auto-forward capability when any standard, policy, or guidance states that additional controls or protection be implemented before sending an email.

Sending information securely

This guidance complements the overall security policy.

This guidance on working securely with paper documents and files applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, occupied premises.

Agencies and arm's length bodies (ALBs) are expected to comply with this corporate framework but may establish their own arrangements tailored to operational needs and should supplement it with local policy or guidance for any business-specific risk.

Related information

IT Security Policy (Overview) on page 22

Objective

The requires employees and contractors to get into the habit of looking after the information that they work with, whether it's on paper or stored electronically, in the same way they would take care of their personal valuables.

Scope and Definition

This guidance helps you understand the risks involved in sending information. It covers any information that relates to the business of the , its stakeholders and partners that have been printed out or written down on paper, and information that has been downloaded from IT systems onto 'removable media'.

This guidance outlines the all the basic guidance on sending information using email, post, courier services and fax.

Context

All information is valuable, and staff are expected to protect everything that relates to the department's business, including information provided by others. This applies to all information, not just information that is covered by the Data Protection Act or classified under the Government Classification Scheme.

There are different rules for managing and protecting different kinds of paper-based information. You need to know how to:

- Identify the correct security level for the information you work with.
- Handle it according to the relevant rules.

Responsibilities

All employees, contractors, partners, service providers and employees of other organisations who are on premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues and the protection of departmental assets.

Policy statements

Using email

Email is the preferred option for securely transferring information between yourself and another civil servant. You use departmental equipment and transfer between or CJSM email accounts.

If the person or organisation you are sending the information to is outside departmental or CJSM networks, you consider the sensitivity of the information. It might be safer to send it on encrypted removable media or in hardcopy.

Sending bulk information

Transferring bulk data be authorised by a senior manager.

The definition of bulk or high volume is not specific. Removable media such as laptops, disks or memory sticks can hold thousands of records. They have the benefit of encryption to prevent access to data accessed, but the damage if they are lost and the information cannot be retrieved remains high. However, information is immediately accessible if even a single paper files is lost, so the risks need to be managed differently.

As an indication, datasets containing the electronic records of 1,000 or more people would count as bulk, whilst decisions on using more secure forms of movement might apply to much smaller volumes of case files. It might also apply to lesser volumes where names and addresses are combined with sensitive information that might lead to identification.

In all cases, consideration be given to the risk and impact of causing individuals or the to suffer harm or loss, service disruption, or reputational damage.

Using post and couriers

There are a range of methods of sending documents, depending on the potential harm that result from loss. This relates to their security classification and the volumes involved. Use a method that is appropriate for the type of information:

- For normal inter-office transit, use DX delivery services or agreed contracts for the movement of papers or files. Royal Mail letter post is otherwise acceptable for standard non-sensitive material, or letters at .
- The classification and any handling caveat such as be shown on the outer envelope. If the contents are sensitive, particularly if they contain personal details intended for an individual, the envelope be marked `ADDRESSEE ONLY`. Post rooms check addressee details, and open any envelope marked in this way.
- If more security is needed, either because material is being sent in bulk or the contents are more sensitive, tracked options including tracked DX or special delivery be used.
- Material marked be sent using any of the previous methods, with a return address and no protection marking on the outer envelope.
- Double enveloping might also provide additional protection, especially if there is a risk the package might burst or if it is being sent to a non- location where the `ADDRESSEE ONLY` instruction might not be recognised.

Confirming delivery

If you are sending sensitive or bulk information, you ensure that the recipient is expecting it and get confirmation of receipt. Consider a solution that allows you to track delivery. If you need to transfer or send personal data to or outside of the European area, discuss it first with the .

Faxing documents between sites

Office faxes only be used for transmission and exchange of information where other more secure means of communication, for example government email, are not possible.

Where use of fax machines (including Goldfax where available) remains the best option, it only be for information classified at and that is not especially sensitive. The reason is that fax material is sent over public networks. Faxed information might be individual items, including personal data.

Bulk transmission of personal data and information marked only be allowed following a risk assessment and approval from the Information Asset Owner.

The following controls and procedures also be applied by staff:

- Ensure that the recipient has a legitimate need to access department information for official business purposes.
- Take care to ensure that the correct number has been dialled, and that the authorised recipient is attending the receiving fax terminal at the time the information is being faxed.
- Immediately contact the authorised recipient to authenticate that they have received the information, verifying the quantity (the number of pages), and content of the information.

- If the recipient's fax line is busy and a transmission is not possible, wait until it is free. Do not leave the fax machine unattended. You confirm that the authorised recipient has received all the information.
- Each transmission should carry the following:
  - A unique reference number.
  - The identity of the originator.
  - The identity of the intended recipient.
  - A record of the number of pages transmitted.
- Ensure that the authorised recipient is aware of the handling requirements for information, including preventing information being viewed or accessed by unauthorised persons in their business.
- If the fax is configured to produce a confirmation of transmission report, including a copy of the first page of the transmission, ensure that you retain this hardcopy information and that it is not left on the fax machine where it might be seen by those who do not 'need to know'.
- Ensure that the fax is configured correctly, and that functions such as polling reception (programming to send messages to specific numbers), redirection, forwarding, and remote control are disabled.

Overview of threats and vulnerabilities

The public service telephone networks through which fax messages are transmitted are exposed to several significant security vulnerabilities and threats. These include:

- The potential that even UK to UK transmission is routed to overseas networks, increasing risks.
- Transmission within the UK may be intercepted at several places along the route.

In addition, the risks associated with fax machines are as follows:

- Unauthorised access to the built-in message stores to retrieve messages.
- Deliberate or accidental programming of machines to send messages to specific numbers.
- Sending documents and messages to the wrong number, either by misdialling, or by using the wrong stored message.
- Viewing of protectively marked messages by unauthorised persons, for example copies left unattended and unsecured on fax machines and traffic logs, and copies of fax messages retained on the machine's memory being accessed.

What to do if you think there has been a security breach

If you suspect that the security of the information you work with has been compromised in any way, you report it immediately. A security breach doesn't have to involve the actual loss of information. The potential loss of information also counts.

For example, if a security cabinet has been left unsecured, there might be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

The level of risk and potential impact to assets and most importantly physical harm to our people and the public determines the controls to be applied and the degree of assurance required. The ensure that a baseline of physical security measures are in place at each site, and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, for example in response to a security incident or a change in the Government Response Level.

The implementation of all security measures be able to provide evidence that the selection was made in accordance with the appropriate information security standards ISO27001/27002, and with Physical Security advice taken from the and (link is external).

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards are subject to annual review or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting .

Annex A: Suitable carriers

This guidance does not provide an exhaustive list of suitable carriers but does identify recommended options. The following notes provide further details.

Royal Mail

Ordinary letter post is acceptable for correspondence with members of the public or items that must be sent to private addresses. To prevent inappropriate opening of personal letters with sensitive personal data sent internally or to other business addresses, you mark the envelope 'addressee only'. This might also require double enveloping to protect the contents in transit, and prevent inappropriate opening on delivery.

Recorded delivery

Recorded delivery be used if the letter contains particularly sensitive information or identity documentation. The sender is given a reference and can confirm delivery and obtain a copy of the signature through the Royal Mail website.

Special delivery

This is similar to recorded delivery, but requires a named signature for receipt. Earlier delivery can be arranged (9am or 1pm). This service also allows online tracking of the item, suitable for more sensitive documents.

For more information, refer to the "Courier and postal services Royal Mail" document available on MyHub (log in to MyHub and use the search facility to locate the document).

DX

Ordinary DX services are acceptable for sending low volumes of files or enveloped papers between sites and other justice agency partners with registered DX addresses. When sending any volume or sensitive papers, managers ensure that the receiving office is expecting the delivery, and check receipt.

Tracked DX

This is recommended when a more formal tracking is required, either because of the volumes of files, or because they contain particularly sensitive case information.

There two further DX options which give added security:

- Courier Tracked.
- Secure DX.

For more information, refer to the "Courier Services Document Exchange and Next Day – DX Network Services" document available on MyHub (log in to MyHub and use the search facility to locate the document).

You can also use tracked courier services provided by FedEx.

Spam and Phishing Guide

This guide outlines the technical implementations that technical users should make to keep systems secure.

Related information

Email Security Guide on page 277

Common email threats

Spam and phishing

To protect against spam and phishing attacks, the makes use of Government services such as National Cyber Security Centre's Suspicious Email Reporting Service and any other services that are appropriate.

Spoofing attacks

To mitigate spoofing attacks, use techniques such as:

- Implementing Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC). Any sender information details such as `from`,

`reply-to`, `return-path`, or even `x-origin` can be spoofed. For further guidance refer to the Email Authentication Guide.

- Using secure email gateways.
- Implementing access controls, such as Multi-Factor Authentication (MFA), to avoid an attacker gaining access to credentials for an email account where they could plausibly spoof the sender's email address.

Protecting a parked domain

DMARC also be implemented on non-email sending domains. This is because the domains might be used for email spoofing and phishing.

Once parked domains are protected, configure them to renew automatically by default.

If you are a domain owner, to protect a parked domain follow these steps:

1. Create an SPF record with no permitted senders. This means that no IP address is authorised to send email for the parked domain.
2. Include an `RUA` address. Aggregate reports can be sent to this address. The reports provide visibility of potential abuse.
3. If you have an `A` record on your domain, but no `MX` records, create a "null" `MX` record that immediately fails any email to the parked domain. Give the `MX` record the highest priority (`0`).

A "null" DKIM record is not required. This is because email will be treated the same as if it had no record at all. However, recipients might treat a "null" DKIM record with extra caution, as it explicitly revokes any keys that might be cached.

Some interfaces might not allow you to implement all these steps. Implement as many as possible.

Compromised email systems

Compromised email systems are often used to send spam messages and conduct phishing campaigns. Protect email systems by using MFA where possible, to mitigate the risk.

Report any account takeovers or email compromise as an incident.

Accidental disclosure

Not all security threats are intentional. Authorised users might accidentally send proprietary information to unintended recipients using email. Report these as an incident.

Man-in-the-Middle attacks

Man-in-the-Middle (MITM) attacks might result in unauthorised access to email whilst the message is in transit. These attacks are used to gain access to sensitive information.

Mitigate MITM attacks by:

- Configuring Secure Multipurpose Internet Mail Extension (S/MIME) to encrypt emails and provide unique digital certificates.
- Implementing certificate based authentication for all end user machines and devices, for example printers with email services enabled.
- Using TLS certificates which use the HTTPS protocol to provide a secure connection between the and third parties when using webmail portals.
- Using SMTPS (SMTP encrypted with TLS) rather than unencrypted SMTP.

Mail Check

Mail Check is an NCSC cyber defence service. It enables email administrators to improve and maintain the security of email domains by preventing spoofing attacks. All domains operated by, or on behalf of, the , be added to Mail Check, regardless of whether the domain is expected to send or receive emails. All future contracts and agreements with third party suppliers make this a requirement.

Mail Check be used only if the email domain name provided is publicly routable from the Internet using the Simple Mail Transfer Protocol (SMTP).

To add domains to the 's Mail Check service subscription, contact the NCSC Mail Check team via .

Email sandboxing

Sandboxing provides an additional layer of protection. Any email that contains URLs, attachments, or suspicious senders can be securely checked for malicious content before they reach the network or mail server. If the email is found to be harmful, it is not sent further. Sandboxing is beneficial, because it:

- Mirrors the end user's computer, and provides a secure space to interact with and analyse potentially harmful communications.
- Allows developers and technical architects to be proactive in minimising the effect of a threat.

For further guidance on implementing sandboxing, including which products you might use, contact the .

URL link rewriting

URL link rewriting is a technique used to detect malicious links in emails. Links in emails are actively scanned. They are then rewritten to point to an Advanced Threat Protection gateway, where two checks occur:

1. Determine if the link is deny-listed by the or has been previously identified as malicious.
2. Scan downloadable content available at the link address.

After the checks have completed, the user continues to the URL or is blocked from access, depending on the results of the checks. If access is blocked, URL rewriting is used to provide an explanation and contact details for additional help.

Protecting against email security threats

To provide protection against email security threats, implement the following controls:

- Implement anti-malware software. Refer to the Malware Protection Guidance for more information.
- Install only the minimal mail server services required. Eliminate known vulnerabilities through patches, configuration, and upgrades. Refer to the Vulnerability Scanning and Patch Management Guide for more information.
- Implement external email warning messages to insert text (usually in the subject line) into an email when it is identified as coming from outside of the .
- Develop email security management plans to define best practices for employees.
- Use SMTP alert policies to track malware activity and data loss incidents from anti-malware software.
- Ensure there is no unnecessary detail on the website or webmail, by considering what visitors need to know with the aim of reducing the threat of spear phishing.
- Restrict auto-forwarding. Refer to the Secure Email Transfer Guide for more information.
- Restrict delegate access. Refer to the Email Security Guide for more information.

The Email Authentication Guide provides further detail on the email authentication controls mentioned in this guide.

Reporting spam or malicious emails

If you think your email service provision has been susceptible to spam or a virus, report it immediately to the on as an IT security incident. Please refer to the IT Security Incident Management Policy for further guidance.

Web Browsing

The provides access to the Intranet and Internet for business use. The access helps you to do your job effectively and efficiently.

security policies governs your use of these facilities.

Reasonable personal use is allowed, if:

- Your line manager agrees.

- It does not interfere with the performance of your duties.

You and your manager are responsible for ensuring that you use these systems responsibly.

If you connect to a website that contains unsuitable, illegal or offensive material:

- Disconnect from the site immediately.
- Inform your #unique_1265.

The Department monitors the use of electronic communications and web-browsing activity. If your email use or web browsing seems unacceptable, your manager can request detailed activity reports.

What websites you can access

The 's approach to website access is continually reviewed and updated. By default, we try to allow access to as much as possible of the internet for all users. Inevitably, there are some restrictions, for the following reasons:

Cyber Security

- The site is an unacceptable security risk for systems or users. For example, sites known to host malware are blocked.

Technical

- The site causes technical issues which interfere with business activities. For example, a video site uses too much network capacity.

Business Policy

- Only a specific individual or group of users can access the site. For example, social media sites are blocked for systems or users in frontline roles.

The list of websites included in each of the categories is as small as possible. But if you cannot access a site that you think should be OK, you can request a review. Similarly, if you can access a site that you think should be blocked, request a review.

The access rules that apply are described in detail here.

What to do if you are blocked from a website that you think should be OK

Log an incident with your #unique_1265.

Provide the following details:

- The address of the website.
- The time you visited the site.
- The details of any block message that you received.

The will investigate the reason why you cannot access the website.

If there was a system error or fault, remedial action will restore access.

If the block is due to an access rule, the Security team reviews whether to change the rule.

What to do if you are able to access a website that you think should be blocked

Log an incident with your #unique_1265.

Provide the following details:

- The address of the website.
- The time you visited the site.
- The reason why you think the site should be blocked.

Other help

- HMPPS Prison - All requests should be directed to the via a local or area IT Manager.

- HMPPS Probation - Log an incident with your #unique_1265.
- All other teams, contact the .

Web browsing security policy profiles

There are two policy profiles, one for the Judiciary, and one for all other staff.

Each profile identifies categories of content that are normally blocked. Content that is not in a blocked category will normally be available to a profile.

Judiciary

All activity is logged. By default, no reporting takes place. However, reporting is permitted following appropriate judicial sanction.

The following categories of content are normally blocked for the Judicial profile:

- Advanced Malware Command and Control
- Advanced Malware Payloads
- Botnets
- Compromised Websites
- Custom-Encrypted Uploads
- Dynamic DNS
- Elevated Exposure
- Emerging Exploits
- Extended Protection
- Files Containing Passwords
- Keyloggers
- Malicious Embedded iFrame
- Malicious Embedded Link
- Malicious Websites
- Mobile Malware
- Newly Registered Websites
- Phishing and Other Frauds
- Potentially Exploited Documents
- Potentially Unwanted Software
- Security
- Sex
- Spyware
- Suspicious Content
- Suspicious Embedded Link
- Unauthorised Mobile Marketplaces
- User-Defined list

All other staff

Limited restrictions are in place to block web access. All activity is logged. Reporting is enabled for all activity.

The following categories of content are blocked for this profile:

- Adult Content
- Adult Material
- Advanced Malware Command and Control
- Advanced Malware Payloads
- Application and Software Download
- Botnets
- Compromised Websites

- Custom-Encrypted Uploads
- Dynamic DNS
- Elevated Exposure
- Emerging Exploits
- Extended Protection
- Files Containing Passwords
- Keyloggers
- Malicious Embedded iFrame
- Malicious Embedded Link
- Malicious Websites
- Mobile Malware
- Newly Registered Websites
- Phishing and Other Frauds
- Potentially Exploited Documents
- Potentially Unwanted Software
- Security
- Sex
- Spyware
- Suspicious Content
- Suspicious Embedded Link
- Unauthorised Mobile Marketplaces
- User-Defined list

Wifi security policy

Introduction

This policy gives an overview of wireless networking (wifi) security principles and responsibilities within the .

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.WIFI.xxx**, where **xxx** is a unique ID number.

Audience

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Any other business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services, including processing, transmitting,and storing data for, or on behalf of, the .
General users	All other staff working for the .

"All users" refers to General users, Technical users, and Service Providers, as defined previously.

Purpose

The purpose of this document is to define a set of security requirements for wifi networks, based on industry good practices and our local requirements.

POL.WIFI.001: Any exceptions to the policy be managed through the 's security risk management process.

Applicability

This policy applies to all owned or managed wifi networks provided for any purpose. It also applies to the use of third-party wifi networks by devices which handle information, for example staff end user computing devices.

wifi networks

POL.WIFI.002: Each wifi network have a defined policy which is reviewed at least annually, that describes:

- The purpose of the wifi network.
- The intended users of the wifi network.
- The Service Owner of the wifi network.
- The access controls that are applied to ensure that only those intended users can connect to the wifi network.
- User and administrator responsibilities for maintaining the security of the wifi network.
- Who has authority to expand or alter the wifi network.
- Logging and monitoring requirements and responsibilities for the wifi network.

General security requirements

The following statements apply to all -provided wifi networks.

POL.WIFI.003: Wifi networks be treated as extensions of trusted LANs or WANs.

POL.WIFI.004: Wifi networks be treated as untrusted bearers for the purposes of application security.

POL.WIFI.005: All products used in an wifi network support WPA2-Enterprise.

POL.WIFI.006: CCMP be used to protect the confidentiality and integrity of information transmitted over the wifi network.

POL.WIFI.007: Other wifi security modes (such as WEP) be enabled.

