

**Ministry of Justice (MoJ) Cyber Security
Guidance: Technical User Edition**

Contents

Cyber and Technical Security Guidance.....	7
Summary.....	7
Offline content.....	7
Getting in touch.....	7
Background.....	7
Information structure.....	8
Information security policies.....	9
Mobile devices and teleworking.....	10
Human resource security.....	10
Asset management.....	10
Access control.....	11
Cryptography.....	12
Physical and environmental security.....	12
Operations security.....	13
Communications security.....	14
System acquisition, development and maintenance.....	15
Supplier relationships.....	15
Information security incident management.....	16
Information security aspects of business continuity management.....	16
Compliance.....	16
Risk Assessment.....	17
Other Guidance.....	17
Intranet.....	17
Technical Guidance.....	17
 Getting in contact.....	 17
Reporting an incident.....	17
Cyber Security Consultancy Team: asking for help.....	18
Overview.....	18
About the team.....	18
Asking for help.....	18
How the Consultancy team handle requests for help.....	18
What happens next.....	18
If things go wrong.....	19
 Information security policies.....	 19
Management direction for information security.....	19
Avoiding too much security.....	19
IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER.....	20
IT Security Policy (Overview).....	21
Line Manager approval.....	28
Shared Responsibility Models.....	29
 Mobile devices and teleworking.....	 30
Mobile device policy.....	30
Remote Working.....	30

Teleworking.....	33
Accessing Ministry of Justice (MoJ) IT Systems From Overseas.....	33
General advice on taking equipment overseas.....	36
Security Guidance for Using a Personal Device.....	37
Human resource security.....	38
Prior to employment.....	38
Personnel security clearances.....	38
During employment.....	39
Training and Education.....	39
Asset management.....	39
Responsibility for assets.....	39
Acceptable use of Information Technology at work.....	39
Acceptable use policy.....	41
IT Acceptable Use Policy.....	42
Guidance on IT Accounts and Assets for Long Term Leave.....	47
Protect yourself online.....	48
Information classification.....	49
Data Handling and Information Sharing Guide.....	49
Government Classification Scheme.....	54
Information Classification, Handling and Security Guide.....	54
OFFICIAL, OFFICIAL-SENSITIVE.....	64
Secrets management.....	64
Media handling.....	65
Removable Media.....	65
Secure Disposal of IT Equipment.....	66
Access control.....	67
Business requirements of access control.....	67
Access Control guide.....	67
Enterprise Access Control Policy.....	69
User access management.....	74
Authentication.....	74
Management access.....	75
Managing User Access Guide.....	76
Minimum User Clearance Requirements Guide.....	77
Multi-Factor Authentication (MFA) Guide.....	78
Privileged Account Management Guide.....	79
User responsibilities.....	80
Protecting Social Media Accounts.....	80
System and application access control.....	82
Account management.....	82
Authorisation.....	83
Multi-user accounts and Public-Facing Service Accounts Guide.....	84
Password Creation and Authentication Guide.....	85
Password Management Guide.....	86
Password Managers.....	88
Passwords.....	89
Password Storage and Management Guide.....	94
Policies for Google Apps administrators.....	95
Policies for Macbook Administrators.....	96
System Users and Application Administrators.....	97

Using LastPass Enterprise.....	102
Cryptography.....	104
Cryptographic controls.....	104
Automated certificate renewal.....	104
Cryptography.....	104
HMG Cryptography Business Continuity Management Standard.....	106
Public Key Infrastructure Policy.....	108
Use of HMG Cryptography Policy.....	117
Physical and environmental security.....	121
Secure areas.....	121
Physical Security Policy.....	121
Equipment.....	123
Clear Screen and Desk.....	123
Laptops.....	124
Locking and shutdown.....	125
Policies for MacBook Users.....	127
System Lockdown and Hardening Standard.....	127
Operations security.....	132
Operational procedures and responsibilities.....	132
Mail Check.....	132
Offshoring Guide.....	132
Public Sector DNS.....	151
Web Check.....	152
Protection from malware.....	152
Malware Protection Guide - Overview.....	152
Backup.....	159
System Backup Guidance.....	159
System Backup Policy.....	161
System Backup Standard.....	163
Logging and monitoring.....	169
Accounting.....	169
Commercial off-the-shelf applications.....	169
Custom Applications.....	170
Logging and monitoring.....	172
Protective Monitoring Guide.....	174
Security Log Collection.....	189
Control of operational software.....	201
Guidance for using Open Internet Tools.....	201
Technical vulnerability management.....	205
Implementing security.txt.....	205
Vulnerability Disclosure Policy.....	205
Vulnerability Scanning and Patch Management Guide.....	206
Communications security.....	214
Network security management.....	214
Code of connection standard.....	214
Defensive domain registrations.....	234
Internet -v- PSN.....	236
IP addresses, DNS information & architecture documentation.....	237

Multiple consecutive (back-to-back) firewalls.....	237
Networks are just bearers.....	237
Information transfer.....	237
Bluetooth.....	237
Criminal Justice Secure Mail.....	240
Data sovereignty.....	240
Email.....	241
General Apps Guidance.....	241
Web Browsing.....	245
System acquisition, development and maintenance.....	248
Security requirements of information systems.....	248
Technical Security Controls Guide.....	248
Security in development and support processes.....	253
Maintained by Default.....	253
Secure by Default.....	253
Source code publishing.....	254
System Test Standard.....	254
Test data.....	259
Using Live Data for Testing purposes.....	259
Supplier relationships.....	263
Information security in supplier relationships.....	263
Assessing suppliers.....	263
Contractual promises.....	263
Security Aspects Letters.....	263
Supplier corporate IT.....	267
Supplier service delivery management.....	268
Baseline for Amazon Web Services accounts.....	268
Information security incident management.....	271
Management of information security incidents and lost devices.....	271
Forensic Principles.....	271
Incident Management Plan and Process Guide.....	290
IT Incident Management Policy.....	307
Lost devices or other IT security incidents.....	317
Information security aspects of business continuity management.....	317
Information security continuity.....	317
IT Disaster Recovery Plan and Process Guide.....	317
IT Disaster Recovery Policy.....	327
Compliance.....	331
Compliance with legal and contractual requirements.....	331
Data destruction.....	331
Data security and privacy.....	336
Information security reviews.....	340
Standards Assurance Tables.....	340
Risk Assessment.....	343

Risk Management.....	343
Infrastructure System Accreditation.....	343
Risk Assessment Process.....	344
Risk Reviews.....	344

Cyber and Technical Security Guidance

Summary

This site documents some of the security decisions that the [Ministry of Justice \(MoJ\)](#) has made for the products we operate, and our relationships with suppliers.

The MoJ [Technical Guidance](#) covers technical decisions in the MoJ more widely.

Note: This guidance is dated: 9 April 2021.

Offline content

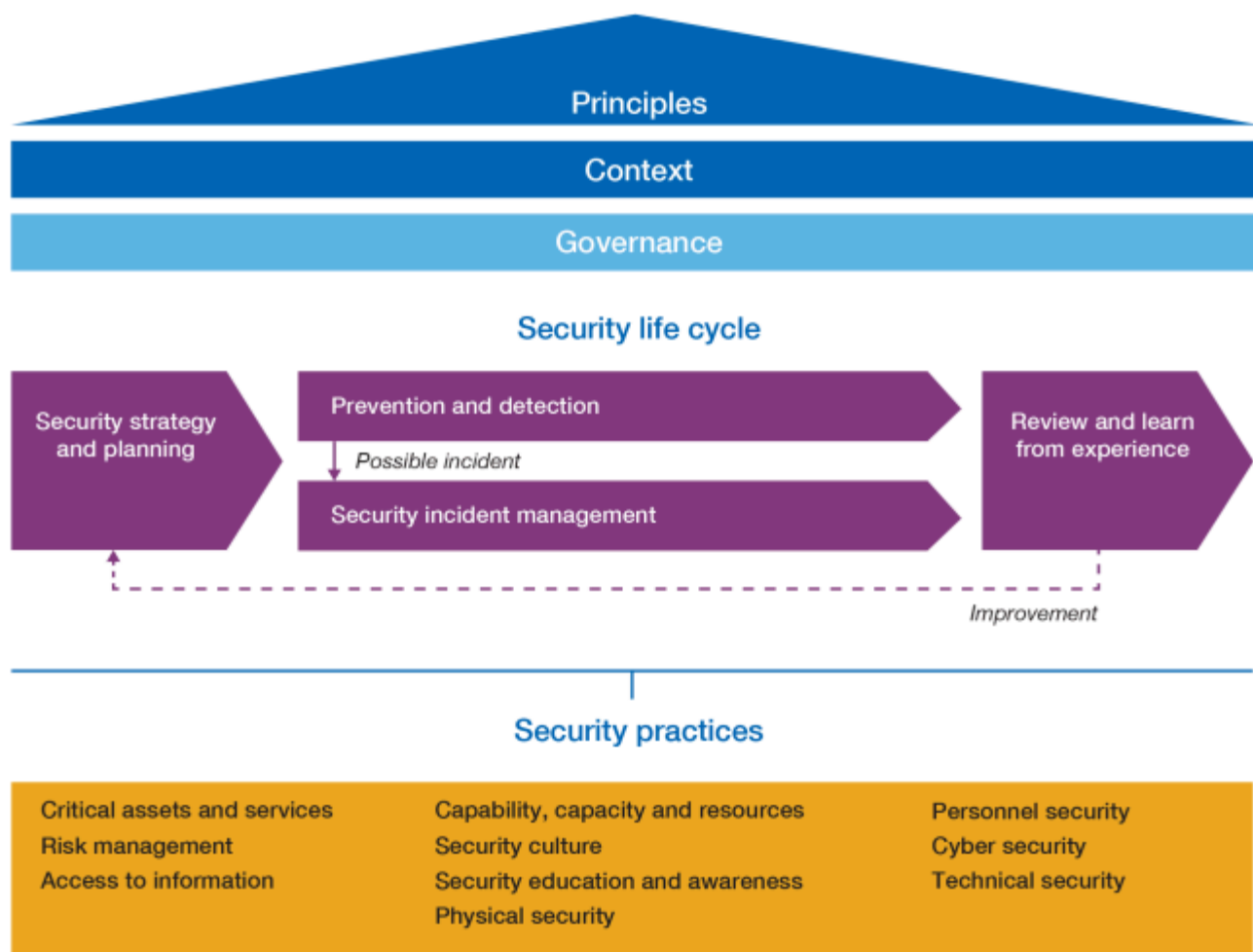
This offline version of the guidance is available as a PDF file for convenience. However, it is time-limited: it is not valid after 9 May 2021. For the latest, current version of the guidance, see [here](#).

Getting in touch

- [To report an incident](#).
- For general assistance on MoJ security matters, email security@justice.gov.uk.
- For Cyber Security assistance or consulting, email CyberConsultancy@digital.justice.gov.uk. More information about the Cyber Security Consultancy Team is [available](#).
- Suppliers to the MoJ should first communicate with their usual MoJ points of contact.

Background

[Government Functional Standard - GovS 007: Security](#) replaces the [HMG Security Policy Framework \(SPF\)](#), last published in May 2018. It also incorporates the [Minimum Cyber Security Standard \(MCSS\)](#) which defines the minimum security measures that departments implement with regards to protecting their information, technology and digital services to meet their SPF and National Cyber Security Strategy obligations.



Sections 6.9 Cyber security and 6.10 Technical security of the standard state:

- The security of information and data is essential to good government and public confidence. To operate effectively, HMG needs to maintain the confidentiality, integrity and availability of its information, systems and infrastructure, and the services it provides. Any organisation that handles government information shall meet the standards expected of HM Government.
- Technical security relates to the protection of security systems from compromise and/or external interference that may have occurred as a result of an attack.

Information structure

The MoJ has developed our cyber and technical security taxonomy as follows:

Level 1	Level 2
Information security policies	Management direction for information security
Mobile devices and teleworking	Mobile device policy
	Teleworking
Human resource security	Prior to employment
	During employment
Asset management	Responsibility for assets
	Information classification

Level 1	Level 2
Access control	Media handling Business requirements of access control User access management User responsibilities System and application access control
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment
Operations security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management
Communications security	Network security management Information transfer
System acquisition, development and maintenance	Security requirements of information systems Security in development and support processes Test data
Supplier relationships	Information security in supplier relationships Supplier service delivery management
Information security incident management	Management of information security incidents and lost devices
Information security aspects of business continuity management	Information security continuity
Compliance	Compliance with legal and contractual requirements Information security reviews
Risk Assessment	Risk Assessment Process

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

Content tagged with the Intranet icon () is on the MoJ Intranet. You will need Intranet access to view that content.

Information security policies

Management direction for information security

Avoiding too much security	All users
IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER	All users

IT Security All Users Policy	All users (Policy)
IT Security Policy (Overview)	All users (Policy)
IT Security Technical Users Policy	Technical Architect, DevOps, IT Service Manager, Software Developer (Policy)
Line Manager approval	All users
Shared Responsibility Models	Technical Architect, DevOps, IT Service Manager, Software Developer

Mobile devices and teleworking

Mobile device policy

Remote Working	All users
--------------------------------	-----------

Teleworking

Accessing MoJ IT Systems From overseas	All users
General advice on taking equipment overseas	All users
Security Guidance for Using a Personal Device	All users

Human resource security

Prior to employment




Personnel security clearances	All users
---	-----------

During employment

Training and Education ()	All users
--	-----------


Asset management

Responsibility for assets



Acceptable use ()	All users
Acceptable use policy	All users (Policy)
Guidance on IT Accounts and Assets for Long Term Leave	All users
IT Acceptable Use Policy	All users (Policy)
Protect Yourself Online ()	All users
Web browsing security ()	All users

Information classification

Data Handling and Information Sharing Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
---	--

Government Classification Scheme ()	All users
Information Classification and Handling Guide	All users
Information Classification and Handling Policy	All users (Policy)
OFFICIAL and OFFICIAL-SENSITIVE	All users
Secrets management	Technical Architect, DevOps, IT Service Manager, Software Developer

Media handling

Removable media ()	All users
Secure disposal of IT equipment ()	All users

Access control

Business requirements of access control

Access Control Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Enterprise Access Control Policy	Technical Architect, DevOps, IT Service Manager, Software Developer

User access management

Authentication	Technical Architect, DevOps, IT Service Manager, Software Developer
Management access	Technical Architect, DevOps, IT Service Manager, Software Developer
Managing User Access Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Minimum User Clearance Levels Guide	All users
Multi-Factor Authentication	Technical Architect, DevOps, IT Service Manager, Software Developer
Privileged Account Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer

User responsibilities

Protecting Social Media Accounts	All users
----------------------------------	-----------

System and application access control

Account management	Technical Architect, DevOps, IT Service Manager, Software Developer
Authorisation	Technical Architect, DevOps, IT Service Manager, Software Developer
Multi-user accounts and Public-Facing Service Accounts Guide	Technical Architect, DevOps, IT Service Manager, Software Developer

Password Creation and Authentication Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Password Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Password Managers	All users
Passwords	All users
Password Storage and Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Policies for Google Apps administrators	Technical Architect, DevOps, IT Service Manager, Software Developer
Policies for Macbook Administrators	Technical Architect, DevOps, IT Service Manager, Software Developer
System User and Application Administrators	Technical Architect, DevOps, IT Service Manager, Software Developer
Using LastPass Enterprise	All users

Cryptography

Cryptographic controls





Automated certificate renewal	Technical Architect, DevOps, IT Service Manager, Software Developer
Cryptography	Technical Architect, DevOps, IT Service Manager, Software Developer
HMG Cryptography Business Continuity Management Standard	Technical Architect, DevOps, IT Service Manager, Software Developer
Public Key Infrastructure Policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Use of HMG Cryptography Policy	Technical Architect, DevOps, IT Service Manager, Software Developer

Physical and environmental security

Secure areas

Physical Security Policy	All users
--	-----------

Equipment

Clear Screen and Desk Policy ()	All users
Laptops ()	All users
Locking and shutdown ()	All users
Policies for Macbook Users ()	All users
System Lockdown and Hardening Standard	Technical Architect, DevOps, IT Service Manager, Software Developer

Operations security

Operational procedures and responsibilities

Active Cyber Defence: Mail Check	Technical Architect, DevOps, IT Service Manager, Software Developer
Active Cyber Defence: Public Sector DNS	Technical Architect, DevOps, IT Service Manager, Software Developer
Active Cyber Defence: Web Check	Technical Architect, DevOps, IT Service Manager, Software Developer
Offshoring Guide	Technical Architect, DevOps, IT Service Manager, Software Developer

Protection from malware

Malware Protection Guide (Overview)	Technical Architect, DevOps, IT Service Manager, Software Developer
Malware Protection Guide: Defensive Layer 1	Technical Architect, DevOps, IT Service Manager, Software Developer
Malware Protection Guide: Defensive Layer 2	Technical Architect, DevOps, IT Service Manager, Software Developer
Malware Protection Guide: Defensive Layer 3	Technical Architect, DevOps, IT Service Manager, Software Developer

Backup

System backup guidance	Technical Architect, DevOps, IT Service Manager, Software Developer
System backup policy	Technical Architect, DevOps, IT Service Manager, Software Developer
System backup standard	Technical Architect, DevOps, IT Service Manager, Software Developer

Logging and monitoring

Accounting	Technical Architect, DevOps, IT Service Manager, Software Developer
Commercial off-the-shelf applications	Technical Architect, DevOps, IT Service Manager, Software Developer
Custom Applications	Technical Architect, DevOps, IT Service Manager, Software Developer
Logging and monitoring	Technical Architect, DevOps, IT Service Manager, Software Developer
Online identifiers in security logging and monitoring	Technical Architect, DevOps, IT Service Manager, Software Developer
Protective Monitoring	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection	Technical Architect, DevOps, IT Service Manager, Software Developer

Security Log Collection: Enterprise IT - Infrastructure	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Enterprise IT - Mobile Devices	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Hosting Platforms	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Log entry metadata	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Maturity Tiers	Technical Architect, DevOps, IT Service Manager, Software Developer

Control of operational software

Guidance for using Open Internet Tools	All users
--	-----------

Technical vulnerability management

Patch management guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Vulnerability Disclosure	Technical Architect, DevOps, IT Service Manager, Software Developer
Vulnerability Disclosure: Implementing security.txt	Technical Architect, DevOps, IT Service Manager, Software Developer
Vulnerability scanning and patch management guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Vulnerability scanning guide	Technical Architect, DevOps, IT Service Manager, Software Developer


Communications security

Network security management

Code of Connection Standard	Technical Architect, DevOps, IT Service Manager, Software Developer
Defensive domain registrations	Technical Architect, DevOps, IT Service Manager, Software Developer
Internet v. PSN	Technical Architect, DevOps, IT Service Manager, Software Developer
IP DNS Diagram Handling	Technical Architect, DevOps, IT Service Manager, Software Developer
Multiple Back-to-back Consecutive Firewalls	Technical Architect, DevOps, IT Service Manager, Software Developer
Networks are just bearers	Technical Architect, DevOps, IT Service Manager, Software Developer

Information transfer

Bluetooth	All users
-----------	-----------

Criminal Justice Secure Mail (CJSM)	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Sovereignty	Technical Architect, DevOps, IT Service Manager, Software Developer
Email ()	All users
General Apps Guidance	All users
Web browsing security policy profiles	All users (Policy)