POL.WIFI.008: All products used in wifi networks support certificate-based authentication.

POL.WIFI.009: On wireless networks, isolation between wifi clients be enabled. Where there is no requirement for devices to communicate directly, isolation be enabled.

POL.WIFI.010: wireless networks use a DNS resolver that chains to the Protective Domain Name Service (PDNS) service.

POL.WIFI.011: All wireless networking equipment be kept patched and secure, whether connecting to wifi services or GovWifi.

POL.WIFI.012: All management of Wireless networking equipment be undertaken in compliance with the Privileged User Access Guide and any relevant Security Operating Procedures (SyOPS).

enterprise wifi networks

Note: enterprise wifi networks are those used solely for users and devices.

POL.WIFI.013: Pre-Shared Keys (PSKs) be used for user or device authentication.

POL.WIFI.014: PSKs be unique per user or device.

POL.WIFI.015: PSKs only be implemented with prior agreement from the cyber security team

POL.WIFI.016: PSKs be changed at least once a year.

POL.WIFI.017: EAP-PSK be used.

POL.WIFI.018: In higher-threat situations such as in a prison location where any unauthorised use of the Wireless network would constitute a security incident, mutually-authenticated authentication based on certificates be used.

POL.WIFI.019: EAP-TLS or EAP-TTLS be used.

POL.WIFI.020: Where user or device groups have differing functions, PKI trust domains be defined and used to maintain functional separation.

special-purpose wifi networks

POL.WIFI.021: If devices, including IoT or legacy devices, cannot meet the general security policy requirements, or if there are non-security reasons for segregating traffic onto different SSIDs, then dedicated wifi networks be created.

POL.WIFI.022: These dedicated networks have reduced authentication controls, for example a shared PSK or a reduced ability to rotate PSKs due to form-factor limitations.

POL.WIFI.023: In such circumstances, special care be taken to ensure that the general network architecture and other security controls constrain network connectivity for clients. The constraints limit network connectivity to the minimum required for them to function properly.

POL.WIFI.024: Other mechanisms such as MAC filtering be used to reduce the chance of misuse.

guest wifi networks

Due to complexities and management effort involved in running wifi solutions, the preference is to utilise the cross-Government GovWifi service: https://www.wifi.service.gov.uk/.

This also has the benefit of being available across HMG Departments and Agencies. GovWifi has a level of pre-registration, monitoring and filtering in place to protect the users. However, GovWifi does not provide enterprise level security functions. GovWifi users are required to maintain their own security controls. For users of GovWifi connections, this means using the -provided VPN services when accessing protected services.

POL.WIFI.025: Any considerations for not using GovWifi in an guest wifi network be discussed and agreed beforehand with the cyber security team.

POL.WIFI.026: Where GovWifi cannot be used, or where an existing guest wifi service exists,the following be in place:

- Regular rotation of the passphrase, with agreement from the . Normally, this requires a fresh and unique passphrase each day.
- Filtering and Monitoring for known 'bad-sites' and threats be in place at the network level.
- Guests wishing to utilise the service first register for access, and can then be provided with the passphrase for that day.

Logging and monitoring

POL.WIFI.027: Security monitoring for wireless networks be implemented, in accordance with the security monitoring policy.

POL.WIFI.028: Security logging be enabled to record activity such as client access events, authentication successes and failures, client association history, and relevant information about devices and users attempting to connect to the wireless network.

POL.WIFI.029: In higher threat environments, security logging also include identification of rogue access points, and logging of all attempted associations with the wifi network.

POL.WIFI.030: For guest wifi networks, but not including GovWifi, audit logs of sites accessed be retained for at least 6 months, including authentication details. This data is held to allow forensic analysis of data in the case of a security incident. No personal information except that required to conduct the analysis is logged or retained.

Using third-party wifi

POL.WIFI.031: staff ensure they have permission from the network owner before using wifi that is not operated by the .

POL.WIFI.032: Staff take reasonable precautions to check that their home wifi network is secure.

POL.WIFI.033: Staff use work-provided mobile phones to 'tether' their -provided devices for connectivity.

POL.WIFI.034: Tethered connections be password protected using unique and complex passwords.

POL.WIFI.035: Tethering passwords for devices be shared with non- users.

POL.WIFI.036: Public wifi networks or guest wifi provided at third-party sites only be used by devices which have suitable encryption for information. Here, 'suitable' means either an 'always-on full-take' VPN, or that provides appropriate application-level encryption for all services. This is currently (October 2021) limited to Dom1 and PTTP/MoJO laptops and mobile devices.

POL.WIFI.037: Staff travelling overseas follow the guidance on accessing IT systems from overseas regarding the use of wifi or other networks.

Enforcement

This policy is enforced by lower level policies, standards, procedures, and guidance.

Non-conformance with this policy could result in disciplinary action taken in accordance with the 's disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the department always cooperates with the relevant authorities, and provides appropriate evidence.

System acquisition, development and maintenance

Security requirements of information systems

Technical Security Controls Guide

Introduction

This guide explains the technical security controls that should be implemented on information systems developed, procured or operated by the or on its behalf. This guide aligns with NIST 800-53 and the NCSC Cyber Assessment Framework (CAF). The guidance provides the with 3 phases or layers of defence. These controls must be implemented to ensure the 's network infrastructure is secure.

Who is this guide for?

This guide has two audiences:

1. The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
2. Any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the MoJ.

What is an 'system'?

Within this guide, a system includes:

- Hardware - laptops, desktop PCs, servers, mobile devices, network devices, and any other IT equipment.
- Software - such as operating system (OS) and applications (both web-based and locally installed).
- Services - such as remote databases or cloud-based tools like Slack.

Related guides

Defensive Layer 1: Creating a baseline security environment Layer 1 sets out the technical controls required to build strong network foundations, including secure configuration and software development.

Defensive Layer 2: Implementing monitoring capabilities Layer 2 builds a monitoring capability for the network and extends existing security controls to mobile devices.

Technical Security Controls Guide: Defensive Layer 1
Defensive layer 1: Creating a baseline security environment

DO

The following security controls should be implemented to create a baseline security environment.

✓ Enforce access control through using Multi-Factor Authentication (MFA), security attributes and enforcing the 'need to know' principle. Dual authorisation must also be used to conduct sensitive system changes. For more information, refer to the Access Control guide.

✓ Implement host-based protection such as host firewalls and host based intrusion detection.

✓ Restrict the use of remote access connections, using the following controls:

- The monitoring and control of remote access methods.
- Ensuring all remote access methods are encrypted.
- Enabling the capability to rapidly disconnect a user from accessing an information system, and/or revoking further remote access.

✓ Implement the following access control and security measures to protect wired and wireless networks:

- Restrict a user's ability to change wired and wireless configurations.
- Use strong encryption and authentication on both wired and wireless networks.
- Carry out regular audits of routers and wireless access points looking for unauthorised units.

✓ Synchronise timestamps with a primary and secondary authoritative time sources.

✓ Classify system connections, and apply restrictions to external systems and public networks.

✓ Test backup solutions at least every three months, to ensure data reliability and integrity.

✓ Use deny-listing/allow-listing tools for current and newly developed software.

✓ Enforce session lock controls with pattern-hiding displays.

✓ Use encryption to protect information. Encryption mechanisms should include:

- Secure key management and storage.
- PKI certificates and hardware tokens.

✓ Ensure that system component inventories:

- Are updated as part of installation or removal tasks.
- Have automated location tracking where possible.
- Have clear and unambiguous assignment of components to systems.
- Do not have component duplication.

✓ To protect the network against malicious actors and code, implement the following security controls:

- Vulnerability scanning tools.
- Intrusion detection systems.
- Signature and non-signature based detection of malicious code or behaviour.
- Software patching and updates.
- Detection of unauthorised commands.
- Tools for real-time analysis of logs.
- Detection of indicators of compromise.

✓ When connecting to external networks and systems, ensure those network and systems provide secure connection, processing, storage, service controls and physical locations.

✓ Make provision for exceptional (excess) capacity or bandwidth demands, exceeding what is required for 'typical' business as usual operations, and implement monitoring and detection tools for denial of service attempts.

✓ Where possible, ensure a redundant secondary system or other resilience controls are in place, using alternative security mechanisms and communication protocols.

DO NOT

The following list identifies what should not be done, and what activities should be limited, to improve baseline security controls.

✖ Allow systems to release information from secure environments unless all the following security controls are implemented on the destination system:

- Boundary security filters.
- Domain authentication.
- Logical separation of information flows.
- Security attribute binding.
- Detection of unsanctioned information.
- Restriction of suspicious inbound and outbound traffic.

✖ Allow general users to make unauthorised configuration changes to the security settings of software, firmware or hardware. Any exceptions, such as software updates, must be risk assessed and approved by IT and the Risk Advisory Team.

✖ Allow users to install software. Instead, software installations should be approved first, and only users with privileged access should be permitted to conduct the installation.

✖ Allow split tunnelling without careful consideration of how traffic will remain protected.

✖ Allow inbound traffic from unauthenticated or unauthorised networks.

✖ Allow discovery of system components or devices on the network.

✖ Enable boundary protection settings that permit different security domains to connect through the same subnet.

Defensive layer 1: Creating a baseline security software development and system configuration

DO

The following list describes what should be in place to create secure software development and configuration environments within the .

✓ If you are developing or maintaining systems or applications, use a development lifecycle and associated tooling which enforces security by design. Examples include:

- Code analysis and testing.
- Mapping integrity for version control.
- Trust distribution.
- Software, firmware, and hardware integrity verification.

✓ Use baseline configuration templates for critical and non-critical assets. These need to include:

- Automation support for accuracy and currency, such as hardware and software inventory tools and network management tools.
- Retention of previous configurations.
- Separate development and test environments.
- Cryptography management.
- Unauthorised change detection

✓ Enforce binary or machine executable code are provided under warranty or with source code, and implement time limits for process execution.

✓ Verify the boot process, and ensure the protection of boot hardware.

✓ Implement low module coupling for software engineering.

✓ Enforce application partitioning.

✓ Take a 'deny by default' approach to boundary protection for both outbound as well as inbound. Example controls include:

- Automated enforcement of protocol formats.
- Separate subnets for connecting to different security domains.

✓ Enforce protocol formats.

DO NOT

The following list outlines the actions that should not be undertaken in relation to software development and secure configuration.

✖ Allow access privileges for library or production/operation environments for unauthorised users.

✖ Configuration changes or applications to go live without testing them in a non-live environment.

✖ Use live data, including personal data, in system or application testing. Exceptions must be approved by the relevant SIRO and, if the live data contains personal data, the Data Protection Officer.

✖ Install or execute off-the-shelf software without ensuring appropriate support and security arrangements and agreements are in place.

Technical Security Controls Guide: Defensive Layer 2
Defensive layer 2: Implementing monitoring capabilities

DO

The following list identifies the security controls that should be implemented to mature existing Layer 1 controls and enable active monitoring of the network.

✓ Monitor login attempts and block access after 10 unsuccessful attempts.

✓ Implement session timeouts and block accounts after a defined period of inactivity, for example, 5 minutes.

✓ Implement a mobile device management solution to enable the wiping of mobile devices where access to the device has been lost or unauthorised access identified, for example, in the event of:

- An identified data breach.
- An identified policy breach such as jailbreaking a device.
- A lost device.
- The end of an employment contract, for example, for an employee or contractor.

✓ Use tools such as Elastic for easy storage, search and retrieval of information from logs, such as security, system or application logs collected from end points. Where artificial intelligence tools for searching these logs are available implement their use, an example might be AWS' Macie.

✓ Terminate network connections associated with communication sessions. For example the de-allocation of:

- Associated TCP/IP address pairs at the operating system level.
- Network assignments at the application level if multiple application sessions are using a single, operating system level network connection.

✓ Implement maintenance tools. For example:

- Hardware/software diagnostic test equipment.
- Hardware/software packet sniffers.
- Software tools to discover improper or unauthorised tool modification.

✓ Use monitoring systems to generate alerts and discuss options with the .

✓ Have the capability to respond to alerts generated by the monitoring system or by users and discuss options with the .

✓ Control the development and use of mobile code, whether developed in-house, third party or obtained through acquisitions, by following a formalised development and onboarding process, refer to the Data Security and Privacy Lifecycle guide.

✓ Implement concurrent session control which is defined by:

- Account type, for example privileged and non-privileged users, domains, or applications.
- Account role, for example system admins, or critical domains or applications.
- A combination of both account type and account role.

✓ Implement spam protection tools, which have the capability to:

- Monitor system entry and exit points such as mail servers, web servers, proxy servers, workstations and mobile devices.
- Incorporate signature-based detection.
- Implement filters for continuous learning.

✓ Use error handling techniques, such as pop-up messages, which provide information necessary for corrective actions without revealing data that can be exploited by threat actors.

DO NOT

The following list describes what actions should **not** be undertaken when implementing Layer 2 security controls.

✖ Allow connections between internal and external systems without carrying out security checks.

✖ Allow the use of unauthorised software. Software must be approved by the . Contact the Security team for advice at .

✖ Allow general users to execute code on their mobile devices. Your devices should be able to:

- Identify malicious code.
- Prevent downloading and execution.
- Prevent automatic execution.
- Allow execution only in secured and segregated environments.

✖ Display internal error messages such as stack traces, database dumps, and error codes to users outside of the -defined personnel and roles.

✖ Allow unauthorised removal of maintenance equipment, for example, backup disks and power supplies.

✖ Decommission maintenance equipment without appropriate security controls, for example:

- Verifying that there is no organisational information contained on the equipment.
- Sanitising the equipment.
- Retaining the equipment within the facility.

Security in development and support processes

Maintained by Default

We believe that technology should be Maintained by Default, particularly in relation to security.

h/t https://www.ncsc.gov.uk/articles/secure-default

Good technical maintenance is security maintenance

Technical maintenance isn't just about patching or upgrades (but they often play a large and important part of maintenance) but more of refreshing designs, methods and approaches to leverage new technologies to increase quality, speed and performance and reducing costs.

Good technical maintenance (including patching and upgrades) includes security benefits whether that is patching a known security issue through to implementing newer cryptography methods that both benefit security but also reduce computational effort or enhance user privacy.

Good technical maintenance (just like other release or change paths) should include an appropriate amount of testing (outside of production) to understand any negative consequences of changes.

Commodity technical maintenance

The expect technology systems to be maintained to ensure the commodity functional elements do not become end of life, or cease function as a result.

Examples include:

- [automated] certificate renewals
- upgrading of hashing methods to implement new standards once they become commonly accepted best practices
- upgrading from SSL v3 to TLS, and from TLS1.[0/1] to TLS1.2, ultimately into TLS1.3 (and beyond)

Secure by Default

We believe that technology should be Secure by Default. This means embedding security from inception, so that it is intrinsic and as transparent as possible.

h/t https://www.ncsc.gov.uk/articles/secure-default

Good technical design is security design

Secure by Default takes a holistic approach to solving security problems. Security is treated as a core fundamental rather than a followup activity.

Embedding security within a design is directly comparable to good modern technical designs and fundamentally ensuring the 'thing' actually works.

Secure by Default

The National Cyber Security Centre (NCSC) describe the Secure by Default principles as:

- security should be built into products from the beginning, it can't be added in later;
- security should be added to treat the root cause of a problem, not its symptoms;
- security is never a goal in and of itself, it is a process - and it must continue throughout the lifetime of the product;
- security should never compromise usability - products need to be secure enough, then maximise usability;
- security should not require extensive configuration to work, and should just work reliably where implemented;
- security should constantly evolve to meet and defeat the latest threats - new security features should take longer to defeat than they take to build;
- security through obscurity should be avoided;
- security should not require specific technical understanding or non-obvious behaviour from the user.

Context is important

The previous principles can generally be applied in most scenarios however interpretation and applicability in context can vary - the Cyber Security team are here to help and advise.

NCSC also have a set of whitepapers which help explain some approaches to building products which align with these principles (and they add to them over time):

- Building a secure feature-rich computing platform, such as a smartphone.
- Storing sensitive data on consumer platforms

Source code publishing

This guidance applies to all staff and contractors who work for the . In particular, it applies to product owners, technical architects, security architects, and developers.

policy about making source code developed by the available complies with UK Government guidance.

By default, developers develop source code in a way that means it can be stored and published in the open. There are exceptions, for example sensitive material such as encryption keys.

This document is not about the use of existing open source materials.

Reasons for working in the open and sharing source code by default

Point 8 of the "Digital by Default" Service Standard states that you should:

> Make all new source code open and reusable, and publish it under appropriate licences (or provide a convincing explanation as to why this cannot be done for specific subsets of the source code).

This includes "Making source code open and reusable".

When you should not publish materials in the open

There are some circumstances when materials should not be public.

Obvious examples include security or encryption keys or credentials, and configuration details. Other examples include:

- Algorithms used to detect fraud.
- Materials that relate to unreleased policy.
- API keys for cloud-hosted applications or environments, for example AWS.

An important exception is for materials developed by third parties. They might have retained ownership of the Intellectual Property (IP).

More guidance to help you decide when to publish materials in the open or not is available here.

System Test Standard

Related information

Technical Controls Policy on page 30

About this document

This document is the System Test Standard. It is designed to help protect IT systems by providing a common standard for system security testing.

How to use this document

The purpose of this standard is to provide a process around the security testing of IT systems and outline what security issues should be considered at each stage of the process.

Note: This document focuses on the security aspects of system testing. It is not intended to provide comprehensive information on general system testing.

Overview
Introduction

The purpose of system testing is to ensure all the functional and non-functional requirements of the system are verified to be operating within specified bounds.

HMG Security Policy Framework mandatory requirements 9 states that:

> Departments and Agencies must put in place an appropriate range of technical controls for all IT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

Policy statements on system testing are covered in the IT Security Technical Users Policy. This document sets out the standard for system test implementation from a security perspective.

Scope

This standard is concerned with the security testing of all IT systems including IT systems hosted by third party suppliers on behalf of the .

Definitions

For the purposes of this standard, the following definitions apply:

System testing	Tests conducted against an application or IT system to ascertain whether that application or IT system has implemented the desired functional and non-functional requirements.
Security testing	The subset of system tests which concentrate on testing an application's or IT system's functional and non-functional security requirements.

Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. System testing is captured as a basic requirement in Level 1, which the will need to demonstrate compliance with in the IAMM return to Cabinet Office.

Testing approach

This standard outlines at a high level the security testing which must be applied to all IT systems to ensure that security vulnerabilities are identified and risk managed appropriately. The aim is for this standard to feed into the overall test requirements and test plan for an IT system.

System testing, in particular system security testing, must be performed in support of the system assurance process to provide confidence that:

- The implementation delivers the agreed security controls.
- There are no unacceptable security vulnerabilities within the delivered solution.