System acquisition, development and maintenance

Security requirements of information systems

Technical Security Controls Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Technical Security Controls Guide: Defensive Layer 1	Technical Architect, DevOps, IT Service Manager, Software Developer
Technical Security Controls Guide: Defensive Layer 2	Technical Architect, DevOps, IT Service Manager, Software Developer

Security in development and support processes

Maintained by Default	Technical Architect, DevOps, IT Service Manager, Software Developer
Secure by Default	Technical Architect, DevOps, IT Service Manager, Software Developer
Source Code Publishing	Technical Architect, DevOps, IT Service Manager, Software Developer
System Test Standard	Technical Architect, DevOps, IT Service Manager, Software Developer

Test data

Using Live Data for Testing purposes	Technical Architect, DevOps, IT Service Manager, Software Developer
--	--

Supplier relationships

Information security in supplier relationships

Suppliers to MoJ: Assessing Suppliers	Technical Architect, DevOps, IT Service Manager, Software Developer
Suppliers to MoJ: Contracts	Technical Architect, DevOps, IT Service Manager, Software Developer
Suppliers to MoJ: Security Aspect Letters	Technical Architect, DevOps, IT Service Manager, Software Developer
Suppliers to MoJ: Supplier Corporate IT	Technical Architect, DevOps, IT Service Manager, Software Developer



Supplier service delivery management

Baseline for Amazon Web Services accounts	Technical Architect, DevOps, IT Service Manager, Software Developer
---	--

Information security incident management**Management of information security incidents and lost devices**

Forensic Principles	Technical Architect, DevOps, IT Service Manager, Software Developer
Forensic Readiness Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Forensic Readiness Policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Incident Management Plan and Process Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
IT Incident Management Policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Lost devices or other IT security incidents	All users
Reporting an incident	All users

Information security aspects of business continuity management**Information security continuity**

IT Disaster Recovery Plan and Process Guide ()	Technical Architect, DevOps, IT Service Manager, Software Developer
IT Disaster Recovery Policy ()	Technical Architect, DevOps, IT Service Manager, Software Developer

Compliance**Compliance with legal and contractual requirements**

Data Destruction	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Destruction: Contract Clauses - Definitions	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Destruction: Contract Clauses - Long Format	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Destruction: Contract Clauses - Long Format (Appendix)	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Destruction: Contract Clauses - Short Format	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Destruction: Instruction and Confirmation Letter	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Security and Privacy	All users

Data Security & Privacy Lifecycle Expectations	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Security & Privacy Triage Standards	Technical Architect, DevOps, IT Service Manager, Software Developer

Information security reviews


Standards Assurance Tables	Technical Architect, DevOps, IT Service Manager, Software Developer
--	--

Risk Assessment

Risk Management

Infrastructure and system accreditation	Technical Architect, DevOps, IT Service Manager, Software Developer
---	--

Risk Assessment Process

Risk reviews ()	All users
--	-----------

Other Guidance

Intranet

There are other cyber and technical security guidance documents available to reference. A large number of these documents are available in the [IT and Computer Security](#) repository on the MoJ Intranet, but these documents are currently being reviewed and progressively are being incorporated into this main [Security Guidance](#) repository.

Technical Guidance

The MoJ [Technical Guidance](#) should be read together with this security-focused guidance.

The [Government Functional Standard - GovS 007: Security](#) provides the base material for all security guidance in the MoJ.

Getting in contact

Reporting an incident

Ministry of Justice (MoJ) colleagues should visit <https://intranet.justice.gov.uk/guidance/security/report-a-security-incident/> on the MoJ Intranet. Alternatively, if the incident is of a cybersecurity nature then use [Report a cyber security incident](#).

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

Cyber Security Consultancy Team: asking for help

Overview

This document tells you about the Cyber Security Consultancy 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 cyber security consultant, send an email to: CyberConsultancy@digital.justice.gov.uk.

About the team

The Cyber Security Consultancy Team is part of Ministry of Justice (MoJ) Security & Privacy. The MoJ Chief Information Security Officer leads the consultants.

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:

CyberConsultancy@digital.justice.gov.uk

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

The consultancy 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 Consultancy team handle requests for help

Each working day, we review all new requests.

Our Service Level Agreement aims 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 Consultancy team, we'll tell you immediately after the initial assessment.

If your request is appropriate for the Consultancy 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: CyberConsultancy@digital.justice.gov.uk.

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

Information security policies

Management direction for information security

Avoiding too much security

This guidance applies to developers and system administrators who work for the Ministry of Justice (MoJ).

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 OFFICIAL-SENSITIVE. 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.

OFFICIAL-SENSITIVE is not a different classification to OFFICIAL. 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 MoJ services. But the IP address of a public sector server or a router should not be personal data.

Remember also that within the MoJ, systems 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 Ministry of Justice (MoJ) 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 MoJ must achieve (and suppliers to MoJ, where they process MoJ 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 cataloging of information held/processed; and
- identification and cataloging 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)

Introduction

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

Who is this for?

This policy is aimed at three audiences:

Technical users

These are in-house MoJ 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 MoJ 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.

General users

All other staff working for the MoJ.

Within this policy, “all MoJ users” refers to General users, Technical users, and Service Providers as defined above.

Associated documentation

For further guidance on IT Security, see the policies below.

- [IT Security All Users Policy](#): which provides further details of the responsibilities of all MoJ users at the MoJ.
- [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 MoJ.

Principles

All MoJ users **MUST**:

- Comply with the MoJ's [Acceptable Use Policy](#) wherever they work.
- Report all security incidents promptly and in line with MoJ's [IT Incident Management Policy](#).
- Make themselves aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other MoJ 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 must follow the guidance set out for all MoJ users in [IT Security All Users Policy](#) **AND** also comply with the [IT Security Technical Users Policy](#).

Service Providers

Service Providers must follow the guidance set out for all MoJ 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 MoJ'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 MoJ always co-operates with the relevant authorities, and provides appropriate evidence.

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

IT Security All Users Policy

Introduction

This policy provides more information on the actions expected of all Ministry of Justice (MoJ) users when using MoJ 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.

Who is this for?

This policy is aimed at three audiences:

Technical users

These are in-house MoJ 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 MoJ 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.

General users

All other staff working for the MoJ.

Within this policy, “all MoJ users” refers to General users, Technical users, and Service Providers as defined above.

Approach

The MoJ ensures that IT security controls are designed and implemented to protect MoJ 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 MoJ. This includes IT systems, whether developed by the MoJ 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 MoJ resources.

Security classification

All MoJ Staff are responsible for ensuring data is:

- Classified correctly as detailed in the [Information Classification, Handling and Security Guide](#).
- 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 MoJ [Access Control Guide](#).

Physical and personnel security

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

- All MoJ 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 MoJ's IT Teams are not directly responsible for the physical security and environment of the MoJ sites.
- Physical security controls and the environment in which the MoJ IT systems operate form part of a system's overall risk landscape. All MoJ users **MUST** ensure they adhere to the security controls and requirements set out in this policy.
- Unless otherwise formally agreed by the MoJ, all MoJ users, including agency staff and contractors who have access to MoJ 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 MoJ 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 MoJGroup Security (mojgroupsecurity@justice.gov.uk) and [CPNI Guidance](#).

Identity and access control

The MoJ [Access Control Guide](#) 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 MoJ [Access Control Guide](#) addresses access control principles such as identification, authentication, authorisation, and accounting.

Password management

The MoJ [Password Management Guide](#) sets out the requirements for strong password implementation and management, to help prevent unauthorised access to MoJ systems. Examples include password creation, authentication, storage and management.

Email security

The MoJ Email Security Guide specifies the controls and processes required to protect the MoJ'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 MoJ's email servers to organisations outside the MoJ 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 MoJ has in place [Remote Working](#) guidance that sets out the requirements for safely accessing and using the MoJ'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 MoJ must be used in line with the [Acceptable Use Policy](#).

Any request to take MoJ IT equipment overseas must follow the guidance provided in the [Acceptable Use Policy](#) and the [Accessing MoJ IT Systems From Overseas](#) information.

Malware protection

The MoJ [Malware Protection Guide](#) specifies the controls and processes required to protect all systems against malware. Malware may enter the MoJ by employee email through the internet, mobile computers, and removable media devices.

The MoJ [Malware Protection Guide](#) addresses the following relevant domains:

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

Roles and responsibilities

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

All MoJ users are required to comply with the roles and responsibilities outlined in the Information Assurance Framework Process.

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

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 MoJ SIRO is responsible for the overall MoJ information risk policy and guidance, and ensures it continues to provide appropriate risk appetite and a suitable risk framework.	<p>Implementing and managing information risk management in their respective business groups.</p> <p>Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.</p> <p>Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.</p>

Role	Responsibility	Which includes...
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 MoJ's risk appetite and risk framework.	In line with the MoJ 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.	<p>Logging and monitoring.</p> <p>Reviewing access permissions.</p> <p>Understanding and addressing risks associated to their information assets.</p> <p>Ensuring secure disposal of information when it is no longer required.</p>
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.	<p>Verify that contracts are written to reflect the MoJ's IT Security Policy.</p> <p>Ensure contractors comply with the requirements set out by this policy and associated documentation.</p> <p>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.</p> <p>Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the MoJ, is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.</p>

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

IT Security Technical Users Policy

Introduction

This policy provides more information on the actions expected of Technical and Service Provider users when using Ministry of Justice (MoJ) equipment and infrastructure. It is a sub-page to the [IT Security Policy Overview](#).

Who is this for?

This policy is aimed at:

Technical users

These are in-house MoJ 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 MoJ 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.

Vulnerability scanning and patch management

The MoJ [Vulnerability Scanning and Patch Management Guide](#) outlines the requirements for maintaining up to date MoJ systems and equipment to protect them from security vulnerabilities.

The guide includes patching schedules for the different MoJ 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 MoJ systems.

Technical controls

The MoJ [Technical Security Controls Guide](#) ensures protection from unauthorised access or misuse of the MoJ IT systems, applications, and data stored within them.

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

- Enforcing access controls in support of the [Access Control Guide](#).
- Building adequate security for the MoJ network and network boundaries.
- Creating secure software development and software configuration processes and designs.
- Monitoring the MoJ 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 MoJ's IT systems must use cryptographic technologies to provide secure connections to third party systems or protect information “at rest” on user devices, including laptops and mobiles.

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 and the [Government Functional Standard - GovS 007: Security](#) (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 MoJ's Staff who use cryptography must 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 MoJ's compliance with the minimum cryptography requirements.

Software development

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

Security incident management

The MoJ's [IT Incident Management Policy](#) covers the end-to-end incident lifecycle, and provides the guidance for the MoJ 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 MoJ [IT Incident Management 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 MoJ Information Assurance Framework Process to be effective, it must extend to organisations working on behalf of the MoJ or handling MoJ 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 must be regularly monitored, reviewed, and audited.
- When the MoJ buys IT goods, services, systems, or equipment, IT security implications must be considered.
- All MoJ IT suppliers who handle and store information on behalf of the MoJ must be assessed annually against the [Government Functional Standard - GovS 007: Security](#) (previously HMG [Security Policy Framework](#)) and the MoJ's [IT Security Policy](#). Additional self-assessment requirements may be stipulated in the contract between the IT supplier and the MoJ. The MoJ's IT suppliers are responsible for carrying out these self-assessments, and for submitting those assessments to the MoJ. The MoJ is responsible for approving the assessments submitted by the supplier.
- The appropriate measures must be put in place for any supplier not meeting compliance requirements, and the relevant MoJ teams must be notified and consulted.
- All MoJ suppliers and contractors adhere to the GDPR and the Data Protection Act 2018.

Further advice can be found in the [Information Classification, Handling and Security Guide](#).

Physical and personnel Security

The Contract owner shall 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 [Security Aspects Letter \(SAL\)](#) is issued to the contractor along with the contract document.

Privileged users

The MoJ's Privileged User Guide sets out the key responsibilities for administrator roles within the MoJ 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 MoJ 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 MoJ 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 must be assessed to identify technical risks.

Audit

A security audit is a systematic evaluation of the MoJ'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 MoJ 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 should 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: correspondence@giaa.gov.uk

When conducting an audit:

- Documentary evidence must be made available to auditors upon request.
- Details provided should include the implementation of any technical security control in an IT system. Documentary evidence of changes must be reviewed.
- The evaluation should 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 must be provided, and the desired risk mitigation as documented in the Information Assurance Framework Process.
- Activities involving verification of operational systems should be carefully planned and agreed to minimise disruptions to business processes.

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Line Manager approval

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Some MoJ 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.

Examples include:

- [General advice on taking equipment overseas.](#)
- [Security Guidance for Using a Personal Device.](#)

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 MoJ IT Policies, just ask: security@justice.gov.uk.

1. Check that your direct report (DR) has said what they want in their request. The request should identify which MoJ 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 MoJ 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 MoJ 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 MoJ IT Policies need a copy of formal approval for other parties. For example, before your DR travels to some countries on MoJ business, send a copy of your approval to Operational Security: OperationalSecurityTeam@justice.gov.uk.

Steps to follow (Direct Reports)

Note: If at any time you need help about this process, or the applicable MoJ IT Policies, just ask: security@justice.gov.uk.

1. Check that your business need is valid.
2. Check which MoJ 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 MoJ 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 MoJ IT Policies. Ensure that you include:
 - Your request.
 - The business case.
 - The list of applicable MoJ 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Shared Responsibility Models

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

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

Shared

MoJ 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.

MoJ specific

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

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

Mobile devices and teleworking

Mobile device policy

Remote Working

Key points

- Be professional, and help keep Ministry of Justice (MoJ) information and resources safe and secure at all times.
- Think about where you are working, for example - can other people or family see what you are working on? Be thoughtful about information privacy.
- Never send work material to personal email accounts.
- Keep MoJ 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.
- Do not leave MoJ equipment unattended.
- Get in touch quickly to report problems or security questions.

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 MoJ, 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 MoJ, 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 MoJ mobile computing equipment.

What is remote working?

Remote working means you are working away from the office. This could be from home, at another MoJ 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-MoJ 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.

Always:

- Keep MoJ equipment and information safe and secure.
- Protect MoJ 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.
- Keep your workspace clear and tidy - follow a 'clean desk policy', including paperwork, to ensure MoJ information isn't seen by unauthorised people.
- Use MoJ 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.

Never:

- Let family or other unauthorised people use MoJ equipment.
- Leave equipment unattended.
- Work on sensitive information in public spaces, or where your equipment can be overlooked by others.
- Advertise the fact that you work with MoJ materials.
- Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
- Send work material to your personal email address.

Working securely

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

- **Work locations** - as with home working above, 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 eg conference and video calls.
- Keep MoJ **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 MoJ systems you access and work with.

Using your own equipment

The main guidance is available [here](#).

Wherever possible, you should always use official MoJ equipment for business purposes. Never send work material to your personal email accounts.

If you are working remotely, or do not have access to MoJ equipment, it might be tempting to use your own equipment, especially printers. The advice is to avoid printing anything, and in particular not to use personal printers.

However, if you really must print MoJ information, you:

- should connect directly to the printer using USB, not WiFi

- should not print out personal information relating to others
- should consult the information asset owner or line manager before printing the information
- must store any and all printed materials safely and securely until you return to MoJ premises, when they must be disposed of or filed appropriately
- **must never** dispose of MoJ information in your home rubbish or recycling

Basically, think before you print.

Privacy

It is important to protect privacy: yours and that of the MoJ. 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 MoJ 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 MoJ information. If anyone might see 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 see the information you are working with.
- Don't 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.

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

Privacy Advice

Privacy Team

- Email: privacy@justice.gov.uk
- Slack: #securityprivacyteam
- Intranet: <https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/>

Cyber Security Advice

Cyber Consultants & Risk Advisors

- Email: security@justice.gov.uk
- Slack: #security

Historic paper files urgently required by ministers, courts, or Public Inquiries

MoJ HQ staff

- Email: Records_Retention_@justice.gov.uk

HMCTS and HMPPS staff

- Email: BranstonRegistryRequests2@justice.gov.uk

JustStore

- Email: KIM@justice.gov.uk

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

Accessing Ministry of Justice (MoJ) IT Systems From Overseas

Note: This guidance information applies to all staff, contractors and agency staff who work for the MoJ.

Note: If you are national security cleared to 'Enhanced SC' or DV levels, follow this process for all your trips, regardless of whether they are for business or personal reasons.

As a government official travelling overseas, you should consider that you may be of interest to hostile parties regardless of your role. By following MoJ policies and processes, you can help reduce the risk to yourself and limit the damage of exposure of sensitive information.

In general, it is acceptable for MoJ users to access MoJ services from overseas, and to do this using their MoJ equipment. But before you travel, consider:

- Do you need to take MoJ IT equipment overseas or access MoJ IT systems to do your job?
- Can the business need be met in another way or by someone else?
- If you just need to manage your inbox while away, can you delegate permissions to your inbox to a colleague to manage on your behalf?
- Have you left enough time to check and obtain necessary approvals? The process can take several weeks, depending on the circumstances. This is because it may be necessary to apply additional technical controls to protect you, your device, and any data the device can access.

Steps to follow before travelling

Part One

1. Get confirmation from your Line Manager that there is a business need for you to take MoJ equipment overseas and access MoJ services. Keep a note of the answers you get.

2. Proceed directly to [Part Two](#) of this process if *either one* of the following two statements apply to you:
 - You are travelling or passing through one of the following high-attention countries: *China, Cyprus, Egypt, India, Iran, Israel, North Korea, Pakistan, Russia, Saudi Arabia, South Africa, South Korea, Syria, Turkey, UAE.*
 - You are national security cleared to 'Enhanced SC' or DV levels.
3. If you have reached this step, you do not need to seek further formal approval for your trip.
4. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.
5. Check if you need to do anything to prepare for [International Roaming](#).
6. Enjoy your trip.

Part Two

1. Collect the following information:
 - Name.
 - Email address.
 - Your business area.
 - Your Security Clearance.
 - The network you use to access MoJ data, services or applications, for example DOM1 or Quantum, or online services such as AWS or Google Workspace.
 - The make/type of equipment you want to take with you.
 - Asset Tag details.
 - Countries you'll be visiting or passing through.
 - Dates of travel.
 - Transport details where possible, for example flights or rail journeys.
 - Proposed method of connecting, for example MoJ VPN, WiFi, or Mobile Data (3G/4G/5G).
 - Reason for maintaining access while overseas.
 - The MoJ data, applications, or services you expect to access during your trip.
 - Who you are travelling with.
2. The next step depends your MoJ business area:
 - If you are part of MoJ HQ, HMPPS HQ or HMCTS, contact your Senior Civil Servant (SCS) and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
 - If you are part of HMPPS (but *not* HQ), contact your Governor and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
3. Fill in the [overseas travel request form](#).
4. Send the completed form to security@justice.gov.uk, including the answers obtained from the earlier parts of this process.
5. Your request is considered, and an answer provided, as quickly as possible.
6. When you have received all the approvals, send a copy of your request and the approvals to OperationalSecurityTeam@justice.gov.uk.
7. When Operational Security have acknowledged receipt of the request and approvals, the formal process is complete.
8. Check if you need to do anything to prepare for [International Roaming](#).
9. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.
10. Enjoy your trip.

International Roaming

While travelling, you might incur roaming charges when using your MoJ equipment for calls or accessing services. These charges can be expensive, and must be paid by your Business Unit. This is another reason for having a good business need to take MoJ equipment overseas.