The following three principles must be applied when putting together a test plan for an IT system:

1. The rigour of the tests must be commensurate with the impact of a security failure.
2. The tests may need to be repeated to provide assurance that subsequent changes to the system or service have not introduced new vulnerabilities.
3. The testing services (automated or otherwise) used must generate security compliance/assurance evidence against known threats and current IT security policies. For example, penetration testing (or ITHC), ad-hoc scanning, secure code review, and software configuration assurance.

Note: It is policy that system testing be conducted in a live environment. System testing should combine tests conducted in a non-live system test environment with tests conducted in a live environment (e.g. an IT Health Check).

The rest of this document is split into four sections:

1. Guidelines: Sets out the basic security requirements for IT system testing and provides guidance on system test data.
2. Risk assessment and management: Outlines the link between system assurance and security testing.
3. Types of security tests: Provides an overview of the common types of security testing.
4. Pre-live security testing: Outlines how security testing links in with the standard set of testing activities which are conducted during the development and deployment phases of an IT system.

Guidelines

HMG IS 1 and 2 require that assurance evidence is provided covering an IT system's business systems design, implementation, and operation.

Security testing of an IT system to obtain the assurance evidence required can occur at various points throughout the system development and deployment lifecycle (refer to Table 1). For example:

Commercial off the Shelf (COTS) product assurance	Test assurance obtained through the use of a security evaluated, either by CESG or via the Common Criteria scheme COTS product. This assurance can be obtained during the system design phase.
System configuration tests	Test assurance obtained before deployment and maintained thereafter in line with the system re-accreditation process. Further details on the Accreditation process can be found in the Accreditation Framework.

System test data

Data used for system testing usually involves test data which have similar characteristics as close as possible to operational data.

Data used for system testing **must not** contain any live data. The use of live data, and in particular live data containing personal information, is prohibited. However, as test data will tend to simulate live operations data, it is important that test data is protected to ensure details of the system design and operation are not compromised.

To protect system test data, the following principles should be followed:

- The test manager must authorise the use of test data.
- Test data should be erased from a testing environment immediately after the testing is complete or when no longer required.
- The copying and use of test data should be logged to provide an audit trail.

In exceptional circumstances, the use of live system data might be permitted. Permission to use live data is by exception only. A valid business case must be approved by the IT Security Officer (ITSO), system assurer, and Information Asset Owner (IAO). Further information can be obtained from the Data Access and Compliance Unit (DACU) who maintain the policy on the use of live personal data.

Note: The risk associated with the use of live personal data for testing might require Senior Information Risk Owner (SIRO) approval. Refer to this information for further details.

Risk assessment and management

As expressed at the start of this section, the rigour of any security tests must be commensurate with the impact of a security failure. This means that a risk based approach must be taken when considering what types of security tests to execute.

The decision on what security tests to include in the overall system test plan must be based on the system IS1 risk assessment, and agreed with the system assurer. The following section (Types of security tests) provides an overview of the types of security tests which must be considered. Further details on the assurance process can be found in the Accreditation Framework.

When a security test has been conducted, it is likely to highlight several risks and issues which need to be remediated and managed appropriately. This remediation is usually captured in a Risk Treatment Plan (RTP) which outlines what the issue or vulnerability identified is, the risk associated with it, and the planned risk mitigation. The RTP needs to be agreed with the system Accreditor prior to being implemented. Further details on this process can be found in the Accreditation Framework.

Types of security tests

Security testing is discussed as part of the NCSC guidance on Building a secure digital service.

This section provides an overview of the three most common types:

- System configuration tests.
- Vulnerability scanning.
- Compliance scanning.

System configuration tests

System configuration tests are first conducted prior to deployment and repeated periodically thereafter with the objective being to ensure that the system or system component does not contain any unacceptable vulnerabilities.

These tests may include:

- Internally conducted tests (e.g. by the system developer) to provide informal assurance that there are no unacceptable vulnerabilities.
- External and perhaps more rigorous tests to provide formal assurance, for example, a penetration test or social engineering test.

There any many different types of penetration test. For most IT systems, the most common conducted is an annual IT Health Check (ITHC).

Internal tests may be performed more regularly to provide informal assurance that on-going changes have not introduced any new vulnerabilities to an IT system, and that existing security controls are operating correctly.

IT Health Check

An IT Health Check (ITHC) is the penetration test conducted as part of the NCSC specified and managed CHECK scheme. It is intended to provide external assurance that an IT system's setup and configuration meets the desired HMG assurance level.

Note: Most systems connected to or other government networks or systems mandate an ITHC every 12 months.

Vulnerability scanning

A vulnerability scan is intended to scan a network (and connected IT systems), cataloguing the patch status of all software and system services, and alerting on those identified which are not up-to-date, based on databases of patches and vulnerabilities. These alerts provide an operational view of the technical vulnerabilities an IT system is exposed to, and the information required to assist an IT system manager in applying up-to-date patches.

This type of scanning is intended to provide regular internal assurance to the ITSO and assurer that operational security risks are being managed effectively.

Compliance scanning

Besides simply testing for the absence of correctly patched software, some vulnerability scanners can also test when an IT system's settings correspond to an established benchmark, for example, to the password requirements, or a commercial security standard such as PCI DSS. The scanner operates by examining the security configuration settings of each IT system client (through a client installed agent) against one or more benchmarks (e.g. PCI DSS or ISO 27001), producing a compliance report as an output which can be supplied as assurance evidence.

Pre-live security testing

During the development and deployment phases of an IT system, there are a number of standard testing activities which are conducted. Security testing is not a separate stream of activity. It must be integrated within the overall set of testing activities.

The Secure code review activity highlights the issues associated with secure code reviews, while the Security consideration activity provides an overview of the security testing consideration which should be applied against each standard testing activity.

Secure code review

In principle, good software development practices and the application of a comprehensive code quality assurance regime should cover the basics of what is required to deliver a secure system. The NCSC provides guidance on Building a secure digital service. It is recommended that those responsible for software development and system testing review the guidance, and ensure any development practices and system testing reflects the guidance provided.

Note: It is essential that the secure coding guidance provided to application developers and the secure code review regime is documented, and made available to the system assurer for review and approval.

Security consideration

Table 1 following provides a high level overview of the security testing which should be considered against each of the main testing activities typically conducted during the development and deployment phases of an IT system.

Table 4: Table 1 – Security consideration

Testing activity	Description	Security testing consideration
Unit, Module, or Package Testing	This is aimed at verifying that individual modules/packages comply with their design.	Refer to Secure code review.
Component Testing	Units or Modules combined into components then tested. This is aimed at verifying that the individual components meet their design and specification requirements. Third party software may also be introduced at this point and tested.	Refer to Secure code review. Functional testing and enhanced secure code review of security enforcing components.
Integration Testing	Involves combining system components together into a complete system release, then testing as a whole.	Functional testing of security enforcing components. Functional testing of the integration of components with security enforcing functions.
Acceptance Testing (FAT and SAT)	The set of tests to be run to demonstrate the suitability of the system to the client. These will typically be a subset of the tests used for system testing in the integration phase.	Testing of both functional and non-functional security requirements. Penetration test or ITHC (refer to System Configuration Tests). Vulnerability scan (refer to Vulnerability Scanning). Compliance scan (refer to Compliance Scanning).

Testing failure

Should a failure occur in any of the security testing activities undertaken, an assessment must be made on what caused the failure and how serious it is. There may need to be discussions with the system assurer to inform them of any serious issues which might affect the assurance of the IT system.

Acceptance testing

As described in the last row of Table 1, some form of security testing must form part of the acceptance criteria for an IT System.

Service Owner Responsibilities

Summary

This document sets out the security responsibilities you have as the person ultimately responsible for a bespoke technology or digital service ("the technology owner") in the .

The list of items below can look intimidating at first glance. However, depending on the nature of your service or technology, some of these items might be quite small.

Every Service have an identified person responsible for performing each of the activities listed below.

One person be responsible for multiple items, provided they have the appropriate skills and training to perform each duty satisfactorily. The Product or Service Owner is responsible for ensuring these activities are allocated and carried out.

Whilst these activities might be performed by a supplier or sub-contractor as part of delivering the service, as Product or Service Owner you remain responsible for ensuring that contract(s) require your supplier(s) to perform these activities in accordance with Security Policies.

The activities do not necessarily need to be performed within your team – for example, you might 'outsource' them to another area such as the Justice Digital Security Operations Centre. You remain responsible for ensuring there is a clear understanding of who is doing what in these relationships.

Activities

Security Risk Management

Ensuring that security risks in the service are managed in accordance with wider departmental policies and escalated as necessary to senior management.

This also includes ensuring that there is a security improvement plan to address any risks and vulnerabilities that emerge in the service.

Secure Configuration

Establishing and implementing default secure configurations for all aspects of the service (for example endpoints, platforms, services, and containers) and ensuring these always remain current and in-place.

Asset Management

All IT assets used in the delivery of the service be tracked in an asset management solution, which be routinely checked for accuracy.

ID and Access Management

Regularly reviewing and ensuring user access and permissions for the service are appropriate and limited to authorised users only (including general user and privileged accounts). Ensuring that robust processes are in place for joiners, movers and leavers (JML) End or change of employment - MoJ Security Guidance.

Security Maintenance

Undertaking regular (automated) activities to ensure the service remains secure – such as regular patching and review.

Development Security

Undertaking regular (automated) activities to ensure the service remains secure – such as regular patching and review.

Threat and Vulnerability Management

Threat and Vulnerability Management - Activities taken to ensure the service remains protected against vulnerabilities, through vulnerability scanning, and remedial actions.

This also includes ensuring that all product teams understand their security dependencies on third parties, and have effective measures in place to deploy mitigations swiftly as required when new threats emerge.

Security Testing

Organising routine and exceptional testing of security controls within the service to ensure they are continuing to function effectively.

Cryptographic and Secrets Management

Where relevant, issuing, managing, and revoking cryptographic credentials via Public Key Infrastructure (PKI). Also, management of shared secrets where required.

Event Detection Activities

Undertaking specific activities to uncover security-relevant events across the service; including operating canary tokens, honeypots, threat hunting, data loss prevention, network monitoring, SaaS security monitoring, and shadow IT detection as applicable.

Event Source Management and Maintenance

Ensuring the service is routinely providing agreed security monitoring events to a security event detection solution.

Incident Management and Response

Developing security incident playbooks, supporting security incident triage; and Data Protection incident investigations, response, and handling to ensure security events cause minimal harm to the organisation, and that evidence is captured for any wider analysis. For more information, refer to the Report a security incident guidance.

Supply Chain Security and Assessment Management

Assessing the suitability of third-party suppliers of the service. Ensuring that the product team understands and undertakes their specific respective security roles and responsibilities with the supplier with respect to the security of the service.

Backup and Recovery

Ensuring all critical information within the service is backed up regularly; the backups are tested regularly, and the service can be completely recovered in the event of a security incident.

Data Protection

Ensuring systems processing personal data are compliant with the Department's Data Protection policy and relevant Acceptable Use Protocols for secure processing, transfers, and storage of personal data. Any data protection risks in relation to confidentiality, integrity or availability of personal data have remediation plans in place.Data Protection - Ministry of Justice HQ Intranet.

Adherence to Policies

Putting in place explicit processes for governance and compliance of security policies, for example how to monitor, report, and maintain compliance.

Secure Use of the Service

Supporting and educating users on how they access and use your service securely. This is context-dependent and might be as simple as ensuring that in-built user guidance helps explain security concepts in your service. For complicated end-user services, this might require eLearning or other targeted training. If you provide a platform, this might involve specific guidance for other services built on it, to explain their security responsibilities.

More Information

For assistance, please contact your local cyber consultant in the first instance. For queries on policy and guidance email

Test data

Using Live Data for Testing purposes

Summary

This document describes the use of live data during testing of systems. In general, using live data for testing purposes is considered bad practice. By default, the does not permit testing using live data. It is highly likely that simply using live data for testing purposes would not be compliant with GDPR.

Following this guidance will help you avoid problems, but cannot guarantee that you have addressed all the concerns. You must carry out a full Data Protection Impact Assessment.

Who is this for?

This guide is aimed at two audiences:

1. The in-house Digital and Technology staff who are responsible for testing systems as part of technical design, development, system integration and operation.
2. Any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the .

Do you really need to use live data?

According to Information Commissioners Office, you may use either live or dummy data to test your products so long as they are compliant with data protection law. However, using dummy data may be preferable as it does not carry any risk to data subjects.

If you are processing live data, you will need to complete a Data Protection Impact Assessment beforehand if there is a possibility of risk to the data subject. The ICO has helpful information about using a Sandbox to help utilise personal data safely.

Data used for testing purposes must have characteristics that are as close as possible to operational data. But that is not the same thing as needing to use live data.

Check whether you really need to use live data, by considering the following questions:

1. **Speed:** What are your time requirements for test data provisioning?
2. **Cost:** What is an acceptable cost to create, manage and archive test data?
3. **Quality:** What are the important factors to consider related to test data quality?
4. **Security:** What are the privacy implications of these two sources of test data?
5. **Simplicity:** Is it easy for testers to get the data they need for their tests?
6. **Versatility:** Can the test data be used by any testing tool or technology?

The best test data simulates live operations data.

Note: It is important that test data is protected to the same standard as the live data. This is to ensure that details of the system design and operation are not compromised.

To protect test data, the following principles should be followed:

- The test manager must authorise the use of test data.
- Test data should be erased from a testing environment immediately after the testing is complete or when no longer required.
- The copying and use of test data should be logged to provide an audit trail.

Note: In the absence of an allocated test manager for a project, refer to the system owner.

By default:

- Data used for testing must not contain any live data.
- Using live data containing personal information is prohibited.

In exceptional circumstances, the use of live system data may be permitted. Permission to use live data is by exception only. A valid business case must be approved by the CISO, system assurer and the Information Asset Owner (IAO).

The Information Asset Owner must ensure that live data will be used lawfully, fairly and in a transparent manner in the interest of the data subject.

A thorough risk assessment, and a Data Protection Impact Assessment, should be carried out to ensure where interdependent applications, systems, services, APIs, BACS, XML, or processes, may be required, these are appropriately reviewed and security controls put in place.

Anonymising data

It might be acceptable to 'anonymise' the live data such that it can be used more safely for testing purposes. Consider:

- Is it possible to do this?
- What processes can you follow to generate acceptable data?
- Is randomisation sufficient?
- What about obfuscation?
- When is production-like data acceptable (or not) for testing purposes?
- How do you ensure that production-like data is sufficient for testing purposes?
- What are the expectations regarding suppliers - for code, and for services?

If you are considering the anonymisation option, pay particular attention to specific types of data that are often sensitive. Examples of data that must be anonymised include:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where it can be used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation
- data concerning criminal offences
- email addresses
- bank details
- telephone numbers
- postal or residential addresses

This list is not exhaustive.

In general, recommendations for anonymising data include:

- Replace with synthetic data.
- Suppress (remove) or obfuscate.
- A useful link for anonymising telephone numbers is here.

If testing is to go ahead
Developer access

In a normal working environment, developers working on an application, platform or service would be segregated away from access to live/production data. They would never be able to access or manipulate this data. The use of live data for test purposes would potentially negate or bypass these controls.

Also, developer roles are often specified as not requiring SC clearance or higher. This applies also to external (3rd party) software suppliers generating bespoke applications or services. The expectation is that the developers do not ever have access to live data.

The use of live data for testing may mean that the clearance levels for developers on a given project would need to be reviewed.

Preparing for tests

Any code or tests involving live data should ensure the following:

- Code performs input validation.
- Output is correctly encoded.
- Full authentication and authorisation is in place.
- Session management is in place to ensure that code and data is not continually available outside the testing activities.
- Strong cryptography is used to protect data 'at rest', 'in transit' and 'in use'.
- All errors and warnings generated by applications, services, or recorded in logs are monitored, captured and actioned.
- A Data Protection Impact Assessment has been performed.
- Any backup processes will correctly filter out or otherwise protect the live data within the test environment.

Supplier relationships

Information security in supplier relationships

Assessing suppliers

The assesses suppliers as a responsible public body managing public funds and data. These assessments range from commercial and legal for the purposes of contract through to risk assessments for the purposes of information security.

The uses a range of risk management techniques including information risk assessments.

Suppliers are expected to create, maintain and demonstrate a mature and considered approach to risk management when engaged with the .

Accreditation

The no longer accredits new systems or suppliers (as defined by CESG Information Assurance Standard 1&2).

The maintains accreditations where committed to by existing contract.

Commodity digital technology

assesses commodity digital technology supply chain such as Software-as-a-Service (SaaS) tools such as , Microsoft Office 365, Trello and Atlassian Cloud based on the Cloud Security Principles, information risk assessment techniques and shared data within HMG.

Contractual promises

The embeds data governance and security-related clauses and schedules with contracts.

The is in the process of standardising and commoditising comprehensive clauses and schedules and will implement them over time.

Security Aspects Letters

Purpose

The will issue a Security Aspect Letter (SAL) where appropriate.

SALs are generally not required at but may issue a SAL where it is optimal to do so or to supersede existing SALs from the previous classification scheme.

This page was last updated on 2018-12-21

Template

Dear `<NAME OR ROLE OF SECURITY DIRECTOR>`,

Subject: Security Aspects Letter

This Security Aspects Letter ('SAL') establishes the security principles which `<ORGANISATION LONG LEGAL NAME, should be highest entity position such as the Group Plc>` and/or its affiliates (together "`<ORGANISATION SHORTNAME>`") shall comply with in producing, handling or storing materials, information or data pertaining to the Ministry of Justice ('Authority').

This letter applies to `<ORGANISATION SHORTNAME>` and any relevant subcontractor within `<ORGANISATION SHORTNAME>`'s supply chain as required.

The following sections have been identified as the main areas where guidance is required. If there are any queries, please ask for clarification.

Purpose

This SAL issued by the Authority intends to convey the security principles required of <ORGANISATION SHORTNAME> to appropriately and proportionately ensure adequate confidentiality, integrity and availability of Authority data.

The SAL is not a complete and exhaustive list of requirements and conveys the spirit of information security and risk management requirements.

<ORGANISATION SHORTNAME> is required to ensure a comprehensive approach to information risk management through procedural, policy, personnel, physical and technical controls while in possession of Authority information.

Markings

This SAL has been developed under the premise that all information assets will be classified OFFICIAL under the UK Government Security Classifications Policy (GSCP) and that some may carry additional descriptors (for example, COMMERCIAL) to re-enforce handling requirements (such as 'need to know' principles) through the use of the handling caveat.

All information must be considered whether it bears a marking or not.

Handling Instructions

It should be noted that assigning an appropriate classification to information remains the responsibility of the creator or owner of the asset. Information marked with the handling caveat may state, or otherwise be accompanied by, additional handling requirements (for example to limit distribution or define additional access controls) which all recipients including the <ORGANISATION SHORTNAME> must comply with.

In general, the Authority expects <ORGANISATION SHORTNAME> to apply the need-to-know principle to information related to Authority systems, and restrict access to such material to those within <ORGANISATION SHORTNAME> (and its supply chain) who genuinely need it to perform their duties. General system information such as system names, IP addresses, high-level designs, etc does not require special handling protections.

Legacy Material

Information marked under the previous classification scheme(s) (such as UNCLASSIFIED, PROTECT, RESTRICTED or CONFIDENTIAL) should be effectively considered unless otherwise stated.

Information marked under previous classification schemes should be reviewed as to whether the information within requires handling caveat markings and/or particular handling guidance before being re-marked as .

Data Aggregation

In aggregation, the impact of a breach of any of these Security Aspects may be higher than the individual records or documents. <ORGANISATION SHORTNAME> should ensure that aggregated or accumulated collections of information assets are protected appropriately.

Data Offshoring

<ORGANISATION SHORTNAME> is permitted to Process Authority data (including Personal Data) outside of the United Kingdom subject to the maintenance of adequate information controls and governance, including (not not limited to), the continuation of the protection of rights and freedoms of Data Subjects in relation to their Personal Data, adequate contractual controls and adequate consideration under the <ORGANISATION SHORTNAME> Information Security Management System (ISMS).

<ORGANISATION SHORTNAME> must not routinely transfer or otherwise Process Authority data within an incompatible legal framework to the United Kingdom - more information on this is available on suitable request from the Authority.

Definitions are as per the Data Protection Act (2018)

Policy Compliance

Effective and appropriately scoped policy controls must be in place to underpin effective information management.

While related information security management certifications recognised by the British Standards Institution (BSI) such as ISO27001:2013, ISO27002:2013 and Cyber Essentials Plus are preferred, they are not required subject to comparable controls, policies and practices being in place.

A robust ISMS must be in place that ensures information assets are appropriately protected.

A holistic approach to information security must include staff awareness and training through to robust technical and enforced access controls.

Physical Security

Physical locations (such as offices and data-centres) must have appropriate physical security characteristics to safeguard information from informational risks.

Personnel Security

All personnel with direct or indirect access to, or influence over, information assets must achieve security clearance to at least the HMG Baseline Personnel Security Standard (BPSS).

Some roles and sites may require additional levels of clearance. These will be advised by the Authority to <ORGANISATION SHORTNAME> on a case-by-case basis.

All required security clearances must be achieved, and warranted to the Authority, prior to commencement of work by the individual unless otherwise agreed in writing by the Authority.

Full details of Security Clearance requirements are available with the Authority Vetting policy.

IT Controls

Systems

IT systems must be assessed under <ORGANISATION SHORTNAME> ISMS to ensure an appropriate level of informational risk understanding and where applicable corresponding controls or risk mitigation strategies.

IT technical controls should make all efforts to align to current recognised good practices and be periodically reviewed (no less than 12 month intervals) to understand and re-align controls where appropriate. Best practices include, but are not limited to, encryption methods, multi-factor authentication and software life cycles.

<ORGANISATION SHORTNAME> must ensure system suitability as per the output of the <ORGANISATION SHORTNAME> ISMS prior to the introduction of non-test data.

<ORGANISATION SHORTNAME> must provide information risk management information to the Authority on request so that the Authority may determine whether the assessment made and controls in place are sufficient and robust.

Any remedial activity that may be required by the Authority will be considered under contractual and commercial arrangements however <ORGANISATION SHORTNAME> must acknowledge that systems must be fundamentally fit for purpose and capable of protecting information assets in proportion to their content and value as defined by <ORGANISATION SHORTNAME> and/or the Authority.

Data transfer protections (data-in-transit)

All Authority, or Authority related data (such as professional work product pertaining to or on behalf of the Authority), must be protected against negative events (such as interception, misdirection, manipulation or otherwise unintended outcome) while in transit.

The Authority considers application or transport level encryption to be sufficient at subject to configuration guidance from the UK National Cyber Security Centre (NCSC) having been met.

Some examples of satisfactory approaches include, but are not limited to:

- Email systems meeting the 'Securing government email' guidance
- Transport Level Encryption (TLS) version 1.2 and higher, aligned to NCSC recommended configuration(s)
- Internet Protocol Security (IPSec) aligned to NCSC recommendation configuration(s)
- NCSC-approved products or services for data transfer
- Authority-approved products or services for data transfer

<ORGANISATION SHORTNAME> should discuss with the Authority where deviations from NCSC recommendations may be required due to technological limitations.

SAL revisions

The Authority reserves the right to issue a revised SAL at any time.

You are requested to acknowledge receipt of this letter and your acceptance of its terms as incorporated into your contract and binding within 14 days.

You are requested to confirm that the details of this SAL have been brought to the attention of the personnel directly responsible for the security of the services provided to, or in support of, the Authority, that they are fully understood, and that the security and information assurance requirements set out in the contract schedules can and will be taken to safeguard the material concerned within 28 days.

You agree to provide a SAL in similar form to all subcontractors, obtain their acknowledgement and provide a copy to the Authority within 28 days.

Yours sincerely,

Chief Information Security Officer Ministry of Justice (UK)

Declaration

<ORGANISATION SHORTNAME> will be required to return a declaration.

Please sign the following declaration and return this letter to the Authority, keeping a copy for your own records. Should you have any queries, please contact the Authority via your point of contact and/or the contact details located within the SAL.

Supplier Declaration

The <ORGANISATION SHORTNAME> hereby confirms that the associated with the requirements described in this Security Aspects Letter have been brought to the attention of the individuals and organisations directly responsible for the provision of the various services. Additionally, that they are fully understood, and that the required security controls can and will be taken to safeguard the material and assets concerned.

For and on behalf of <ORGANISATION SHORTNAME>

…….. (name)

…….. (position) [Should be at least Director level]

……(date)

Distribution

Internal within Authority:

Action:

- Authority Security & Privacy

Information:

- Director of Authority Service Delivery
- Head of Service Delivery
- Authority Commercial

External:

Action:

- <ORGANISATION SHORTNAME>

Supplier corporate IT

The does not by default prohibit the use of supplier organisation corporate IT for processing data. The expectation is that the supplier corporate IT environment is well designed, maintained, governed, and defended, in line with large scale commercial threat models.

Subject to the requirements described in this document, the does not require suppliers to create or maintain dedicated or segregated IT solutions for processing data classified at .

For data classified at , additional comprehensive security assurance is required. The assurance include controls and governance processes. The assurance be appropriate to the information sensitivity. Contact the for assistance regarding acceptable security assurance for data.

Technical security

Supplier corporate IT systems are expected to maintain appropriate levels of technical security defences. These defences protect appropriately all types of data. This includes data processed or stored in any way by supplier corporate IT systems.

Examples of appropriate defences include, but are not limited to:

- Use of current Transport Layer Security or IPSec for in-transit encryption.
- Hashing and cryptography mechanisms for data stored at-rest.

The defences scale from individual data items in a database, up to entire storage facilities.

Supplier systems be proportionally resilient to malware. This might be achieved by ensuring segregation between systems, users, and data. Other industry standard best practices, such as email attachment scanning or filtering, might also be suitable.

Email security

Supplier corporate email systems processing data align to the UK government secure email policy, thereby following widely accepted best practices.

Supplier corporate email systems are not required to integrate to the Public Services Network (PSN).

Data Governance
Data offshoring

Supplier's process data, including Personal Data for which the is responsible, outside of the United Kingdom, subject to the maintenance of acceptable information controls and governance.

data be processed within a legal framework that is incompatible with that of the United Kingdom.

Working overseas

Supplier staff are not prohibited from working overseas while processing data, subject to implementing and maintaining acceptable information controls and governance. In particular, the controls and governance align and comply with policy on remote working and working overseas.

When working overseas, it might be necessary to limit access to information while the user travels. Alternatively, it might be appropriate to use secondary, temporary accounts, to avoid primary account compromise. Contact the for assistance regarding acceptable security assurance when working overseas.

Data backups

Supplier corporate IT systems backup data for extended retention times. An example would be keeping archived or deleted emails for an additional few months. Backup systems also exist in such a way that individual backup items cannot be individually deleted, but instead are subject to a system-wide backup rotation or retention schedule.

Suppliers discuss and agree these cases with the .

Local end-user device data

The acknowledges that corporate users typically "download" files, for example from local email client caching to file downloads using a web browser. These files might remain within `Downloads` folders, until explicitly deleted by the user.

Suppliers include and address these types of data locations in data governance regimes.

Supplier service delivery management

Azure Account Baseline Templates

The lowest acceptable common denominator to appeal to the largest possible number of people for security-related promises, capabilities and configurations of Azure accounts.

Baseline

The baseline for Azure accounts is formally published as part of the Security Guidance from the Digital and Technology Security and Privacy team.

Background

As an organisation expands its use of Azure services, there is often a conversation about the need to create multiple Azure subscriptions to ensure separation of business processes or for security, compliance, and billing. We tend to use separate Azure subscriptions for each business unit so that it can meet the different needs of the organisation. Although creating multiple subscriptions has simplified operational issues and provided benefits like security and resource isolation, a smaller blast radius, and simplified billing, it results in widely varying security posture across the subscriptions and there is the need to align all of these subscriptions to a baseline secure standard.

Areas of Concern

Azure Security Center.

Azure Identity Management (PIM).

Azure Defender.

Web Application Firewall.

Monitor.

Advisor.

Regions.

Azure Storage Encryption.

Key Vault.

Tagging.

This section provides the definition of baseline controls and list of templates that cover the baseline and governance guardrails that can be implemented in new accounts.

Azure Security Centre

Use Azure Security Centre to ensure workloads are secure and to strengthen the security posture of the Azure estate. With continuous assessment, newly delivered resources are assessed and scored based on recommendations against Azure Security Benchmark.

Azure Identity Management (PIM)

Enabling PIM helps to mitigate the risk of excessive, unnecessary or misused access rights by allowing administrators to discover, restrict and monitor access to Azure Active Directory resources. Essentially, it means that any user

with access to the data is only allowed access to certain files or services, assigned by the global and privileged role administrators.

Recommendations to improve overall Azure security posture by monitoring at a minimum include:

- Block or secure risky user accounts.
- Require users to register for Multi-Factor Authentication (MFA).
- Enable the use of Just-in-Time access, so that administrators can create privileged access for a specific time frame.

Refer also:

- Azure AD Privileged Identity Management.
- Activate my Azure AD roles in PIM.

Azure Defender

By enabling Azure Defender and integrating with Azure Security Center, you get an additional layer of security with which you can protect workloads hosted in Azure. Defender provides protection from most advanced threats, such as brute force, remote desktop protocol (RDP) or SQL injection attacks.

Refer also:

- Enable Azure Defender.
- Enable Defender for Key Vault.
- Enable Defender for SQL.

Web Application Firewall

Azure Web Application Firewall (WAF) on Azure Application Gateway is a cloud-native service that provides centralised protection to web applications from common cyber attacks. Azure WAF protects against crawlers and scanners, SQL and command injection, cross-site scripting, HTTP protocol violations, anomalies, and other common web attacks. A WAF can support configurable request size limits and custom rules, exclusion lists, and geo-filtration of traffic.

Refer also:

- Azure WAF deployment.

Monitor

Azure Monitor is the centralised console where you can create alerts around various resources in your subscription and also manage them. Alerting in Azure Monitor includes creating and managing alert rules, and creating and managing action groups.

Refer also:

- Create, view, and manage activity log alerts by using Azure Monitor.

Advisor

Azure Advisor takes the guesswork out of optimising your Azure deployments. Specifically, providing highly-personalised recommendations and best practices which are both actionable and proactive. Azure Advisor helps you find ways to reduce costs related to Azure service subscriptions, improve the performance, security, and availability of resources that are in use.

Refer also:

- Azure Advisor.

Regions

The does not use non-EU Azure regions, for strategic compliance and performance reasons. For more information on regions, refer to Conditional Access : Block by region.

Azure Storage Encryption

Azure Storage data encryption and decryption is transparently done using 256-bit AES. Azure Storage encryption is for all storage accounts, including both Resource Manager and classic storage accounts. This cannot be disabled, as the data is secured by default. All Azure Storage resources, such as blobs, disks, files, queues, and tables, including all object metadata, are also encrypted at rest.

Refer also:

- Azure Storage encryption for data at rest.

Key Vault

Azure Key Vault protects encryption keys and secrets stored in Azure. The material might be certificates, connection strings, and passwords. However, steps should be taken to maximise the security of your vaults and the data stored within them while storing sensitive data, including enabling Defender for Key Vault to safeguard your data.

Refer also:

- Best practices to use Key Vault.
- Defender for Key Vault.

Tagging

Assigning tags to Azure resources is essential in creating a well-organised and transparent classification, and achieving significant cloud cost optimisation. When implemented, this practice can provide a consistent basis for applying policies across the organisation.

Refer also:

- Assign policy definitions for tag compliance.

Baseline for Amazon Web Services accounts

The has a 'lowest common denominator' for security-related promises, capabilities and configurations of Amazon Web Services (AWS) accounts.

The baseline is not a holistic 'do' and 'do not' list, but a minimum line in the sand for what 'at least' be done.

The base principle

All AWS accounts **must** use a series of agreed configurations to enable and support good tenancy within AWS and a suitable cyber security posture.

Anti-solutionising

This baseline discusses outcomes not *how* the baseline will be achieved/implemented.

The Security team strongly encourage the use of the highest abstraction level of services available from AWS to achieve these goals, and minimising the amount of custom code and configuration which needs to be developed (and thereafter, maintained) to satisfy each baseline.

Initial considerations

The type of hosting is the first consideration. service developers utilise Cloud Platform for new services. Anyone developing new services refer to the How to host services page which provides initial guidance.

Legacy applications be hosted via the Modernisation Platform.

Security incidents

The Security team should be added as a security contact for all Information security incidents generated by AWS. The contact details for an AWS Account can be updated using the reference here.

- Full Name: `Security Team`
- Title: `Mx`

- Email Address:

Baseline
IAM Access Analyzer

Use IAM Access Analyzer to audit and identify resources that are shared with an external entity.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
IAM Access Analyzer is enabled on all accounts, in all used regions, all of the time.	Alerts fire for new findings.	Findings are archived (if intended) or resolved (if unintended) within 7 days.

GuardDuty

Use AWS' commodity IDS solution to detect/protect from malicious or unauthorised behavior.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
GuardDuty is enabled on all accounts, in all regions, all of the time.	Alerts fire when GuardDuty is not enabled in a AWS account. Alerts fire for at least `HIGH` and higher (or some version of) GuardDuty matches.	GuardDuty is automatically re-enabled.

CloudTrail

Use AWS' native activity audit platform (with adequate non-repudiation) to capture what AWS user (IAM etc) activity and changes are made within our AWS accounts

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
CloudTrail is enabled within all accounts, all of the time. CloudTrail logs are carbon copied to an AWS account controlled by Cyber Security.	Alerts fire when CloudTrail is not enabled in an AWS account.	CloudTrail is automatically re-enabled.

Config

Use AWS' native AWS configuration activity audit platform to capture what changes are being made to AWS configurations.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
Config is enabled within all accounts, all of the time. Config logs are carbon copied to an AWS account controlled by Cyber Security via CloudTrail.	Alerts fire when Config is not enabled in an AWS account.	Config is automatically re-enabled.

Tagging

Tag all of our AWS objects, so we know they have a purpose and are intentional with defined ownership.

We have our own infrastructure ownership/tagging standards.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All relevant AWS objects are tagged as per requirements.	Creating AWS user is notified automatically in increasing urgency when object is untagged. AWS account owner (and increasing escalation) is automatically notified when objects remained untagged.	Untagged objects are forcefully and automatically shutdown/disabled or isolated after 7 consecutive days of not being tagged.

Regions

Do not use non-EU AWS regions for strategic compliance and performance reasons.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
No AWS account can create resources outside of AWS EU regions.	Alerts fire when non-EU resources are created to both the infrastructure teams and resource creator.	Non-EU resources are automatically and forcefully shut down after 12 hours.

Identity and Access Management

Enforce Identity and Access Management and Joiners, Movers and Leavers (JML) within AWS. We also need to ensure accounts that legitimately exist are well protected.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
AWS user accounts have a defined and peer reviewed method for request/creation. Viable, authoritative and 'single source of truth' documentation exists to describe each AWS account and who should and should not have access (in terms of roles). Idle AWS user accounts are suspended. MFA is required, always, enforced by policy. Root user account usage is considered abnormal. Passphrase and/or MFA seed cycled on every AWS root account use.	AWS group account owners are alerted when new AWS accounts are created. Idle (30 or more consecutive days of non-activity) AWS user accounts issue suspension notices to AWS group account owners and target users. Where an account does not have MFA, the user and AWS group account owners are notified after 7 consecutive days. Any login or use of an AWS root account issues login alerts to the AWS group account owners.	Idle AWS user accounts are automatically suspended past threshold. Non-MFA AWS user accounts are automatically suspended past threshold. Alerts fire when an AWS root user account is used but the credentials are not updated within 7 days of use.

For more information on MFA, refer to the Multi-Factor Authentication guidance.

Encryption

Use native AWS configuration options to make reasonable efforts to protect data.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All AWS objects supporting encryption must have it enabled.	S3 buckets without suitable SSE-* encryption enabled are alerted to resource creator and account owner.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and Security.

'World' Access

Ensure that public access to AWS data storage and compute is intentional, to avoid the 'leaky bucket' problem, and to aid attack surface minimisation.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All AWS S3 objects should be not world (public) readable unless specifically intended to do so.	S3 objects are programmatically reviewed (including 'open' ones) against the source infrastructure-as-code, if there is a mismatch the resource creator and AWS account owner notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and Security. After 7 days, the S3 object permissions are forcefully and automatically changed to remove 'world' access.
Compute (for example, EC2 or ECS) instances should not be directly accessible from public networks unless through specific intentional design and should be behind CloudFront and/or applicable load balancing (preferring AWS LB technology). It must be truly exceptional for common service ports (for example, TCP80 or TCP443) to be served directly from compute resources.	Compute instances are programmatically reviewed to ensure they are not internet-accessible unless explicitly designed and documented to be so. If there is a mismatch the resource creator and AWS account owner notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and Security. After 7 days, the relevant security groups are forcefully and automatically changed to remove 'world' access.