By default, MoJ equipment is not enabled for use overseas. Before travelling, raise the relevant IT Catalogue request to have International Roaming enabled for the duration of your trip, and to activate the remote wipe function. This helps protect the MoJ equipment in case of loss or theft.

If you have any problem when using MoJ equipment overseas

Contact the [Service Desk](#) immediately. Tell them if the MoJ equipment is lost, stolen or was potentially compromised. This includes any time the equipment is deliberately removed out of your sight, such as by a customs official.

If any security-related incident occurs overseas, regardless of whether it involves MoJ equipment, you should contact the [Operational Security Team](#) as soon as possible. See the guidance on [Reporting a Security Incident](#) on the MoJ Intranet. This includes information on reporting an incident outside of UK working hours. For convenience, the out-of-hours telephone number for reporting incidents is repeated [below](#).

If there is a problem with your MoJ equipment, it might be necessary to disable your ability to connect to the MoJ network or services from your device. The Service Desk will do this if required. MoJ-issued phones might still have some functionality, to let you make phone calls, but the device should be treated as compromised and not used any more for any MoJ business.

Related pages

- [General advice on taking Equipment overseas](#)
- [Overseas travel](#)
- [Staff security and responsibilities – during employment](#)

External websites

- [Foreign & Commonwealth Office – travel & living abroad](#)

Contacts

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

Dom1 - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

Information Incident Reporting Line

- Tel: +44 (0)20 3334 0324 for HMPPS staff at any time.
- Tel: +44 (0)20 3334 0324 for MoJ staff **outside UK working hours**.

During UK working hours, MoJ (but not HMPPS) staff should follow the process on the [Reporting a Security Incident](#) page on the MoJ Intranet.

MoJ Phone and Mobile Devices

- Email: MoJ_Phone_and_Mobi@justice.gov.uk

MoJ Security

- Email: security@Justice.gov.uk

General advice on taking equipment overseas

As a government official travelling overseas, you should consider that you are highly likely to be of interest to a range of hostile parties, regardless of your role or seniority. Laptops, tablets and phones are very desirable pieces of equipment to steal and travelling overseas with it puts you at a greater security risk of being a victim of theft.

You should never put yourself in any danger to protect the security of an IT device, as the level of impact to the Ministry of Justice (MoJ) of a compromise does not warrant the risk of injury or loss of liberty. By following your department policies and the advice issued, you can help reduce the risk to yourself and your colleagues.

General guidance

Remove unnecessary files from your device when travelling overseas so that the risk of data exposure is reduced in case of loss or theft.

Keeping safe whilst conducting sensitive work overseas

Be aware that voice calls and SMS messages are not secure and voice calls can be intercepted whilst overseas. Keeping your phone with you at all times helps in having a high level of physical control over the equipment:

- Keep any password/PIN separate from the device.
- Be careful when using your device in situations where it may be lost or stolen, such as busy public places and while transiting customs or security at airports.
- Think about where you are working to ensure that you are not being observed (for instance, somebody looking over your shoulder in a crowded place).
- Never leave the device unattended - not even for a moment.
- If it is not practical to keep the device with you securely at all times (for instance, you are at the swimming pool or gym), consider storing the device in the hotel safe.

Note: Standard hotel safes are not entirely secure and it is normally possible for hotel staff to override controls to gain access. In addition therefore you should also store your device in a tamper proof envelope. You should ensure you have a sufficient number to last the duration of your period of travel. If the tamper evident seals show signs of disturbance or the device exhibits strange behaviour, it should be considered compromised. In either case, you must discontinue use of the device and contact your Service Desk immediately and report the device as potentially compromised.

Guidance on using mobile phones

As a government official you may be of interest to a range of hostile parties and therefore:

- If it is not practical to keep the device with you securely at all times (for instance, you are at the swimming pool or gym), consider storing the device in the hotel safe.
- Avoid conducting work related sensitive phone conversations as they can be intercepted and if you do, ensure you can't be overheard. Examples of sensitive information might include prisoner/offence details, court cases of foreign nationals, terror attacks and extremists.
- Do not use public charging stations or connect the phone to a vehicle by USB or Bluetooth as information can be downloaded from your phone.
- Be aware that hotel and public WiFi spots are not secure, as they can easily be monitored.
- Make sure you use the phone's password or PIN.
- If the phone is taken from you or you believe it may have been compromised in any way, report it to the [Departmental Security Officer](#).

What to do if you are asked to unlock the device by officials

The extent to which an individual wishes to prevent the customs or security staff from accessing the data will directly relate to its sensitivity. Do not risk your own safety. If the device is being carried by hand to an overseas destination, the sensitivity of the data it holds should not justify any risk to personal safety.

- Try to establish your official status and good faith from the outset.
- Remain calm and polite at all times.

- Carry the names and telephone numbers of a relevant departmental contact and invite the official(s) to contact them to confirm that you are who you claim to be.
- If the official continues to insist on the user inputting his/her password, repeat the above steps.
- State that you are carrying official UK government property that is sensitive and that you cannot allow access.
- Ask to see a senior officer or supervisor. You may want to take the names and/or contact details of any officials involved in the event that you wish to pursue a complaint, or an investigation is required, even at a later date.

If you are on official business:

- State that you are a UK civil servant etc. travelling on HMG official business.
- Where appropriate, produce an official document (e.g. on headed notepaper or with a departmental stamp) or identity card that clearly gives your name, photograph and affiliation.
- Produce a letter of introduction from the overseas organisation or individual you are visiting.
- Carry the names and telephone numbers of the officials to be visited in your destination and invite the official(s) to contact them to confirm that you are who you claim to be.

In the event that a device is removed out of your sight (such as by a customs official) then it should be considered compromised. You must [contact the Technology Service Desk immediately](#) and report the device as potentially compromised.

The Technology Service Desk will disable your ability to connect to the MoJ network from your device. Be aware that although the device will still work as a mobile phone, it should be treated as compromised and not used for any MoJ business.

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.

If unsure, contact your Line Manager.

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

Security Guidance for Using a Personal Device

Summary

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ). It provides advice about using personal devices for work purposes.

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

Not everyone has access to an MoJ device for remote use. If you need equipment, you can request it. It can be provided quickly. Contact your Line Manager for details, and to raise a request through the Service Desk.

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

Note: Except when connecting to an MoJ [virtual environment](#), or with documented approval in exceptional circumstances as described [below](#), you must not use a personal device for work purposes.

Guidance

- If you have an MoJ-issued device or virtual environment, you must use that.
- You must not use a personal device to access Office 365 tools (email, calendar, Word, Excel, Powerpoint, etc.) for work purposes.
- You must not use a personal device to access Google Workspace tools (Gmail, Docs, Slides, Sheets, Drive, Meet, Hangouts, etc.) for work purposes.
- This guidance applies to all tools accessed through a web browser or installed client applications.
- Do not send MoJ information to your personal email account.
- Do not use personal accounts for work purposes.
- Do not store work files or information on a personal device (desktop, laptop, tablet or phone).
- Do not store work files or information on a personal storage device or memory stick (external drive, thumb drive, USB stick, etc.).
- Some teams within the MoJ might 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 Operational Security Team: security@justice.gov.uk.

Note: You are not asked or required to use your own devices for work purposes. If you have access to MoJ devices for work purposes, you must use them by default.

Virtual environment

The MoJ can enable 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 MoJ Service Now.

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

Human resource security

Prior to employment

Personnel security clearances

Baseline Personnel Security Standard (BPSS)

Unless otherwise agreed formally by the Ministry of Justice (MoJ) in writing, any person (whether MoJ staff, contractor or through supply chain) who has access to, or direct control over, MoJ data must have satisfactorily completed the baseline.

The [BPSS](#) is published on [GOV.UK](#).

National Security Clearances

The MoJ will advise on a case-by-case basis if an individual requires a [national security vetting and clearance](#).

The MoJ does **not** have a standing requirement for system administrators or application developers to maintain Security Check (SC).

During employment

Training and Education

Why?

The Ministry of Justice (MoJ)'s Information Security awareness programme plays an essential part in maintaining security. It informs all MoJ 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.

Source

Guidance is provided to staff via the Security section of the MoJ Intranet, <https://intranet.justice.gov.uk/guidance/security/>. All new staff starting work within the MoJ will receive mandatory IA training. This should ensure that the new staff member is made aware of their security responsibilities whilst working at the MoJ.

Asset management

Responsibility for assets

Acceptable use of Information Technology at work

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Everyone working at the MoJ has access to MoJ 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](#).

Summary

Be sensible when using MoJ IT resources:

- The resources are for you to do MoJ 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 MOJ 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 see those details.

Unacceptable use of MoJ 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 your work email address for personal tasks.
- Using a personal account or personal email address for work tasks.
- Excessive private use during working time.
- Installing unlicensed or unauthorised software.

Why unacceptable use is a problem

Unacceptable use of IT might affect the MoJ 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 MoJ IT resources. This includes keeping your usernames and passwords safe and secure.

While you might be careful about acceptable use of MoJ 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 MoJ IT

Limited personal use of MoJ 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 MoJ 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 MoJ 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 MoJ mobile phone, and then using the other device for any of the above activities.

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

All use of MoJ IT resources is monitored and logged. This includes mobile phone usage listed in account bills. It is possible to see 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 MoJ 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 MoJ 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, please follow the [Use of Removable Media policy](#).

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 information applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Guidance about Acceptable Use of IT within the MoJ is available [here](#).

The definitive list of Acceptable Use Policy statements is available [here](#).

IT Acceptable Use Policy

This document is the Ministry of Justice (MoJ) ICT Security – IT Acceptable Use Policy. It provides the core set of ICT security principles and expectations on the acceptable use of MoJ ICT systems.