Security Hub

Security Hub enabled where possible.

Over time we will be able to use this more, but in the immediate future this will enable us to do CIS-based scans.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
Security Hub is enabled on all accounts, in all regions, all of the time.	Alerts fire when Security Hub is not enabled in a AWS account.	Security Hub is automatically re-enabled.

Implementation

Various AWS account baseline templates have been developed and published for use.

Baseline for Azure Subscriptions

The has a 'lowest common denominator' approach to apply to the largest possible number of people for security-related promises, capabilities and configurations of Azure Subscriptions.

The baseline is not a holistic 'do' and 'do not' list, but a minimum line in the sand for what 'at least' be done.

This guidance is Version 1.4, January 17, 2022.

The base principle

All Azure Subscriptions utilise a series of agreed configurations to enable and support good tenancy within Azure accounts, and a suitable cyber security posture.

Anti-solutionising

This baseline discusses outcomes, not how the baseline is achieved or implemented.

The Cyber Security team strongly encourages the use of the highest abstraction level of services available from Azure to achieve these goals, and minimising the amount of custom code and configuration which needs to be developed (and thereafter, maintained) to satisfy each baseline.

Initial Considerations

The type of hosting is the first consideration. service developers utilise Cloud Platform for new services. Anyone developing new services refer to the How to host services page which provides initial guidance.

Legacy applications be hosted via the Modernisation Platform.

The requirement to use Azure also include basing new services or subscriptions on existing or predefined settings and policies.

For UK Government Services, there are Blueprints available to ensure compliance with meeting Standards and Policies. If these exist, they be replicated and applied to new services or subscriptions.

Security incidents

The Cyber Security team be added as a security contact for all Information or Cyber Security incidents. The contact details for raising Incidents need to be managed internally, for example using an Intranet page.

Baseline

The following are the minimum requirements for usage of Azure.

Identity and access management (IAM)

Utilise Identity and access management (IAM) to defend against malicious login attempts and safeguard credentials with risk-based access controls, identity protection tools and strong authentication options – without disrupting productivity and use IAM for Joiners, Movers and Leavers (JML) within Azure. Ensure Services or Subscriptions that legitimately exist are well protected.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Azure Active Directory is enabled on all accounts, in all used tenants or subscriptions, all of the time.	Alerts fire for new findings.	Findings are archived (if intended) or resolved (if unintended) within 7 days.
Azure user accounts have a defined and peer reviewed method for request or creation. Viable, authoritative and 'single source of truth' documentation exists to describe each Azure account and who should and should not have access based upon Role Based Access Control (RBAC). Idle Azure user accounts are suspended. MFA is always required and always enforced by policy. Root user account usage is considered abnormal. Passphrases or MFA seeds are cycled on every Azure root account.	Azure group account owners are alerted when new Azure accounts are created. Idle (30 or more consecutive days of non-activity) Azure user accounts issue suspension notices to Azure group account owners and target users. Where an account does not have MFA, the user and Azure group account owners are notified after 7 consecutive days. Any login or use of an Azure root account issues login alerts to the Azure group account owners.	Idle Azure user accounts are automatically suspended past threshold. Non-MFA Azure user accounts are automatically suspended past the threshold. Alerts fire when an Azure root user account is used but the credentials are not updated within 7 days of utilisation.

For more information on MFA, refer to the Multi-Factor Authentication guidance.

Advanced threat protection

Leverage Azure to identify and resolve vulnerabilities, assess threats efficiently, and ultimately focus on real threats.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Azure Security Center is enabled.	Security management system that strengthens the security posture of your data centres, and provides advanced threat protection across your Azure workloads in the cloud.	Protection is automatically re-enabled.
Azure Defender is part of the Azure Security Center and also be enabled.	Alerts fire when Defender for Identity is not enabled in an Azure account.	Protection is automatically re-enabled.
Enable Azure Bastion or Just in Time (JIT) for VM access for new services.	Requests are logged in Azure Activity Log, to monitor and audit access.	Protection is automatically re-enabled.

Firewall

Leverage Azure for protection of your web applications from common exploits and vulnerabilities.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Web Application Firewall (WAF) is enabled.	Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.	Protection is automatically re-enabled.
Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources.	Centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.	Protection is automatically re-enabled.

Monitor

Leverage the Azure solution for collecting, analysing, and acting on telemetry from your cloud and on-premises environments.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Monitor is enabled within all subscriptions, all of the time.	Alerts fire when Monitor is not enabled in an Azure resource.	Monitor is automatically re-enabled.

Advisor

Leverage Azure's native configuration activity audit platform to capture what changes are being made to Azure configurations.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Advisor is enabled within all accounts, all of the time.	Alerts fire when it identifies new and available recommendations.	Advisor is automatically scanning the estate for vulnerabilities and areas of concern. Monitor them and review. Security or high impact alerts should be remediated and escalated to senior management.

Regions

Do not use Non-UK Azure regions for strategic compliance and performance reasons.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
An Azure subscription create resources outside of Azure UK regions.	Alerts fire when non-UK resources are created, to both the infrastructure teams and resource creator.	Non-UK resources are automatically and forcefully shut down after 12 hours.

Encryption

Leverage native Azure configuration options to make reasonable efforts to protect data.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Azure Storage Service Encryption - protect and safeguard your data and meet your organisational security and compliance commitments.	Blob Storage without suitable encryption enabled are alerted to the resource creator and account owner.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting, Cyber Security and Cyber Security.
Manage Encryption for data storage.	Storage without suitable encryption enabled is alerted to the resource owner and account owner.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting, Cyber Security and Cyber Security.
Key Vault - Provides security solution and works with other services by providing a way to manage, create, and control encryption keys.	Azure Key vault triggers events when the status of a secret stored in the key vault has changed.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting, Cyber Security and Cyber Security.

Public / 'World' Access

Ensure that public access to Azure data storage and compute is intentional, to avoid the 'leaky bucket' problem, and to aid attack surface minimisation.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
All Azure Data Storage objects should be not world (public) readable unless specifically intended to do so.	Data Storage objects are programmatically reviewed (including 'open' ones) against the source infrastructure-as-code, if there is a mismatch the resource creator and the Azure account owner are notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and Cyber Security. After 7 days, the Data Storage object permissions are forcefully and automatically changed to remove 'world' access.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
Compute instances should not be directly accessible from public networks unless through specific intentional design and should be behind a firewall (Azure based technology). It be truly exceptional for common service ports (for example, TCP80 or TCP443) to be served directly from compute resources.	Compute instances are programmatically reviewed to ensure they are not internet-accessible unless explicitly designed and documented to be so. If there is a mismatch the resource creator and the Azure account owner are notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and Cyber Security. After 7 days, the relevant security groups are forcefully and automatically changed to remove 'world' access.

Implementation

Infrastructure as Code (IaC) is the preferred method for initiating Services to encourage swift and predefined deployment.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
All Azure Services be defined in a IaC format.	Ensure IaC is maintained as reflects the current service.	7 days to correct and replace IaC data.

Tagging

Assigning tags to Azure resources is essential in creating a well-organised and transparent classification, and achieving significant cloud cost optimisation. When implemented, this practice can provide a consistent basis for applying policies across the organisation.

What be in place	Monitoring	Resolution or escalation if baseline is broken or violated
All Azure Assets be Tagged.	Report created to show missing Tags for relaying to Service Owners	Best Practice to apply.

Information security incident management

Management of information security incidents and improvements

IT Security Incident Management Policy

Related information

Technical Controls Policy on page 30

How to use this policy

This policy is for all users and is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This policy describes what is needed to manage an IT Security Incident.

Information is listed beneath the following headings:

Security Team

In this policy, ' Security Team' refers to all the security teams within the .

The Security Team are responsible for:

- incident ownership, monitoring, tracking and communication
- sanctioning enhanced monitoring where appropriate
- updating the incident management database
- analysing security incidents as required
- initiating a forensic investigation (in accordance with the IT Investigations - Planning and Operations Policy)
- providing progress reports to relevant parties

To contact the Security Team, send an email to .

Policy statements

This policy refers to the Policy Statements, **POL.IMP.001** to **POL.IMP.014**.

POL.IMP.XXX indicates the specific policy statement to be adhered to.

What is IT security management?

IT Security Incident management is the ability to react to IT security incidents in a controlled, pre-planned manner.

Preparation and planning are key factors to successful information security management. This policy sets out good practice for dealing with IT security incidents.

Definition of an IT Security Incident

A security incident is defined by the National Cyber Security Centre (NCSC) as:

- a breach of an IT system's security policy in order to affect its integrity or availability
- the unauthorised access or attempted access to an IT system

An IT incident may result in sensitive information being exposed, which might compromise business delivery or the Data Protection Act.

An incident might also cause harm or damage to individuals or organisations and result in operational disruption or reputational damage to the .

All staff be aware of the definition of a security incident and how to report it.

Incident Response

An incident response is the action taken when a security incident is detected or reported.

Responding to an incident requires informed decisions, taken as part of a consistent approach that is designed to reduce the consequences of the incident.

The process to respond to an incident be described in detail in an Incident Response Plan.

POL.IMP.001: Each IT system and service have an IT Security Incident Response Plan.

The IT Incident Response Plan and Process Guide has information on what to include in a Response Plan.

Types of Incidents

Types of IT Security related incidents include:

- breaches of the IT Security Acceptable Use Policy
- detection of malicious code such as viruses and malware
- network attacks or Denial of Service (DOS) attacks
- scanning and probing of a network, which might consume significant network resources
- the discovery of a new network vulnerability
- release of a patch or software update which is considered critical or an emergency
- a penetration test on a live operational IT system that reveals critical vulnerabilities
- unauthorised access to an IT system
- personal data incident due to accidental or deliberate loss or release of personal information
- any alert or activity report generated by an IT system that proves to be a real security alert

Incident Detection and Reporting

Security incidents may be discovered by:

- protective monitoring solutions
- incident reports by staff
- third-party reports to the
- breaches of IT Security Policy detected by an IT system
- data surrounding IT security incidents or suspected IT security incidents can be captured and monitored for suspected malicious activity or breaches of security

POL.IMP.002: All IT Security incidents or suspected incidents be reported to the IT Service Desk as soon as they are identified.

POL.IMP.003: All IT Security incidents involving personal data be reported to the Data Protection Team.

The Security Team is responsible for maintaining a database of IT Security incidents across IT systems.

This database contains:

- security incident reports
- the status of all reported security incidents and any actions taken to mitigate them

Further guidance on how to report a security incident.

Incident Categories

Security incidents are categorised to assess their impact and required level of escalation.

The three categories are:

- Low impact
- Medium impact
- High impact

POL.IMP.004: All IT Security incidents be categorised by the incident response team.

An IT incident may need to be recategorised if there are changes to the nature and impact of the incident.

Low impact incident

Low impact incidents are typically minor events such as a low-level breach in IT Security or a short-term loss of an IT service.

Medium impact incident

Medium impact incident are typically caused by:

- disregard for the IT Security Policy leading to a minor breach in security or the potential of data loss
- inappropriate use of IT assets
- theft or loss of data from an IT system that does not contain any personal information and is not protectively marked
- damage to an IT asset that impacts its usability
- connecting unauthorised equipment to an IT system
- prolonged or permanent failure of an IT system
- prolonged set of unsuccessful attempts to scan an IT network or instigate a denial of service attack
- a new critical security vulnerability in an IT system
- localised report of malicious code such as a virus on a terminal

High impact incident

High impact incidents require immediate escalation to the relevant Senior Information Risk Owner (SIRO), the Security Team, and the Data Protection Team if personal data is involved.

High impact incidents may require forensic investigation. There is more information on this in the IT Investigations - Planning and Operations Policy.

High impact incidents are typically caused by:

- malicious activity or espionage
- an incident that attracts media coverage
- intrusion into an IT network
- widespread malicious code attacks
- the theft or loss of personal or protectively marked data from an IT system

Escalations

If an incident needs to be escalated, it follow the chain of command through the incident response command structure.

The exact chain of escalation be outlined in the IT system's Incident Response Plan.

A typical command chain might be from the incident manager to the Major Incident Management team, to the relevant SIRO to Chief Security Officer (CSO) to Ministerial response.

Reasons for escalation might include:

- issues of national security
- if the incident is receiving media coverage
- if the incident has caused harm to a member of staff or public
- the has suffered reputational damage
- a requirement to report to another Department or central management function
- significant actual or potential loss of personal information where the Information Commissioner’s Office and Cabinet Office need to be informed

POL.IMP.005: Each IT Security Incident Response Plan include a pre-arranged escalation path, where each stakeholder is named and is aware of their role. Contact the Major Incident Management team if you need help creating documented escalation paths.

Incident Management Stakeholders

There are likely to be both internal and external stakeholders involved in incident management and response.

These will vary depending on the specific IT system or service.

POL.IMP.006: All staff report any actual or suspected incidents, including breaches of Security Policy, to their line manager and to the IT Service Desk.

POL.IMP.007: As part of operational readiness, Each SIRO ensure that each IT system or service under their remit has an IT Security Incident Response Plan. A guide for writing a plan is available in the IT Security Response Plan and Process Guide.

POL.IMP.008: All High impact IT Security incidents and any IT Security incident involving personal data be reported to the SIRO for your business area.

POL.IMP.009: All IT Security incidents involving the suspected or actual loss, theft, or compromise of an Information Asset be reported to the Information Asset Owner (IAO).

POL.IMP.010: If the IT Service Desk receives a report of a security incident, this be reported to the Security Team.

Investigations

The Security Team is responsible for the investigation of all IT Security incidents.

If legal or disciplinary proceedings require evidence to be gathered, a forensic investigation may be needed. The IT Investigations - Planning and Operations Policy gives more information.

POL.IMP.011: The Security Team maintain documentation on investigations undertaken.

POL.IMP.012: Any investigation of an IT Security incident and the events surrounding it be reported to all relevant stakeholders.

System Recovery

Following an IT Security incident, the IT system, services or any compromised assets be restored to business as usual (BAU).

If IT systems or services are restored using backups, the systems or services being restored pre-date the incident and contain any weaknesses that could be exploited further.

POL.IMP.013: The IT Security Incident Response Plan show how an IT System or service will be restored or recovered following an IT Security incident. The method used to restore or recover an IT System be captured in the system's disaster recovery plan.

The IT Disaster Recovery Plan and Process Guide has more information.

Lessons Learned

Once the cause of an IT Security incident has been identified steps be taken to make sure it will not happen again.

A report be prepared that describes:

- the incident
- the investigation
- the actions taken to restore the IT system or service to BAU
- all lessons learned

Lessons learned include action points on how to improve the business systems to reduce the likelihood of the incident re-occurring.

This report be sent to the SIRO who is responsible for forwarding it to all relevant stakeholders.

POL.IMP.014: For each Medium and High impact IT Security incident, a report be prepared, to include:

- a description of the incident
- a description of the incident investigation and its outcome

- mitigations and actions taken to resolve the incident
- any lessons learned and recommendations made

Lost devices or other IT security incidents

This guidance applies to all staff and contractors who work for the .

Related information

Laptops on page 148

What to do if your device is lost, stolen, or compromised

If data or information is lost or compromised, you should always report it as a data incident.

Note: You can help reduce problems by making sure that devices used for tasks are always shut down before leaving Government premises. Locking a laptop, or 'putting it to sleep' is not completely secure. A lost or stolen laptop can be accessed more easily if it is only locked or sleeping. A shut down makes sure that all security measures are in place, such as full disk encryption.

If you think your device is lost, stolen, 'hacked', or in some way compromised, you must:

1. Contact your . The analyst will ask the relevant questions and note responses on the ticket.
2. Tell your line manager as soon as possible.
3. For a lost or stolen device, contact the Police and make sure you get the incident reference number.

Summary

Find out more about how to report a security incident.

Information security aspects of business continuity management

Information security continuity

IT Disaster Recovery Plan and Process Guide

How to use this plan and process guide

This guide for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This plan and process guide is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This guide gives information on how to create and develop an IT Disaster Recovery Plan for your IT system or service.

The National Cyber Security Centre (NCSC) also offers guidance on how to effectively detect, respond to and resolve cyber incidents.

Business Impact Assessment

The service or system owner carry out a Business Impact Assessment (BIA) in order to:

- get an overview of the Business as Usual (BAU) functions for the IT system or service
- get an understanding of the business criticality of the service the IT system supports
- calculate a Recovery Point Objective (RPO), this is the maximum amount of data the business can afford to lose during a disaster
- calculate a Recovery Time Objective (RTO), this is the amount of time before the disaster begins to seriously impede the flow of normal business operations

Suggested content

Disaster recovery plans are specific to each individual IT system or service. They are intended to offer guidance to every listed role when responding to an incident.

When deciding the content of a Disaster Recovery Plan for an IT system or service, a useful start is to identify every potential disaster that may affect the system or service, together with procedures to resolve each one.

Each Disaster Recovery Plan include:

- the point at which the recovery plan be used
- a clear and detailed process to recover the IT system to BAU
- a list of key roles and a description of their responsibilities - each role have at least two sets of contact details
- a list of internal and external stakeholders to be contacted as soon as the incident happens, each stakeholder have at least two sets of contact details
- a communication list of everyone who needs to be contacted, together with the chains of communication that be followed
- a list of people who can undertake the role of recovery manager
- a series of steps to follow in order to mitigate the incident
- a list of criteria needed to initiate a forensic investigation, and the role(s) responsible for it
- clear instructions on how to escalate to a higher level of incident response, to include names and contact details and the reason for escalating the incident
- methods to maintain business continuity whilst the IT service is unavailable
- a process to identify and capture lessons learned during the incident
- the requirement for a written report for medium and high impact incidents

All plans be stored securely both online and offline. Roles and stakeholders mentioned in the plan know of its location and be able to access it.

Reviewing and testing

Disaster Recovery Plans be reviewed regularly, and updated if there have been any changes to systems or services, personnel, or communication chains.

Plans be tested and practiced regularly to help familiarise each of the roles with their responsibilities within the response process.

This is not an exhaustive list. If you need support in creating a plan, please contact the Service Operations Centre (SOC) and the Major Incident Team.

IT Disaster Recovery Policy

How to use this policy

This policy is for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This policy is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This policy describes what is needed to recover from an IT Disaster Event.

Information is listed beneath the following headings:

Policy Statements

This policy refers to Policy Statements, **POL.ITDR.001** to **POL.ITDR.014**.

POL.ITDR.XXX indicates the specific policy statement to be adhered to.

What is an IT disaster event?

An IT disaster event is any incident that causes actual or potential loss of availability or integrity of an IT system, which results in the IT system being unable to function during business as usual (BAU) operations.