Introduction

MoJ ICT systems and services are first and foremost provided to support the delivery of MoJ's business services. To achieve this, most MoJ users are provided with an appropriate general purpose computer environment (i.e. a standard MS Windows desktop) and access to services and communication tools such as e-mail and the Internet.

This policy outlines the acceptable use of MoJ IT systems and services, and, expectations the MoJ has on its staff in this area.

Scope

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

Failure to adhere to this policy could result in:

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

POL.ITAUP.001

All Users **must be** made aware of the IT Acceptable Use Policy (this document) and provided with security awareness training which covers this policy.

POL.ITAUP.002

All Users **must undergo** refresher security awareness training which covers 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 MoJ ICT systems. All Users have a role in protecting the information assets which are under their control or have access to.

MoJ ICT 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 ICT system (include support and system administrative Users) are familiar with these SyOPs and are provided with the appropriate training.

POL.ITAUP.003

All ICT systems **must have and maintain** a set of Security Operating Procedures (SyOPs). For systems undergoing the Accreditation process, these SyOPs can be included as part of the RMADS.

POL.ITAUP.004

All Users of an ICT system (this includes support and system administrative staff) must read the SyOPs applicable and **must acknowledge** that they have both read and understood it before being granted access. A record must be kept of this event and made available to the system Accreditor upon request.

POL.ITAUP.005

All Users **must be** made aware that non-conformance to system SyOPs constitutes a breach of the MoJ IT Security Policy which may result in disciplinary action.

POL.ITAUP.006

Any change to an ICT system's SyOPs **must be** approved by the system Accreditor in advance.

POL.ITAUP.007

Any request to perform an action on an ICT system which contravenes its SyOPs **must be** approved by the system Accreditor or MoJ ITSO in advance.

For most Users, access to MoJ ICT systems and information held on them is through using a desktop terminal, remote access laptop and/or mobile device (such as a Blackberry 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 [ICT Security - Information Classification and Handling Policy](#).

General Security Operating Procedures (SyOPs)

The policy refers to a key set of general SyOPs which are listed below:

- [IT Security Operating Procedures - System Administrators](#).
- [IT Security Operating Procedures - Administrators and Users](#).
- [Remote Working](#).
- IT Security Operating Procedures - ICT Equipment: Desktop – Corporate.
- IT Security Operating Procedures - ICT Equipment: Mobile Devices - RAS Laptop.
- IT Security Operating Procedures - ICT Equipment: Mobile Devices – Blackberry.

To minimise the number of SyOPs in circulation and standardise procedures, the SyOPs listed above act as the primary set where individual ICT systems are expected to conform to in terms of their own SyOPs. Any deviations or additions are at the discretion of the system Accreditor.

POL.ITAUP.008

All ICT systems **must have** documented SyOPs which comply with the general SyOPs listed in this policy (see [here](#)). Any deviations or additions must be recorded in separate SyOPs which form an addendum to one of the SyOPs listed [here](#).

Note – An ICT system may make use of, in their entirety, one or more of the SyOPs listed above as the procedures of that IT system do not deviate from those described in these general SyOPs.

Removable Media

Removable storage media include devices such as USB memory sticks, writeable CDs/DVDs, floppy discs and external hard drives. These devices can potential contain large amounts of protectively marked data and pose a significant risk to the Confidentiality of data held on them. As such, the MoJ controls the use of removable media through SyOPs, technical security controls, and requiring movements of bulk data to be authorised by MoJ ICT IA, this includes completing an Information Asset Movement Form.

POL.ITAUP.009

Any removable media device **must be** approved by MoJ ICT IA where that device is used to store protectively marked data. The type of device and associated SyOPs must be approved by the system Accreditor prior to operational use.

POL.ITAUP.010

All Users **must ensure** that all data stored on or transported by removable media is in accordance with the applicable system SyOPs.

POL.ITAUP.011

All Users **must seek** approval from MoJ OST prior to any bulk transfer of protectively marked data using removable media. MoJ ICT IA will advise on any technical and procedural requirements such as data encryption and handling arrangements.

Passwords

The username and password combination, in the main, is the primary access credential used for authenticating a User to an ICT systems and authorising their 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 **must not** share or disclose any passwords with any other person.

POL.ITAUP.013

All Users **must not**:

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

Legal and regulatory requirements

There are a number of legal and regulatory requirements for which the MoJ must comply with, this in addition to HMG security policy as expressed in the [HMG Security Policy Framework](#).

POL.ITAUP.014

All Users **must be** made aware of legal and regulatory requirements they must adhere to when accessing MoJ ICT systems. This must be included as part of the SyOPs.

MoJ's Corporate Image

Communications sent from MoJ ICT systems or products developed using them (e.g. MoJ branded document or PowerPoint presentation) can damage the public image of the MoJ if, it is for purposes not in the interest of the MoJ, or, it is abusive, offensive, defamatory, obscene, or indecent, or, of such a nature as to bring the MoJ or any its employees into disrepute.

POL.ITAUP.015

All Users **must ensure** that MoJ ICT systems are not used in an abusive, offensive, defamatory, obscene, or indecent, or, of such a nature as to bring the MoJ or any its employees into disrepute.

Potential to cause offence and harm

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

POL.ITAUP.016

MoJ ICT systems **must not** be used for any activity that will cause offence to MoJ employees, customers, suppliers, partners or visitors, or in a way that violates the [MoJ Code of Conduct](#).

Personal use

The MoJ permits limited personal use of its ICT systems provided this does not conflict or interfere with normal business activities. The MoJ monitors the use of its IT systems and any personal use is subject to monitoring and auditing (see [here](#)), and may also be retained in backup format even after deletion from live systems.

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

- Filtering of Internet and e-mail traffic – All Internet and e-mail traffic is filtered and analysed, further details are provided [here](#).

- Policy and procedures – This policy and associated SyOPs set out the restrictions placed on the use of an ICT system.

POL.ITAUP.017

Users **must ensure** any personal use of MoJ ICT systems does not conflict or interfere with normal business activities. Any conflict is to be reported to their line manager.

POL.ITAUP.018

Users **must ensure** that any personal use of MoJ ICT systems is inline with any applicable SyOPs and this policy.

POL.ITAUP.019

Users **must be** aware that any personal use of MoJ ICT systems which contravenes any applicable SyOPs, or this policy, constitutes a breach of the IT Security Policy and may result in disciplinary action.

Maintaining system and data integrity

Users need to 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 will affect either the integrity of that system or the integrity of shared data needs to be undertaken or supervised by authorised User or system Administrator.

POL.ITAUP.020

All Users **must request** any changes to ICT system/s or ICT equipment through the IT helpdesk. Further details are provided in [IT Security Operating Procedures - Administrators and Users](#).

Electronic messaging and use of the Internet

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

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

Also, the use of any high bandwidth services, such as video steaming websites, creates network capacity issues which cause the poor performance key MoJ ICT services. As such, the MoJ restricts access to the Internet based on job role. Amendments can be made on the submissions of a business case for approval by MoJ Operational Security Team (OST).

The MoJ will regard as a disciplinary offence any usage of electric communications (e-mail and other methods such as instant messaging) and the Internet which, breaks the law, contravenes MoJ HR policies, or involves unauthorised access or handling of material that is deemed to be inappropriate, abusive, offensive, defamatory, obscene or indecent.

External E-mail 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 MoJ deploys a number of security controls to protect its Users from Internet and e-mail borne attacks, however these controls are reliant on Users to remain vigilant, follow any applicable SyOPs, and report any suspicious behaviour.

POL.ITAUP.021

All Users **must use** the Internet and e-mail (and other electronic communication systems) in accordance with this policy document.

Managing e-mail use

Users are responsible for ensuring that all information is handled in line with protective marking of that information in accordance with [IT Security - Information Classification and Handling Policy](#).

The MoJ is connected to the Government Secure Intranet (GSi), which provides a secure environment for sending/receiving E-mails between Government departments. This allows Users with a MoJ E-mail account (e.g. suffix

'@justice.gsi.gov.uk') to send E-mails which attracts a protective marking up to and including RESTRICTED to another MoJ or government User where their E-mail suffix ends in '.gsi.gov.uk'.

POL.ITAUP.022

All Users **must ensure** that protectively marked information contained within or attached to an e-mail is handled in accordance with [ICT Security - Information Classification and Handling Policy](#).

E-mail is a major source of malware and route into the MoJ for criminal organisations to defraud staff or exfiltrate information. All Users need to exercise care when handling emails and report any suspicious activity as an IT security incident.

POL.ITAUP.023

All Users **must ensure** that they do not:

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

POL.ITAUP.024

Where a User suspects that an E-mail received is from an untrusted, unknown or unsolicited source, they **must** report it as an IT security incident.

Connectivity and remote access

Remote access is provided to MoJ ICT systems and services allowing Users access from offsite and home locations to connect in. The main methods of access are either via a RAS laptop and/or Blackberry device. In the main, remote access is to a protectively marked MoJ IT system (up to and including RESTRICTED). As such Users need to be aware of both the security controls and procedures of the device used as well as the general physical security considerations. This includes any restriction on the carriage of such devices as they may contain HMG protectively marked data and HMG cryptographic material.

MoJ ICT IA 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 **must be** aware of the [Remote Working](#) guidance and must confirm that they have read and understood it before being provisioned with any remote access devices or equipment (e.g. RSA token).

POL.ITAUP.026

Any User wishing to take a remote access device out of the UK **must consult** [Remote Working](#) guidance before doing so or the applicable device IT Security Operating Procedures document.

Monitoring of communications

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.

The MoJ monitors telephone usage, network, email and Internet traffic data (including sender, receiver, subject; attachments to an e-mail; 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.

The MoJ, so far as possible and appropriate, respects the privacy and autonomy whilst working of all Users, but further to [this information](#), any personal use of MoJ ICT systems will also be subject to monitoring. By carrying out personal activities using MoJ ICT systems, Users are consenting to the MoJ processing any sensitive personal data which may be revealed by such monitoring (for example regular visits to a set of websites).

For the purposes of business continuity it may sometimes be necessary for the MoJ to access business communications (including within e-mail mailboxes) while a User is absent from work (including holiday and illness). Access will only be granted through submission of a formal request to the IT Helpdesk where approval is required from the relevant line manager where the MoJ ITSO and MoJ HR may be consulted.

POL.ITAUP.027

All Users **must be** aware their electronic communications are being monitored in accordance with this policy.

POL.ITAUP.028

All Users **must be** aware that business communication (such as e-mail mailboxes) may be accessed if they are absent from work. This can only be requested and authorised by a line manager where the MoJ ITSO and MoJ HR may be consulted.

Guidance on IT Accounts and Assets for Long Term Leave

Audience and Document Purpose

This document is intended for Ministry of Justice (MoJ) 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 MoJ, **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 at: <https://intranet.justice.gov.uk/guidance/security/it-computer-security/acceptable-use/>
- 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 at: <https://intranet.justice.gov.uk/guidance/security/emergencies/coronavirus-guidance/security/remote-working/>.

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 MoJ, 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 OFFICIAL-SENSITIVE. This is in line with the necessity rigorously to apply the “need to know” principle for OFFICIAL-SENSITIVE information. See 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 above 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 [MoJ Technology Portal](#). Please see the Knowledge Base article on “Returning your MoJ 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. See the Knowledge Base article on “How to Re-instate a Deactivated Email Account or Mailbox”.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

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 see 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, see the [Acceptable Use guidance](#).

Information classification

Data Handling and Information Sharing Guide

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

Overview

Introduction

The [Government Functional Standard - GovS 007: Security](#) identifies mandatory requirements about the value and classification of information assets. To comply with these requirements, the MoJ needs to ensure that:

Where information is shared for business purposes, departments and agencies must 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 must 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 MoJ guidance sharing information within the MoJ 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 OFFICIAL with the SENSITIVE handling caveat, often written as OFFICIAL-SENSITIVE. While this approximate correspondance might be helpful, you should always review classification where older terms are used, to ensure that the correct current classification is used.

Scope

The MoJ Information Assurance (IA) team provide general guidance on the handling of protectively marked data, whilst this document concentrates on providing guidance on information stored on MoJ IT systems and exchanged electronically within the MoJ and with external parties.

This guide is split into three sections:

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

A [Data Movement Form](#) must be completed for all transfers where information is transferred from an MoJ IT system to another MoJ IT system or external party. Further details on the form can be found [here](#).

Note: This document provides guidance for handling and sharing of information and data up to and including OFFICIAL and OFFICIAL-SENSITIVE, or the older Impact Level (IL) 3. Where information attracts a high protective marking or IL, advice must be sought from the MoJ Operation Security Team (OST) and MoJ IT Security Officer (ITSO).

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 MoJ will need to demonstrate compliance against this requirement.

Handling data on MoJ IT systems

This section covers how data must be handled on MoJ 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 **SENSITIVE**. See the [Information Classification and Handling Policy](#) for further details.

Ownership of information

All MoJ 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 must 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 must 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 MoJ 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 MoJ preference for transferring data is to use a secure accredited government network whether that is a MoJ 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 **OFFICIAL-SENSITIVE**, 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. See the [Access Control Guide](#) for further information.

Any additional controls must be captured on the DMF (see [Data Movement Form](#) where advice should be obtained from the MoJ Chief Information Security Office (CISO) 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, see 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 must be sought from the Operational Security Team: OperationalSecurityTeam@justice.gov.uk, or CISO on the best option to use when completing the DMF (see [Data Movement Form](#)).

Optical media

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

Data at rest on MoJ-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. MoJ-issued laptops use an approved whole disk encryption product. This allows data to be safely stored.

Disposal and decommissioning

Sensitive data must not be kept for longer than is needed. The IAO must check for compliance, including any mandatory retention period.

Physical media containing sensitive data must 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 must 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 must ensure that any data shared can be adequately secured by the recipient. The sensitivity of data must 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

MoJ staff, including contractors and agency staff, must 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 MoJ staff must avoid exposing sensitive data to unnecessary risks, in particular by observing all aspects of the MoJ [Acceptable Use Policy](#).

Authorisation must 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 MoJ, and to help you complete a DMF.

Internally within the MoJ

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

Where information is transferred between MoJ 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, by enabling proof of sending or proof of receipt.

Information transferred between two MoJ IT systems requires a completed and authorised [Data Movement Form](#) using one of the [data in transit](#) options.

Information sharing with other HMG department

Information shared with another government department must be transferred to an assured system. This means the system must be assured to the same level as the data being transferred. The transfer must 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, MoJ 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, must be authorised by the relevant IAO. An appropriate contract, [Data Movement Form](#), and Non-disclosure Agreement (NDA) must 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 OFFICIAL-SENSITIVE, it must 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 must be undertaken with appropriate security controls in place, using the guidance from this document, and seeking advice from Information Assurance and the MoJ CISO as required.

Sharing across an unsecured network

Sensitive data must 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 e-mail.

Sharing information above OFFICIAL

Where there is a business requirement to share information classified higher than OFFICIAL, advice must be sought from the Operational Security Team: OperationalSecurityTeam@justice.gov.uk or CISO prior to completing a [Data Movement Form](#).

Data Movement Form (DMF)

The purpose of the DMF is to ensure that the movement of information assets is secure, and in compliance with the [Government Functional Standard - GovS 007: Security](#).

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

Using SecureZIP

SecureZip is a compression and encryption product which can be used to encrypt sensitive data for use in removable media and e-mail 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 e-mail 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.

Best practices for everyone

The MoJ 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.

If a system or another person provides you with a password, change it before doing any MoJ 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 must 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 must 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

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Government Classification Scheme

These summary guidelines are based on “The Government Security Classification (GSC)” as issued by the Cabinet Office in 2018. The link below provides full handling guidance for information classifications including OFFICIAL, SECRET and TOP SECRET:

<https://www.gov.uk/government/publications/government-security-classifications>

In summary, the majority of information that is created or processed by the public sector is now classified as OFFICIAL. The other two classifications are SECRET and TOP SECRET.

SECRET classification should be used on very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors.

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

Classifications can have additional indicators, providing extra information about looking after the information with that classification. A frequently-seen example is OFFICIAL-SENSITIVE. This is still classified as OFFICIAL, but there is an additional indicator that tells you the information is of a more sensitive nature, and so should be handled and looked after accordingly.

Information Classification, Handling and Security Guide

Introduction

All Ministry of Justice (MoJ) employees interact with information, and are responsible for its protection. Information security must be considered during the process of designing, maintaining, and securing the MoJ'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 MoJ – 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 MoJ uses are OFFICIAL, SECRET, and TOP SECRET. This follows the [HMG Government Security Classifications Policy](#).

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
OFFICIAL	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 OFFICIAL information, someone would be expected to have achieved Baseline Personnel Security Standard (BPSS) assessment.
SECRET	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 SECRET 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 SECRET assets, or be required to work in areas where SECRET or TOP SECRET information might be overheard.
TOP SECRET	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 MoJ'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 MoJ'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 OFFICIAL information. Within this, some production data might be classified as SECRET information.
- Most personal data is OFFICIAL information. Within this, some personal data might be classified as SECRET information if it meets the risk threshold defined.

The table below 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
OFFICIAL	<p>All information related to routine public sector business, operations and services.</p> <p>Almost all personal information falls within the OFFICIAL classification.</p> <p>OFFICIAL-SENSITIVE is not a separate security classification. It should be used to reinforce the “need to know” principle, beyond the baseline for OFFICIAL.</p>	OFFICIAL data does not need to be marked except where SENSITIVE, and must be marked OFFICIAL-SENSITIVE.
SECRET	Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime.	Must be marked
TOP SECRET	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 below:

- 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 [MoJ Data Destruction guide](#) to understand when the disposal should be witnessed and recorded.

OFFICIAL and OFFICIAL-SENSITIVE

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

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

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

Use **OFFICIAL-SENSITIVE** 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 **OFFICIAL** classification.

SECRET

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

SECRET information should not usually be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is **SECRET**, contact the Cyber Assistance Team (CAT) immediately: CyberConsultancy@digital.justice.gov.uk.

To help decide whether some information should be classified as **SECRET**, 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 **OFFICIAL** classification.

TOP SECRET

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

TOP SECRET information should not be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is **TOP SECRET**, contact the Cyber Assistance Team (CAT) immediately: CyberConsultancy@digital.justice.gov.uk.

To help decide whether some information should be classified as **TOP SECRET**, 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 **OFFICIAL** or **SECRET** classification, as appropriate.

Reclassifying information

The asset owner has responsibility for reclassifying an asset. If another user has reason to believe that an asset is incorrectly classified or has an incorrect handling caveat, they should normally discuss this with the asset owner. The other user cannot unilaterally reclassify the asset.

The exception is where the asset might need a higher classification than that assigned by the asset owner. The reclassification must still be communicated to the asset owner, for consistency. If it is agreed that the classification should be increased, check with the Operational Security Team (OperationalSecurityTeam@justice.gov.uk) whether additional actions are required to protect the material.

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 **SECRET**. 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 **OFFICIAL**, with the **SENSITIVE** 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 **OFFICIAL**, with the **SENSITIVE** 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 **SENSITIVE** handling caveat is not required.

The original report retains its **OFFICIAL** classification and **SENSITIVE** 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 **OFFICIAL**, with the **SENSITIVE** 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 **SECRET**. They discuss this decision with the asset owner, so that the original report is correctly reclassified.