What is IT disaster recovery?

IT disaster recovery is the planned response to a disaster event which will restore an IT system to BAU operations.

IT Disaster Recovery Plan

An IT Disaster Recovery Plan lists the actions to be taken to recover an IT system from a disaster event, together with a list of key roles and their responsibilities.

POL.ITDR.001: Each IT system have an IT Disaster Recovery Plan.

The IT Disaster Recovery Plan and Process Guide describes the information to include in a Disaster Recovery Plan.

Roles and Responsibilities

POL.ITDR.002: All Disaster Recovery Plans contain an up to date list of roles and responsibilities.

Each role have a name, with at least two sets of contact details.

POL.ITDR.003: All staff who are listed in a Disaster Recovery Plan be aware of their role and its responsibilities.

The list of roles and responsibilities include internal and external stakeholders, together with everyone listed on the communications list.

The list of roles and responsibilities align with the Incident Management Plan (IMP).

A variety of individuals and teams may be responsible for business and IT service continuity, and escalation in case of a disaster. These may include:

- Executive Committee
- Senior Information Risk Owner (SIRO)
- Chief Security Officer (CSO)
- Information Asset Owner (IAO)
- Service Operations (SO), which includes the Major Incident Management Team and the Security Operations Centre (SOC)
- IT Service Continuity Management

A Disaster Recovery plan include the relevant escalation process through the teams and individuals listed for each IT system.

Planning

An IT Disaster Recovery Plan supports the decisions and steps taken to reduce the effects of disasters and identifies the steps needed to recover IT systems back to BAU.

An IT Disaster Recovery Plan :

- contain identified risk scenarios and strategies to recover from them
- describe the circumstances in which the plan is invoked.

Business Impact Assessment

A Business Impact Assessment (BIA) be undertaken to identify the key disaster recovery requirements of the assets, services, and business processes supported by a specific IT system.

The BIA contain:

- a Recovery Time Objective (RTO): the time between a disaster event occurring and full IT systems and services being restored
- a Recovery Point Objective (RPO): the period of time during which the business can tolerate data loss

POL.ITDR.004: A Disaster Recovery Plan contain an RTO and RPO. The plan may contain more than one of these depending on the system.

POL.ITDR.005: Any disaster recovery action ensure that the IT system can recover from a disaster within the RTO recorded in the BIA.

POL.ITDR.006: Any disaster recovery action ensure that the IT system can recover from a disaster within the RPO recorded in the BIA.

Testing and Readiness Review

An IT Disaster Recovery Plan be tested regularly to ensure that:

- the plan remains fit for purpose
- the plan reflects all changes in personnel and updates to system information
- everyone with a role in the plan knows their responsibilities

POL.ITDR.007: Each IT system have its IT Disaster Recovery Plan tested before commencing live operations.

POL.ITDR.008: All IT Disaster Recovery Plans be tested at least annually, and after significant update to an IT system. The testing schedule be outlined in the IT Disaster Recovery Plan.

POL.ITDR.009: The IT Disaster Recovery Plan be reviewed after each test and updated as required to ensure it is fit for purpose.

POL.ITDR.010: Each IT Disaster Recovery Plan define the circumstances when the plan is to be invoked.

Reporting and Alerting

The reporting and alerting structure of an IT Disaster Recovery Plan align with that of the corresponding IT Security Incident Response Plan.

Every stakeholder that needs to be informed, be listed as a key contact within the plan.

POL.ITDR.011: The reporting and alerting structure within an IT Disaster Recovery Plan align with the relevant IT Security Incident Management Plan and Business Continuity Plan. Responsibility for business continuity resides with the SO.

Recovery and Review

The process to recover from a disaster event ensure that security vulnerabilities are not introduced or re-introduced during the restoration process.

POL.ITDR.012: Each IT Disaster Recovery Plan contain pre-defined and tested processes and procedures to restore an IT system or services, which has been disrupted or disabled during a disaster event.

POL.ITDR.013: Each Disaster Recovery Plan describe in detail the procedures to enable an IT Security System return from recovery mode to BAU.

Lessons learned be collated in an after-action report and be fed back to appropriate stakeholders.

POL.ITDR.014: Following a disaster incident, an after-action report be produced, which contains:

- all lessons learned
- actions to be taken to update processes and plans

IT Investigations - Planning and Operations Policy

How to use this policy

This policy is for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This policy is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

Policy Statements

This policy refers to Policy Statements, **POL.POP.001** to **POL.POP.015**.

POL.POP.XXX indicates the specific policy statement to be adhered to.

IT Forensics

IT forensics is the collection, storage, analysis and preparation of digital evidence that might be required in legal or disciplinary proceedings,

Data used in a forensic investigation be collected, preserved and analysed using systemic, standardised and legally compliant methods.

This will ensure that data gathered is admissible as evidence in a legal case, dispute or disciplinary hearing relating to an IT security incident.

There are two types of forensic investigation:

- proactive forensic monitoring - as part of an indentified security control
- reactive investigation - where a suspicious incident has been identified or reported

A forensics investigation be carried out:

- if an area needs proactive monitoring to enable forensic investigation
- if a business function makes a request via incident management escalation channels, to gather forensic evidence.
- if an investigation is requested as part of the IT security incident management process
- if requested as part of a leak investigation.

POL.POP.001: Each IT system or IT domain be covered by a Forensic Readiness Plan.

POL.POP.002: Each Forensic Readiness Plan include:

- an assessment of the risk management benefits
- authorisation from the IT Security Team and Senior Information Risk Officer (SIRO)
- a corresponding IT security incident management plan

Risk management benefits include risk assessments and cost-benefit-analysis, which will determine if an investigation is viable from a risk and cost perspective.

POL.POP.003: Forensic investigations in support of leak investigations be requested by the individual responsible for the leak investigation.

Integrity of Digital Evidence

POL.POP.004: Each forensic investigation be guided by the principles set out by the ACPO guidelines issued by the National Police Chiefs' Council (NPCC).

The integrity of data, which subsequently relied upon in court, be maintained throughout the forensic investigation process.

Any person accessing data as part of an investigation be competent to do so and able to justify the relevance and implications of their actions.

Each investigation be documented clearly and leave an audit trail that will enable a third-party to examine each process and replicate the findings,

The person leading the investigation is responsible for ensuring that all methods used are carried out in accordance with the law.

Investigations be conducted in line with policies.

Evidence Collection and Storage

Security teams be able to monitor systems to detect and respond to potential security incidents. If an incident needs to be investigated further, forensic tools be used to assess and gather evidence.

The Forensic Investigation Owner (FIO) is responsible for the collection and management of digital evidence.

An external organisation conduct the investigation on behalf of the .

Each item of evidence collected be managed according to the relevant Forensic Readiness Plan.

POL.POP.005: Each Forensic Readiness Plan include a process for the collection and storage of digital evidence, to include provision for where this task is conducted by an external organisation.

POL.POP.006: All users of an IT system be made aware that their access is monitored, and that IT forensic techniques be used to capture evidence as part of an investigation into an IT security incident.

POL.POP.007: A Forensic Readiness Plan contain clearly defined procedures and methods for conducting a forensic investigation. The be able to resume business operations following an IT security incident. Any forensic investigation be conducted in a manner that enables the restoration of IT services.

POL.POP.008: A Forensic Readiness Plan consider business continuity arrangements to ensure that essential functions are able to be restored. Digital evidence be handled carefully in order for it to remain admissible.

POL.POP.009: Each forensic investigation have a clearly documented chain of custody for all digital evidence.

POL.POP.010: The Security Team is responsible for the integrity of digital evidence. Each forensic investigation have a named FIO who is responsible for the investigation and management of digital evidence.

POL.POP.011: Any investigative action taken on a piece of evidence be captured and recorded. This record include details of the action taken and the person responsible for undertaking that action.

POL.POP.012: Admissibility of evidence in a court of law depends on how the evidence was captured. Before capturing any evidence, advice be sought from the legal team and forensic investigation provider.

POL.POP.013: Each Forensic Readiness Plan include details of how to securely dispose of evidence when it is no longer required. This conform with Secure disposal of IT equipment.

Legal Requirements

Investigations of electronically stored information within the conform to the latest legal and regulatory guidelines.

BS 10008:2022 provides information on the collection of electronically stored information as evidence.

POL.POP.014: During each forensic investigation, methods used to capture digital evidence be in accordance with BS 10008:2022.

Reporting and Communication

Each IT Security Incident Management Plan contains a communication plan and an escalation plan that be followed when responding to an IT Security incident.

The IT Security Incident Response Plan and Process Guide gives more information.

For major incidents it might be necessary to consider escalating the forensic investigation process to an external body. This might be:

- Law Enforcement
- National Cyber Security Centre (NCSC)
- Cabinet Office
- legal advisors
- Other Government Agencies as required

POL.POP.015: Each Forensic Readiness Plan include the reporting structure and escalation path for internal and external teams and the individual responsible for managing the incident. This be consistent with the corresponding IT Security Incident Response Plan and Process Guidea. The forensic investigation process enable the chain of evidence to be passed to outside agencies, if required.

IT Security Incident Response Plan and Process Guide

How to use this guide

This guide is for all users and is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This guide gives information to help create and develop an IT Incident Response Plan for your IT system or service.

The also offers guidance on how to effectively detect, respond to and resolve cyber incidents.

Suggested content

Incident response plans are specific to each individual IT system or service.

When deciding what should go into an Incident Response Plan for an IT system or service, a useful start is to identify every potential incident that might affect the system or service, and list the ways to resolve each one.

Each Incident Response Plan include:

- a list of key roles together with a description of their responsibilities - each role have at least two sets of contact details
- a list of internal and external stakeholders to be contacted as soon as the incident happens, each stakeholder have at least two sets of contact details
- a communication list of everyone who needs to be contacted, together with the chains of communication that be followed
- a list of people who can undertake the role of incident manager
- a series of steps to follow in order to mitigate the incident
- a method to identify the need for forensic investigation, and the role responsible for invoking it
- clear instructions on how to escalate to a higher level of incident response, to include names and contact details and the reason for escalating the incident
- a detailed process to recover the system to business as usual (BAU)
- a process to identify and capture lessons learned from the incident
- the requirement for a written report for medium and high impact incidents

All plans be stored securely both online and offline. Roles and stakeholders mentioned in the plan know of its location and be able to access it.

Incident response plans are intended to be flexible guides to help every role listed to respond to an incident.

Reviewing and testing

Incident Response Plans be reviewed regularly, and updated if there have been any changes to systems or services, personnel, or communication chains.

Plans be tested and practiced regularly to help familiarise each of the roles with the response process.

This is not an exhaustive list. If you would like support in creating a plan, please contact the Service Operations Centre (SOC) and the Major Incident Team.

Compliance

Compliance with legal and contractual requirements

Data destruction

Data Destruction

'Data destruction' is the process of erasing or otherwise destroying data stored on virtual/electronic or physical mediums such as, but not limited to, printed copies, tapes and hard disks in order to completely render data irretrievable and inaccessible and otherwise void.

The base principle

For legislative, regulative, privacy and security purposes, it **must** be possible to decommission and delete (irreversibly 'erase' or 'destroy') data and confirm to a degree of relative confidence it has been completed.

Data should be erased from all related systems, such as disaster recovery, backup and archival, subject to reasonable data lifecycle caveats.

Destruction standards

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning
- NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation
- Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): https://www.pcisecuritystandards.org
- DIN: http://www.din-66399.com/index.php/en/securitylevels

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

Data lifecycle caveats

Automated systems involved in data management and associated lifecycles may not be capable of immediate destroying data on demand.

Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

There is generally no need to attempt to manually delete such data prior to the automated retention lapse as long as it is ensured that if the data is restored prior to data destruction it is not processed.

It is important that the final expected data where all data lifecycles will have completed to be readily identifiable with high confidence.

Definitions

The current draft of the definitions that are required by the current draft short and long format data destruction clauses.

Definitions to be added into definition contract schedule

Data Destruction - Data destruction is the process of erasing or otherwise destroying data or information whether in physical form (such as printed paper) or stored on virtual/electronic or physical mediums such as, but not limited to, tapes and hard disks; the purpose is to render data completely irretrievable and inaccessible, and therefore void.

Supplier - ?

Authority - ?

Buyer - ?

Data Process/Processing - means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Long format clause

The current draft of the commodity long format data destruction clause.

`Highlighted` words indicate potential requirement for contextual change, requirement of definition and so on.

Clause

1. Data Destruction
    a. The `Authority` requires the `Supplier` to ensure that `Data Destruction` has been adequately completed at the natural end and/or termination of contract as per `Schedule XX`.
    b. The `Supplier` shall take all reasonable commercial measures to ensure Data Destruction is an irrevocable action to prevent the reconstitution of data, in alignment with methods described in `Appendix XX`.
    c. The `Supplier` shall notify the `Authority` when data destruction has taken place, including the final date by which such destruction shall be complete in the case of scheduled data destruction or natural data management lifecycles such as through automated backup or disaster recovery systems.
    d. Where data cannot be immediately destroyed, access control methods must be put in place to limit the ability the ability for `Data Processing` until data destruction can be completed.
    e. The `Supplier` shall provide evidence of data destruction on request from the `Authority`, including but not limited to, copies of third-party data destruction certificates, copies of internal policy and process documents in relation to data management and data destruction.
    f. The `Supplier` shall notify the `Authority` within `24 (twenty-four) hours` of identification of unsuccessful or incomplete data destruction.

Long format appendix

The current draft of the commodity long format data destruction appendix. The appendix is a dependency of the long format clause itself.

`Highlighted` words indicate potential requirement for contextual change, requirement of definition and so on.

Appendix

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning

- NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation
- Payment Card Industry Data Security Standard (Data Destruction): https://www.pcisecuritystandards.org
- DIN: http://www.din-66399.com/index.php/en/securitylevels

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific `Authority` guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific `Authority` guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimetres squared with a maximum strip width of 6 (six) millimetres

The required outcome is to ensure that `Authority` data is inaccessible by any reasonable commercial and resourced means (such as commercially available data recovery services).

Short format clause

The current draft of the commodity short format data destruction clause.

`Highlighted` words indicate potential requirement for contextual change, requirement of definition and so on.

Clause

The `Supplier` shall return all `Authority` Data in a machine-readable non-proprietary format defined by the `Authority` within `30 (thirty)` calendar days of the end of the contract.

The `Supplier` must also state, ensure and warrant the final calendar date by which any associated data management lifecycle system(s) will be complete, including the manual or automated data destruction at the end of such period. Such data management lifecycle(s) may include, but are not limited to, the `Supplier`'s supply chain and/or Data Processors, backup system(s) and/or disaster recovery and business continuity system(s). The `Authority` retains all applicable rights to instruct the `Supplier` to destroy all `Authority` Data according to the terms of this `[G-Cloud]` contract.

The `Supplier` is required to ensure adequate and complete Data Destruction of `Authority` Data, including any relevant and associated non-proprietary `Supplier` Data or work product stemming from the `Buyer` Data that the `Supplier` has not been otherwise permitted to retain or use.

Data Destruction must follow applicable guidance from the UK National Cyber Security Centre (NCSC) and/or the Payment Card Industry Data Security Standard (PCI-DSS) and/or DIN 66399.

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific `Authority` guidance: the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific `Authority` guidance: paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimetres squared with a maximum strip width of 6 (six) millimetres.

Instruction and Confirmation Letter

The current draft of a templated data destruction letter, that may be issued by the to a supplier. The letter describes required actions and information, followed by a responsive declaration from the supplier.

Letter issued by

Background

For legislative, regulative, privacy and security purposes, it must be possible for Suppliers to decommission and delete (irreversibly "erase" or "destroy") data and warrant the same. Similarly, any storage media holding such data must be securely and comprehensively erased before reuse or disposal (such as at end-of-life).

An example of a data destruction obligation is where a Supplier (acting as a "Data Processor", as defined by Data Protection legislation) working on behalf of, or supplying services to, the (the "Data Controller", as also defined by Data Protection legislation). The Data Processor, including any sub-processor instructed or otherwise involved in Data Processing on the Data Processor's behalf, must comply with instructions from the Data Controller regarding data irrespective of any commercial contract or promise such as a Data Subject exercising the "right to be forgotten".

This document provides an acceptable data destruction baseline from the , and associated declaration. When followed completely, this baseline for data destruction is considered sufficient to comply with data decommissioning and disposable tasks (and corresponding supplier assurances) for material classified as under the UK HMG Government Security Classifications Policy (including sensitive personal data or sensitive commercial data within the same).

Data Lifecycle

The informally acknowledge that automated systems involved in data management and associated lifecycles may not be capable of immediate decommissioning data on demand. Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

The require positive confirmation of the final date by which these systems will have completed their data lifecycle tasks and data destruction will have been completed by.

Where data cannot be erased immediately, there must be methods in place to limit and constrain access to the data until the data lifecycle is complete or manual intervention can be made and subsequent data destruction assured.

The reserves all rights regarding instructions relating to data. This includes any need for immediate data destruction.

Standards

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning.
- NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation.
- Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): https://www.pcisecuritystandards.org.
- DIN: http://www.din-66399.com/index.php/en/securitylevels.

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

The required outcome is to ensure that data is inaccessible by any reasonable commercial and resourced means (such as commercially available data recovery services).

Supplier declaration

Please sign the following declaration and return this letter to the , keeping a copy for your own records. Should you have any queries, please contact the CISO via .

Return electronically. Electronic signatures or otherwise positive confirmation are accepted.

Chief Information Security Officer Ministry of Justice 102 Petty France Westminster, London SW1H 9AJ

Date: _____

We hereby confirm that all Ministry of Justice data, including non-proprietary data generated through the provision of Service, has been suitably, appropriately, and irreversibly destroyed in its entirety and rendered permanently inaccessible and void.

Data backup, including disaster recovery systems, will automatically conduct appropriate data destruction as part of an automated data life cycle on or before the _____ (Strike as applicable)

Anonymised and/or non-Personal Data has been retained for statistical analytical purposes only. We warrant compliance with all applicable data protection and privacy legislation in this regard. (Strike as applicable)

Contract/project reference: _____

For and on behalf of organisation: _____

Name: _____

Position: _____

Date: _____

Data security and privacy

Data Security and Privacy

We believe that our technology must keep data safe and protect user privacy.

Our digital projects contain important information. Serious data breaches might result if we fail to:

- protect information
- handle it correctly at all times
- dispose of it safely when it is no longer required

Breaches might cause:

- harm to individuals
- financial loss to the
- a loss of confidence in us as an organisation

For personal data, the EU General Data Protection Regulation (GDPR) and UK Data Protection Act (2018) apply. These make the consequences of data breaches very clear.

To follow the data regulation/legislation, we **must** ensure that:

- we protect data to the best of our organisation's capabilities
- we collect data only for described, lawful purposes
- we use data only for the described, lawful purposes

Related information

Email blocking policy on page 271

Why are security and privacy important?

Breaches can have an adverse effect the relationship between citizen and government.

Not only do we have a duty to protect citizens data, but the penalties for violations are also severe. Under the GDPR, serious infringements can result in fines of up to €20M.

We must apply appropriate security and privacy protection to all the information we hold and process, at all times.

We should treat all data as sensitive unless proven otherwise.

All our work must follow this ethos.

When this applies

This principle applies to **all** technology projects and business activities.

While GDPR applies only to personal information, all projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow guidelines unless exceptional and approved circumstances apply.

You can design your product to handle personal information correctly. There are a small number of extra steps you will have to take. Remember that personal data includes anything which might identify an individual. Even online identifiers, such as cookies, are personal data.

The Information Commissioner's Office (ICO) - the UK's independent regulatory office for data protection - has published guidance on how to determine what is personal data.

A Data Protection Impact Assessment (DPIA, formerly commonly known as a Privacy Impact Assessment or PIA) is required for all projects. There are some exceptions described by the ICO.

Data privacy

The provides services, guidance, and support for all aspects of data privacy and protection.

For example, they have protocols and procedures to help ensure acceptable use of personal information.

Data Security & Privacy Lifecycle Expectations

Following are a series of data security and privacy expectations of projects at various stages in their lifecycle.

These measures can help simplify and ease the burden of embedding data security and privacy at the heart of projects.

Pre-Discovery and Discovery

Assess the data security and privacy implications of the project requirements thoroughly. Do this as part of the broader work addressing the project's strategic imperatives.

In particular:

- From the start of the project, and throughout its duration, think about how data security and privacy might affect the functionality and delivery of the project.
- Consult with technical architects to help inform and enhance the ways of delivering the work, whilst continuing to ensure compliance.
- Discuss any problems or ramifications that arise with legal or business experts. Identify areas where the required data security and privacy compliance might cause issues for functionality.

Alpha

During this stage of the project lifecycle, internal and external (Cabinet Office / Government Digital Service) teams will perform service assessments. These will specifically check for aspects of GDPR/DPA18 compliance.

In particular:

- >That the majority of compliance considerations have been addressed at this stage.
- That the development team can say how their work ensures compliance.
- That the technical architecture choices can be tested against data security and privacy requirements. As an example, blockchain technologies might not be acceptable as they can prevent automated removal of information when it is no longer required.

Beta (Private and Public)

These are assessments performed as the service transitions from Private to Public availability. The assessments are again performed by internal and GDS teams. Use live systems for the assessments.

In particular:

- All manually actionable data security and privacy requirements must be met.
- Manual testing is expected.
- Automatic deletion is not required yet, because the service is unlikely to have enough data at this stage. However, plans and mechanisms for automatic deletion should should be in place.
- Data should be backed up exactly as expected for a live service.

Live

These are the final (Live) service assessments. They are again performed by internal and GDS teams.

In particular:

- Data sharing aspects might not yet be fully defined. Other consuming or supplying systems might not have established dependencies on the information shared.
- Some aspects of reporting might still need manual action. The newness of the system makes business MI requirements a work-in-progress.

Post-Live (Ongoing)

These are the tasks that enable the final aspects of security and privacy for your project.

In particular:

- The final automated tasks are ready. The project cannot close until these are done.
- Data security and privacy compliance checks move to an ongoing status. Reporting takes place as required to internal stakeholders or the ICO.
- Schedule and run regular data mapping exercises. These ensure full and current understanding of data flows to and from any organisations or systems that depend on the information.

Data Security & Privacy Triage Standards

Following are a series of common area guides from Digital & Technology Triage Standards.

Purposeful Capture of Data

Only collect or store data if it is relevant, and needed for a specific purpose or task.

Ensure that:

- Everyone on the team understands why specific data is collected and stored. They should be able to justify this, backed with legal reasoning, as required.
- Each product has a clear privacy notice, describing how any personal data is handled. The notice contains a clear description of what we will do with their information, why, and how. Write it in terminology the general public can understand.
- Using an individual's information is only for the specific purposes or processes for which it was captured. There should be no superfluous information stored.
- The privacy notice describes any use of information for management or reporting purposes. Anonymise any personal information used for these purposes. In other words, before use, remove any fields or data that could identify the individual.
- You justify any special categories of needed information. The Information Commissioner's Office (ICO) - the UK's independent regulatory office for data protection - has outlined a list of special categories.

Amending/Deleting Data

EU GDPR & the UK Data Protection Act (2018) requires that individuals agree to the handling and processing of their personal information. Many systems will need processes, to change, prevent, or stop handling personal

information. The process might be have to be manual. Quite apart from GDPR/DPA18, these capabilities are generally useful for all systems.

Ensure that:

- The system has a defined retention schedule. These are normally drawn up between the SRO and the legal team. They detail how long we can keep information in the system before we must delete it.
- The system can delete records automatically at the end of the retention period. It should also be possible to remove records manually if required.
- Decisions or processes made using an individual's information can be stopped upon request.
- Ensure that information can be amended or re-examined manually, if necessary.
- If deletion is not possible, the system must be able to strip all identifying information from the records. This should make it impossible to identify an individual. Anonymising data should make it fall outside of the GDPR remit. The privacy notice should also mention this.

Security / Architecture Considerations

Much of the estate architecture is ready for GDPR/DPA18, or transformation is already in progress. Current projects must also incorporate data security and privacy mechanisms for GDPR/DPA18 compliance. Guidance from technical architects is essential to help projects. Ensure that:

- You know where data for the system is stored. Ask which countries and jurisdictions hold the data. Check that the storage complies with GDPR/DPA18 requirements.
- The procedures to follow in response to a data breach are clear. Developed them with the help of the live service and cyber security teams.
- There is 100% confidence that data is backed up and protected against loss or other threat scenarios. Test and challenge this confidence frequently. Always test within the timescales defined in the retention schedule.
- The IA register lists the system. For potentially sensitive or risky data sets, check that the risk register also lists the system.

Sharing Information

Many systems depend on data from more than one source. For example, data might come from cross-estate and cross-government levels. This makes accountability for the data vital: who owns it, and who is responsible for it.

Acceptable information sharing involves two distinct perspectives:

1. Sharing with other systems. There must be public transparency and understanding about using the information. Similarly for any dependencies on the information. To provide this detail, create data maps with the help of the system technical architects. Make sure that the maps include correct links between the data controller who originated the information and any other processors of the data.
2. Sharing with other organisations. There must always be an auditable record of the agreement between the organisations. This could be part of a contract, a data sharing agreement, or other general memorandum of understanding. Review the record at regular intervals so that it still meets the user or business needs, and continues to be relevant.

Subject Access Requests

At any time, a person about whom we hold personal data can request a copy of all the information we hold about them. This is not a new requirement, and was part of original data protection legislation.

However, the £10 fee charged before is now waived. This makes it likely that there will be more Subject Access Requests in the future. Design your product to make it as simple as possible to perform Subject Access Requests quickly and easily. Authorised individuals from across all data storage locations should be able to respond.

Law Enforcement Directive (L.E.D.)

Some systems hold information about criminals or criminal offences. This is sensitive data. An additional regulation applies to them: the Law Enforcement Directive.

Affected systems must record whenever an individual record is viewed or amended. Keep this log for audit purposes.

Project Lifecycle Data Security and Privacy Expectations

When developing a system, there are some measures you can take that will simplify and ensure timely GDPR compliance.

Pre-Discovery and Discovery

Assess the data security and privacy implications of the project requirements thoroughly. Do this as part of the broader work addressing the project's strategic imperatives.

In particular:

- From the start of the project, and throughout its duration, think about how data security and privacy might affect the functionality and delivery of the project.
- Consult with technical architects to help inform and enhance the ways of delivering the work, whilst continuing to ensure compliance.
- Discuss any problems or ramifications that arise with legal or business experts. Identify areas where the required data security and privacy compliance might cause issues for functionality.

Alpha

During this stage of the project lifecycle, internal and external (GDS) teams will perform service assessments. These will specifically check for aspects of GDPR compliance.

In particular:

- That the majority of compliance considerations have been addressed at this stage.
- That the development team can say how their work ensures compliance.
- That the technical architecture choices can be tested against data security and privacy requirements. As an example, blockchain technologies might not be acceptable as they can prevent automated removal of information when it is no longer required.

Beta (Private and Public)

These are assessments performed as the service transitions from Private to Public availability. The assessments are again performed by internal and GDS teams. Use live systems for the assessments.

In particular:

- All manually actionable data security and privacy requirements must be met.
- Manual testing is expected.
- Automatic deletion is not required yet, because the service is unlikely to have enough data at this stage. However, plans and mechanisms for automatic deletion should should be in place.
- Data should be backed up exactly as expected for a live service.

Live

These are the final (Live) service assessments. They are again performed by internal and GDS teams.

In particular:

- Data sharing aspects might not yet be fully defined. Other consuming or supplying systems might not have established dependencies on the information shared.
- Some aspects of reporting might still need manual action. The newness of the system makes business MI requirements a work-in-progress.

Post-Live (Ongoing)

These are the tasks that enable the final aspects of security and privacy for your project.

In particular:

- The final automated tasks are ready. The project cannot close until these are done.
- Data security and privacy compliance checks move to an ongoing status. Reporting takes place as required to internal stakeholders or the ICO.

- Schedule and run regular data mapping exercises. These ensure full and current understanding of data flows to and from any organisations or systems that depend on the information.

Information security reviews

Standards Assurance Tables

The Cyber Security team have developed a 'Standards Assurance Table' (SAT) in the form of a Google Sheet template.

The SAT measures technology systems (and surrounding information governance) against the UK Cabinet Office Minimum Cyber Security Standard (MCSS) and UK National Cyber Security Centre (NCSC) Cloud Security Principles (CSPs).

For transparency and open-working purposes, a redacted copy of the Standards Assurance Table has been published. Please note, this is not the functional template used within the .

SAT Template

The SAT itself is written to be self-explanatory to a cyber security professional who is already aware of the MCSS/CSP and has a familiarity with information risk management concepts.

- Black labelled sheets describe the SAT and how it should be used
- Blue labelled sheets are the ones to complete
- Yellow labelled sheets are automatically calculated, providing reports based on the blue labelled sheet data
- Green labelled sheets offer help/guidance on SAT components

Key SAT concepts

The SATs have measures including "Objectives", "Evidence", "Confidence", an overall "Delta" (which is the most pertinent SAT output) and "Further Evidence Required", with supporting commentary.

The primary SAT purpose is to help assess a system against the MCSS/CSP. It is used to determine confidence whether or not the evidence demonstrates the system is compliant (or not).

Evidence is analysed to determine confidence that the evidence demonstrates the system meets (or does not meet) the standards. It also indicates the 'gap' (delta) between the system's posture according to said evidence and the standards.

Objectives

The MCSS/CSPs have been distilled into 39 objectives. The Assessor (normally a cyber security professional) completes the SAT by evaluating the target system against the objectives.

The categories used within the MCSS are discussed separately.

Objectives are templated. This means they can be added to but existing objectives must not be deleted or edit in-place.

Evidence

To avoid assessments that are ultimately anecdotal, the assessor will only rely upon written evidence.

Evidence can come in the form of transcribed conversations, diagrams, documentation or other auditable information about a system.

Evidence might not be directly related to the system itself but form a part, for example, where there is a wider document that is not system orientated but which describes who is relevant role holders currently are.

Evidence is described as being 'Held', 'Partial', 'Not Held' or 'N/A' (where the Objective is not applicable to the system being assessed).

Confidence

The assessor reviews the evidence and uses their professional opinion to indicate a Confidence Score.

The Confidence Score uses a scale from 0 (no confidence at all) to 14 (high level of confidence), or 'N/A' (where the Objective is not applicable to the system being assessed).

Delta

The Delta Rating is the resulting 'distance' between the assessed system posture against an Objective and the confidence of the same.

Mathematically, the final Delta Rating is N/A (where the Objective is not applicable to the system being assessed) or 0 to 14 (inc).

A wide delta (higher numerical value) indicates that the Objective is not met. A narrow delta (lower numerical value) indicates that the Objective is closer to being met.

The Delta Rating is automatically calculated as '14 minus Confidence Score'.

Further Evidence Required

The assessor indicates what further evidence *types* in their view are required based on the evidence they have thus far.

The Further Evidence Required (Help) sheet has a calculator which the assessor will use.

The data point is currently a unique number to assist with future automated analysis. The format and range of values for the data point is currently under active review and so subject to change without notice.

Understanding the Objectives, gathering evidence for the assessor

Teams/individuals responsible for the design, creation, implementation, support and maintenance of systems should have viable written evidence (regardless of format) that should be made available to various teams on request, for example, security or to internal audit.

Using the categories used within the MCSS as a basis, some indicative questions and documentation expectations are discussed in this guidance.

IDENTIFY

Possible documentation

- Team organisation charts
- Data Privacy Impact Assessments (DPIAs)
- Information risk management documentation (for example, RMADS)
- Information flow diagrams

Thought questions

- Who is responsible and/or accountable for the the system whether from an operational or budgetary perspective?
- Who is responsible and/or accountable for the information held inside the system?
- What security-focused work has been conducted recently (within the last year) on any suppliers and supplier systems to ensure they are safe for use/integration?
- Where is the system technically hosted?
- In what services or geographical locations does the system *store* data?
- In what services, geographical, or legal locations does the system *process* data?
- What are the consequences if the system is unavailable to users or data has been lost/corrupted?
- How do the consequences of unavailability change over time? (For example, after one hour, one day, one week, one month... permanent.)
- What changes - if anything - regarding business continuity / disaster recovery processes or plans if the system is unavailable or data has been lost/corrupted?

PROTECT

Possible documentation

- Data Privacy Impact Assessments (DPIAs)
- Information risk management documentation (for example, RMADS)
- Information flow diagrams

- Technical/system architecture documentation
- Penetration test / IT Health Check reports and remedial documentation
- Risk registers

Thought questions

- How does the system ensure only authorised people can use the system?
- How are system users managed for joiners, movers and leavers?
- How is the system's underlying software kept up to date for security software patching?
- How does the system protect itself appropriately and proportionately from attackers?
- What assurance is there that the system can protect itself from attackers over time, so it is secure now but also will remain secure in the future?
- How often has technical security testing been conducted? Where within the system?
- How does the system stay up to date using modern encryption to keep data safe?
- Does the system use multi-factor authentication (MFA, also known as 2FA)?
- For people who have access to the system, do they have all the right clearances in place? How is this assured?

DETECT

Possible documentation

- Information risk management documentation (for example, RMADS)
- Technical/system architecture documentation
- Penetration test / IT Health Check reports and remedial documentation
- Risk registers

Thought questions

- How does the system, and accompanying operational support teams, know/detect when the system is under attack?
- How is access to the system (both authorised and unauthorised) logged so retrospective investigations can take place to determine 'who did what when'?
- How is the required level of detail in logs determined? How long are log files retained?

RESPOND

Possible documentation

- Information risk management documentation (for example, RMADS)
- Technical/system architecture documentation
- Operational/support documentation

Thought questions

- What plans, processes or procedures are in place to respond to a detected cyber attack?
- How are these plans kept up to date and relevant?
- Does everyone who needs to know about these plans know about them?
- Has the plan been tested in the last 12 months?
- How are stakeholder communications handled during a security incident?
- How are external communications handled during a security incident for external parties, such as supervisory bodies, the NCSC or Cabinet Office?

RECOVER

Possible documentation

- Operational/support documentation
- Retrospective session notes

Thought questions

- What happens for business continuity / disaster recovery if the system is unavailable or data has been lost/ corrupted?
- Have these measures been tested in the last 12 months?

Risk Assessment

Risk Management

Infrastructure System Accreditation

Summary

Accreditation is the formal, independent assessment of an IT system or service against its Information Assurance (IA) requirements.

The Accreditation Framework explains how accreditation forms part of the wider Information Risk Management strategy, is owned by the business owners of the system, and is implemented in a proportionate, pragmatic, and cost-effective manner. The framework includes information about who is involved in accreditation, their roles and responsibilities, and the stages of accreditation and risk assessment.

Accreditation must be considered for any system that handles information relating to business or customers.

What is an IT Health Check, and why is it important?

An IT Health Check (ITHC), also known as a Penetration (Pen) Test, is an important component in the over-arching Security Assurance activities and one of several possible mechanisms used to provide confidence and assurance of the security baseline design.

An ITHC is a series of controlled ethical hacking tests and actions designed to deliberately identify and expose security vulnerabilities that might be present in IT solutions. The objective of scrutinising an IT solution in this manner allows the project and business teams to understand the risk exposure should it become compromised and formulate a remediation plan to mitigate and protect the systems and data that might reside in it.

When should an ITHC be considered?

There are 3 primary scenarios when an ITHC might be undertaken:

Introduction of new IT services

An ITHC at this phase of a project life cycle helps to establish the security baseline before the solution is made available for wider use. It provides the ability to act on any risks and issues identified whilst in a safe environment and reduces impact on others (users as well as systems) overall.

Changes to an existing IT baseline

Any major design change to an existing IT service should include a review for a new ITHC to determine that the baseline change does not introduce security risks. ITHC's are normally performed prior to formal release/rollout of the changes being made and therefore identification and mitigation plans can be established and undertaken in a safe environment.

Scheduled ITHC for existing IT services

As technology continues to evolve, it is important to understand the impact that this might have on existing solutions. Therefore, is it recommended that Product and Service owners work with the CAT Team (Cyber Assistance Team) to review existing IT solutions and plan to undertake an ITHC on an agreed schedule. This helps to re-assess the security baseline, remediate any risks and issues as agreed, and therefore provide ongoing protection of systems and data.

What can be tested?

The ITHC is performed by highly trained pen testing specialists, and (typically) by an external 3rd party ITHC service provider.

There are many types of penetration tests that can be applied, including but not limited to:

- Network and host configuration
- Web application
- Wireless network
- Client-server application
- End User devices such as laptops or mobile phones
- Social engineering
- Build configuration

Cloud Platforms

If the application or service you intend to test is hosted within a cloud platform service offering, such as Azure and AWS (Amazon Web Service), there are Rules of Engagement that you should be aware of. Information can be found for the following:

- Microsoft Azure: https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement
- AWS: https://aws.amazon.com/security/penetration-testing/

Further to this, the MoJ AWS Cloud Platform Team have produced additional guidance that can be accessed here: https://user-guide.cloud-platform.service.justice.gov.uk/documentation/other-topics/security-testing-and-ithc.html#security-testing-and-ithc

Vulnerability Scanning

A vulnerability scan is not the same as an ITHC however, it can be performed and used to help build on the overarching story of the product being tested.

A vulnerability scan is automated and is entirely software whereas an ITHC is conducted by trained, qualified professionals, and uses human interaction and human ingenuity to discover flaws that automated tools often miss.

Further information and guidance about vulnerability scanning can be found here: https://security-guidance.service.justice.gov.uk/vulnerability-scanning-guide/#roles-and-responsibilities.

Primary Points of Contact

The Cyber Assistance Team (CAT) Consultants are the primary points of contact for projects and Product/Service owners. The Consultants will work with the team to help ascertain the ITHC requirement and scope, as well as any forward schedule for ongoing ITHC requirements. You can contact the CAT Team directly to request Consultation support if one is not already working with your project already:

CyberConsultancy@digital.justice.gov.uk

How can I book an ITHC?

If you have a requirement to conduct an ITHC on your network and/or application, please complete and submit the New ITHC Request form:

New ITHC Request Form

The Cyber Security, Privacy and Live Service Delivery Team manage the engagement and planning coordination between yourself and the 3rd party ITHC Team. If you have any queries, you can contact the team via:

security@justice.gov.uk

Governance, workflow and timeline considerations
Timeline Consideration

It is recommended that an approximate timeline of 8 weeks is considered in your project plan to enable the planning and undertaking of the ITHC. Maturity, size, and complexity of the scope will influence this.

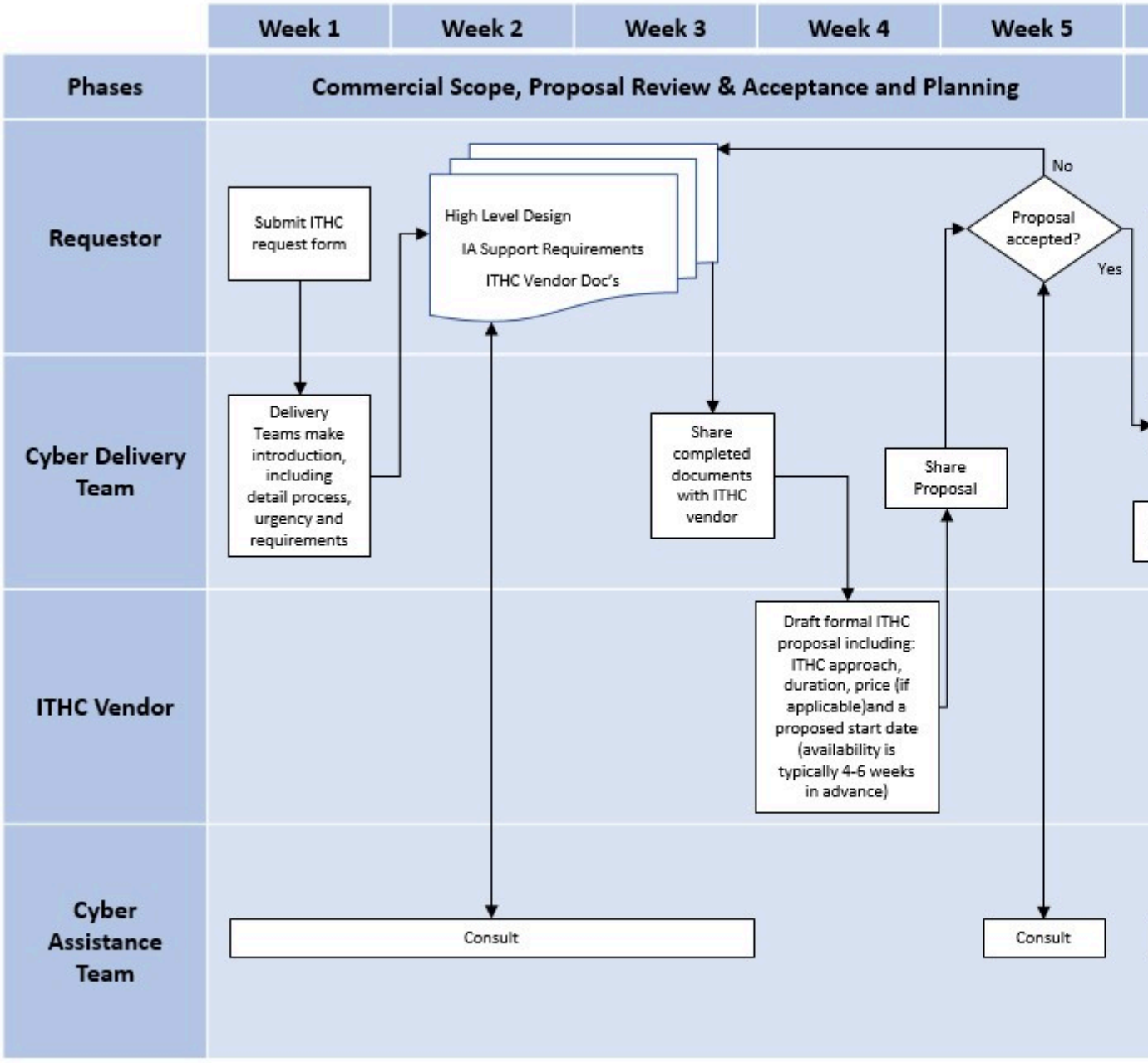
Scope Changes

Changes to scope can be reviewed and considered. However, there is a risk that this will affect delivery dates, ITHC Provider availability, and end quote price.

In scenarios where the formally agreed test dates are impacted, charges might be incurred for delays and cancellations.

It is strongly recommended that ITHC scope is understood and confirmed as much as possible, and prior to submission.

The following workflow aims to provide an overview as to the primary roles and action owners involved in the ITHC process:



How to reach us

Should you have any further queries about the ITHC process then please don't hesitate to contact the Cyber Security, Privacy, and Live Service Delivery Team:

security@justice.gov.uk

Risk Assessment Process

Risk Reviews

Information and the supporting processes, systems and networks are important and valuable assets. They are central to enabling the to perform its functions and provide services to the public, the legal professions, and other government departments and organisations.

Confidentiality, integrity and availability of information is essential to maintain the 's ability to provide efficient and effective services, maintain compliance with legal and regulatory requirements, and maintain its and the Government's reputation.

The and its information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, fire and flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

The 's dependence on its information systems and services means that there is always a possibility of technology-enabled security threats. Connections between the 's computer networks and public and other private networks, and sharing of information resources, further increase the difficulty of achieving and maintaining control.

It is essential that the identify its information security requirements. There are three main sources of these requirements.

- The legal, statutory, regulatory and contractual requirements that the , its partners, contractors and service providers have to satisfy.
- The principles, objectives and requirements for information processing that the and Government have developed to support their operations, for example the protective marking system and government baseline security standards.
- Assessed risks to the . Through risk assessment, threats to assets are identified, the potential business impacts of these threats are estimated, and the vulnerability to and likelihood of occurrence of the threats are evaluated.

Assessing information security risk

Security requirements are identified by a methodical assessment of security risks. Expenditure on security controls needs to be balanced against the business harm likely to result from security failures. Risk assessment is systematic consideration of:

- The business harm (the 'impact') which is likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.
- The realistic likelihood of such a failure occurring in the light of the threats to and vulnerabilities of the system, and the controls currently implemented.

Managing information security risks

The results of the risk assessment are identified risks and risk severities. These help guide and determine the appropriate management action, and priorities for managing information security risks. Risks with a high severity level would justify the expenditure of more resources to control them than risks with a low severity level.
Risk Management involves identification, selection and implementation of justified security and contingency 'countermeasures' to reduce risks to an acceptable level.

Countermeasures can act in different ways such as:

- Reducing the likelihood of attacks or incidents occurring.
- Reducing the system's vulnerability.

- Reducing the impact of an attack or incident should it occur.
- Detecting the occurrence of attacks or incidents.
- Facilitating recovery from an attack or incident.

Risk management requires a judgement about what is an acceptable level of risk. Although this is a business decision, it does require a thorough understanding of the nature of the risk and the effectiveness of the countermeasures implemented to manage the risk. For some systems or scenarios, specialist advice might be needed.

When taking risk management decisions, consideration must be given to the full implications of the decisions taken. Failure to implement some countermeasures might breach legal or regulatory requirements. This is unlikely to be an acceptable risk management decision. Failure to meet other countermeasures might breach Government information security standards; as a consequence it might not be possible to link the system with other systems. This might limit the usefulness of the system.

Consideration must also be given to what are tolerable financial losses, political sensitivities and adverse publicity. The cumulative effect of accepting high levels of risk should also be taken into account.

Information security in projects

Information security controls are considerably cheaper and more effective if incorporated at the system requirements specification and design stage. Information risk assessments must be part of the project process.

Ongoing information security risk management

Effective risk management does not end once a risk assessment has been done and the required countermeasures implemented. Checks need to be carried out to ensure that the countermeasures are being applied effectively. It is also important to carry out periodic reviews of security risks and implemented controls to:

- Take account of changes to business requirements and priorities.
- Consider new threats and vulnerabilities.
- Confirm that controls remain effective and appropriate.

The role of security in risk assessment and risk management

The security team can provide help in all areas of security risk management for systems. Examples include:

- Advice on risk assessments.
- Help with carrying out risk assessments.
- Assist with the risk management decision process.
- Help with creating and managing documentation compliant with standards.
- Assisting with mandatory Government risk assessments.
- Advice on compliance checking.

Glossary and Acronyms

Glossary

This information is a reference list of terms and abbreviations.

The NCSC has a comprehensive cybersecurity glossary available on its website.

Terms

2FA	Refer to Multi-factor authentication.
Authorised User	Any user of services covered as authorised by the .

Blue Team	The internal security defence team in an organisation. Within the , this work is performed by the Security Team.
Brute Force Attack	The application of lots of computer power, to try and perform a task using a huge number of values. Typically used to try out many passwords, to gain access to systems.
Business Continuity Plan (BCP)	A document that outlines the procedures in place for a business to continue to operate, despite an unexpected disruption to services. These disruptions might be things such as cyber attacks, pandemics, or natural disasters.
Credentials	Information used to prove someone's identity, to confirm that they really are who they say they are. Typically includes passwords, tokens, and certificates.
Critical infrastructure attack	Critical infrastructure refers to the physical and cyber structures, facilities, and systems that are essential for a country to function. Attacks on these resources would harm the physical security, economic security, or public health of the country.
Customer	Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term customers is also sometimes informally used to mean users, for example "this is a customer focused organisation".
Dark web	Generic name for encrypted online content that is not indexed by search engines. The information is only accessible with special software or tools.
Data breach	An incident where data is accessed in a non-authorised way.
Decryption	The reverse of an encryption process.
Distributed Denial of Service (DDoS) attack	Legitimate users cannot access computer services, because threat actors are overloading the service with requests. Also referred to as a Denial of Service (DoS) attack.
Digital footprint	A collection of data and information traces left behind by a user, as they do activities online. For example, all the things you've ever searched for on Google.
Double encryption ransomware	Refer to ransomware.
Encryption	The process of converting human-readable text into unreadable 'disguised' information, or 'ciphertext'. You can see it, but you can't understand it. Only someone with a decryption key can convert ('decrypt') the unreadable information back into human-readable form again.
Exfiltrate	The formal name for a technique used by threat actors and malware to surreptitiously copy and transfer data out of a system. This is data theft.
Exploit	A program or process that takes advantage of a vulnerability in a system to cause system problems, or to access or modify information without authorisation.

Incident	Any event which is not part of the standard operation of a service, and which causes, or might cause, an interruption to, or a reduction in, the quality of that service. A breach of the security rules for a system or service.
Incident Management	The process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to return the IT service to users as quickly as possible.
Insider threat	Any threat from current or former employees of an organisation who have inside information or authorised credentials that might be used to cause harm to the organisation, accidentally or maliciously.
Macro	A small program or script that automates tasks in an application, such as Microsoft Office. Might be used by attackers can use to gain access to, or harm, a system.
Malware	Malicious software. This includes things like viruses, trojans, worms, or any code that can have a negative impact on an a system.
Multi-factor authentication (MFA)	Use of two or more different components to verify a user's claimed identity. Typically an extra component, in addition to a password. MFA often uses an authenticator app or SMS text to deliver a single use code. Also Two-factor authentication (2FA).
Open Source Intelligence (OSINT)	Information gathered from public information. This includes data from social network accounts, company websites, and other openly available information sources.
Operational Security Team (OST)	Deprecated name for the Security Team within the . The Security Team help protect against cyber attacks, and help manage incidents. Sometimes referred to as the Blue Team. They can be contacted through email: .
Out of band check	An additional check performed using a different communication channel, to verify identity or intent. The check helps prevent phishing or social engineering attacks. For example, if you receive an email from a senior manager, asking you to perform an unusual task, you should want to check that the request is genuine. If you reply by email to the original request, that's an 'in band' check, and can't be trusted, because it's possible the manager's email has been compromised. But if you called the manager by mobile phone to check the request, that's using a different communication technology, so it's an out of band check. A threat actor would have to compromise both the manager's email and their mobile phone account to succeed in tricking you. For more detail on out of band checks, refer to this additional information.
Password	A secret string of characters, numbers, and often symbols. When used with a valid user ID, a password enables access to an account.
Patching	Applying updates to software or firmware to improve security and enhance functionality.

Phishing	Untargeted mass emails sent to many individuals. The email typically asks for sensitive information, or encourages you to visit fake websites, or to send money. For more information, refer to the phishing guide.
Problem	A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.
Problem Management	The process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimise the impact of incidents which cannot be prevented.
Process	A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process might include any of the roles, responsibilities, tools, and management controls required to deliver the outputs reliably. A process might define policies, standards, guidelines, activities, and work instructions if they are needed.
Ransomware	Malicious software that makes data or systems unusable by encrypting it and then demanding a payment from the victim to decrypt it. Double Extortion Ransomware exfiltrates the data before encryption and demands a ransom payment to stop the threat actor releasing the data to the public, as well as for decrypting the system.
Red team	This is an internal or external team that tests organisational security by simulating cyber attacks as realistically as possible. Together with the Blue Team, the team helps to improve the cyber defences of the organisation.
Resolution	Action taken to repair the fundamental cause of an incident or problem, or to implement a workaround.
Resolver Group	May include a wide range of IT teams, including support and development personnel, other Service Management Functions (SMFs), other units within the organisation, outsourcing providers, partners, and other third parties.
Service Desk	The single point of contact between the service provider and the users. A typical Service Desk manages incidents and service requests, and handles communication with the users.
Social engineering	Manipulating people into doing things or divulging information that is of use to a threat actor.
Tabletop	An exercise created to try out Business Continuity Plans (BCPs). These exercises create realistic scenarios, and play through a number of obstacles, to ensure organisations have robust BCPs.

Tailgating	An unauthorised individual forcefully or stealthily gaining access to a building, typically by entering immediately behind an authorised user.
Threat actor	A general term that encompasses all types of individuals and groups that use cyber methods to cause harm. This includes competitors seeking to steal information, cyber criminals attacking for political or monetary gain, accidental or malicious insider threats, spies, social and political activists, and assorted hackers.
Trend Analysis	Analysis of data to identify time related patterns. Trend analysis is used in Problem Management to identify common failures or fragile configuration items, and in Capacity Management as a modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.
Virtual Private Network (VPN)	An encrypted network created to allow secure connections for remote users.
Vulnerability	A weakness in software, a system, or process. A threat actor might seek to exploit a vulnerability to gain unauthorised access to a system.
Zero day (0day)	A vulnerability in a system that few people know about. threat actors can exploit an 0day to attack or affect data and systems.
Zero trust	The assumption that all requests and connections are potential breaches, and so must be verified and authenticated before being allowed.

Out of band checks

An out of band check is when an individual uses a different method of communication than the one the message came from. This method means that if one communication method is compromised, you quickly find out by using a different communication method to confirm validity. The likelihood of multiple communication methods for the same person or team being compromised is low.

Out of band checks are an easy method to confirm the legitimacy of communications and requests. They can confirm the identity behind a message or request, and they can confirm the validity of the message or request itself. Social engineering techniques and phishing tactics take advantage of people who do not use out of band checks. By doing an out of band check, these sorts of attacks can be stopped very easily.

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call - but not email - to confirm that they did indeed send the original email. If they did send the email, you can proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

Example 2: You receive a phone call from someone claiming to be your bank, or HMRC, or HMCTS. You hang up the call, and locate the official website for the company. You should be able to find multiple official contact details there. Use one of these to contact the place the caller claimed to be from. If, for example, the claim was that your bank was calling, you can call the direct number and speak to the switchboard about the reason for the initial call. They will forward you to the correct department. You can then confirm the validity of the original call, and so confirm whether the original caller was actually from your bank or not.

Example 3: Someone enters your place of work, and claims to have a meeting with a specific person. Unfortunately, there is no record of this on the expected visitor list. You can call or email the person within your place of work to

confirm the visitor is legitimate. This check also works if tradespeople arrive unexpectedly, because you can contact both the relevant person within your place of work and also contact the company they claim to be from, using the company's official website contact details.

Example 4: You receive an email requesting that you reset your password immediately. The email contains a link to perform the password reset. You have not attempted to login to that account recently. You should use an internet search for the website or type the URL directly if you know exactly what it should be. When you attempt to login, the website will let you know if you need to reset your password. If not, you know someone else has attempted to gain access to your account. That would mean the password reset request was not legitimate, and most likely a phishing attempt hoping to get your username and password through the reset link in the original email. Similarly, if you get an MFA request unexpectedly, do not confirm it unless you were indeed attempting to access that account immediately before the request came through. If you get an MFA request, but had not been trying to connect using the account, you should change the account password as soon as possible, because it might have been compromised.

When doing an out of band check, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, perform an out of band check by making a phone call. If someone calls you, perform an out of band check by using the Internet. It is very unlikely that multiple communication channels have been compromised.

Be sure to get official contact details for companies only from their official websites. Never be afraid to hang up on someone and check their identity through another method, especially if they are asking for sensitive or personal information or credentials. Never be afraid to check the legitimacy of unusual email requests. by contacting the sender through a different communication channel.

Doing an out of band check lets you confirm that the messages come from the person they claim to be, and that the requests are valid. This helps prevent you or your company from losing money to fake invoices, from accidentally giving up sensitive information or credentials, and from having unauthorised individuals in your place of work. Doing an out of band check is fast and easy.

All members of your workplace should be happy to receive such a check. It shows that you take security seriously, and that you are helping to protect them as well as yourself.