Handling and securing information

The [HMG Government Security Classifications Policy](#) 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 **OFFICIAL** and **OFFICIAL-SENSITIVE** information

Type	Measure	Example
PERSONNEL	Make sure all MoJ staff including contractors undergo baseline security clearance checks.	A contractor working with the MoJ Security Team must undergo a baseline background check (i.e. BPSS check) at minimum. Refer to Security Vetting Guidance .
PHYSICAL	<p>Make sure that you lock your screen before you leave your desk.</p> <p>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.</p> <p>The MoJ has additional requirements when moving assets which can be found in the HMG Government Security Classifications Policy.</p>	A software developer working from a flatshare should take calls in private, and use headphones and a privacy screen.

Type	Measure	Example
TECHNICAL	Transferring information from one location to another requires planning and preparation, including a risk assessment. More information on this is available in the HMG Government Security Classifications Policy , and from your manager.	A technical architect working on the requirements for a new MoJ platform should lock their laptop before leaving their desk.
	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 Digital Marketplace (GCloud) 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.
	Digital Marketplace (GCloud) services can be used for OFFICIAL 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 MoJ 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 [HMG Government Security Classifications Policy](#) for further guidance.

Handling and securing **SECRET** information

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

Type	Measure	Example
PHYSICAL	<p>Consider using multiple layers of security to protect SECRET information. SECRET information should be held on a secure computer network which is physically isolated from unsecured networks and the internet.</p> <p>Transferring SECRET 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 HMG Government Security Classifications Policy and from your manager.</p>	<p>Imagine you are moving locations for a server used to host SECRET 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.</p>
TECHNICAL	<p>SECRET information at rest should be protected with very strong encryption. Contact the MoJ Security Team for more information: security@justice.gov.uk.</p> <p>Care should be taken to ensure that SECRET information in transit is only shared with defined recipient users through assured shared infrastructure or using very strong encryption.</p> <p>SECRET information should be processed on IT systems which have been approved for the SECRET threat model. Advice on what commercial IT systems meet this requirement is available from the MoJ Security Team: security@justice.gov.uk</p>	

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 [HMG Government Security Classifications Policy](#) for further guidance.

Handling and securing TOP SECRET information

Type	Measure	Example
PERSONNEL	Ensure employees and contractors undergo Developed Vetting (DV) security clearance checks.	A contractor working with the MoJ Security Team should have at least DV clearance before being allowed to access TOP SECRET information.
PHYSICAL	<p>Handling and storing TOP SECRET information requires exceptional planning, monitoring, and record-keeping.</p> <p>Working remotely with TOP SECRET is not permitted due to the extreme sensitivity of the information.</p> <p>Transferring TOP SECRET information from one location to another requires even greater planning and preparation than for SECRET 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 HMG Government Security Classifications Policy and from your manager.</p>	<p>Imagine you are moving locations for a server used to host TOP SECRET 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.</p>
TECHNICAL	When physical security measures cannot be used, TOP SECRET information at rest should be protected with extremely strong encryption. Contact the MoJ Security Team in these circumstances: security@justice.gov.uk .	

Type	Measure	Example
	<p>Care should be taken to ensure that TOP SECRET information in transit is only shared with defined recipient users through accredited shared infrastructure or using extremely strong encryption.</p> <p>TOP SECRET information should be processed on IT systems which have been approved the TOP SECRET threat model. Advice on what commercial IT systems meet this requirement is available from the MoJ Security Team: security@justice.gov.uk.</p>	

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 [HMG Government Security Classifications Policy](#) for further guidance.

Note: For further information on statutory disclosures and transfer to national archives, please refer to the [HMG Government Security Classifications Policy](#).

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Information Classification and Handling Policy

Introduction

This document provides the core set of IT security principles and expectations on the handling and classification of information on Ministry of Justice (MoJ) IT systems.

The MoJ stores and processes a wide variety of information, some of which attracts an HMG protective marking or contains personal information. The MoJ 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 MoJ IT systems.

Scope

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

The overarching policy on information classification and handling is maintained by [MoJ 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 MoJ business groups, where the responsibility resides with the business group SIRO.

All MoJ 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 MoJ, 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 MoJ 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 [MoJ IT Security Policy](#), all MoJ 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/>.

Reclassifying information

The asset owner has responsibility for reclassifying an asset. If another user has reason to believe that an asset is incorrectly classified or has an incorrect handling caveat, they should normally discuss this with the asset owner. The other user cannot unilaterally reclassify the asset.

The exception is where the asset might need a higher classification than that assigned by the asset owner. The reclassification must still be communicated to the asset owner, for consistency. If it is agreed that the classification should be increased, check with the Operational Security Team (OperationalSecurityTeam@justice.gov.uk) whether additional actions are required to protect the material.

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 OFFICIAL or higher. This includes, but is not limited to, printed reports, removable media, electronic messages (such as e-mail) 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 Chief Information Security Office (CISO).

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 CISO.

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 MoJ IT systems

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

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

OFFICIAL, OFFICIAL-SENSITIVE

h/t <https://www.gov.uk/guidance/official-sensitive-data-and-it>

OFFICIAL

OFFICIAL is a UK HM Government information asset classification under the [Government Security Classifications Policy \(GSCP\)](#).

OFFICIAL-SENSITIVE

OFFICIAL-SENSITIVE is **not** a classification. SENSITIVE is a handling caveat for a small subset of information marked OFFICIAL that require *special* handling by staff above and beyond the decribed OFFICIAL baseline.

The SENSITIVE handling caveat is a *reminder* as opposed to a requirement for additional controls nor a description of a minimum set of controls.

DESCRIPTORS

Descriptors *can* be applied (but they do not need to be) to help identify certain categories of SENSITIVE information.

Descriptors should be applied in the format OFFICIAL-SENSITIVE [DESCRIPTOR]

The Cabinet Office maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments:

- **COMMERCIAL**: Commercial- or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed.
- **LOCSEN**: Sensitive information that locally engaged staff overseas cannot access.
- **PERSONAL**: Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals, or the personal / medical records of people in sensitive posts (e.g. military, SIA).

Descriptors are **not** codewords.

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 SECRET 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 Ministry of Justice (MoJ) 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

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

What is 'removable' media?

Laptops and [USB memory sticks](#) are the MoJ'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.

MoJ 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 MoJ-approved USB sticks with device encryption be used.

USB memory sticks

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

1. You must only connect approved external removable storage media to MoJ systems.
2. Connecting non-approved memory sticks is a breach of MoJ 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: OperationalSecurityTeam@justice.gov.uk.

4. Each request is evaluated by MoJ 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 MoJ 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 MoJ's recognised central procurement systems are encrypted and protected to MoJ security standards. You must use MoJ processes to obtain any equipment used for business purposes, including mobile computing devices and removable media.

What's expected of you

Keeping MoJ 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Secure Disposal of IT Equipment

The Ministry of Justice (MoJ) and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, including desktop computers, laptops, USB memory sticks and other mobile devices. This equipment is procured and managed through MoJ suppliers, who are normally responsible for the secure disposal of the equipment when it is no longer used. Typically, a supplier managed device will have a supplier asset tag on it, making it easier to identify who to ask for help with disposal.

However, there are also other devices across the MoJ 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.

To determine the correct disposal requirement, use the following table to identify the correct outcome, depending on the type of equipment and its security classification. If the table does not cover your exact requirement, contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

Note: When disposing of SECRET or TOP SECRET equipment or materials, always contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

Equipment or asset type	Data deletion method	Disposal 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	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 4 pieces. This can be done either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a Lower Level degauss and then apply a destructive procedure that prevents the disk from turning. For example, punch holes into the platters, or twist or bend them.

Equipment or asset type	Data deletion method	Disposal method
Magnetic tapes and floppy disks	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. See also the note following 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. A high capacity CD and DVD shredder is available at 102 Petty France, suitable for items up to TOP SECRET. Contact OperationalSecurityTeam@justice.gov.uk for help with this option.

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 above. Assurance shall be required that the appropriate destruction has taken place for any locally procured MoJ assets, and that an audit trail is available for inspection upon request by MoJ security.

Wherever possible and appropriate, managers should pool together equipment with that of local colleagues to share service costs.

If you have any concerns about moving items between sites securely, contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

Contacts

The following organisations are approved to help you with security disposal of equipment:

- TYR security: g-cloud@tyr-security.co.uk
- Data eliminate: info@dataeliminate.com

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Access control

Business requirements of access control

Access Control guide

Introduction

This guide explains how the Ministry of Justice (MoJ) 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.

Who is this for?

This guide is aimed at two audiences:

1. The in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation.
2. Any other MoJ 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.

Related guides

Further guidance on how to manage user access can be found in the guides below.

- [Privileged Accounts](#).
- [Management Access](#).
- [Minimum User Clearance Requirements](#).
- [Multi-Factor Authentication \(MFA\)](#).

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 MoJ 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 (see the [Accounting section below](#) for further information).
2. **Authentication:** To access MoJ systems, users must authenticate themselves. They can do so using:
 - something they know (such as a password - the primary authentication method used at the MoJ)
 - 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 MoJ, must use Multi-Factor Authentication (MFA) to prove user identity. See 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 Center's (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 see 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 Privacy Team for advice on protecting sensitive personal information - privacy@justice.gov.uk.
- 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 MoJ Data Protection Officer if a Log involves personal information. See the [Accounting Guide](#) for further information.
- tampered with under any circumstances, for example through modification or removal.

See the [Security Log Collection Guide](#) for more information.

Segregation of duties

In some parts of the MoJ, 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)

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Enterprise Access Control Policy

All Ministry of Justice (MoJ) 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 MoJ 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 MoJ IT systems starting from when a User is initially registered through to the revocation of access rights and removal of their User account.

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).

- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI ([Centre for the Protection of the National Infrastructure](#)), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

User and Information Access management

Access control is primarily about enforcing three information security principles:

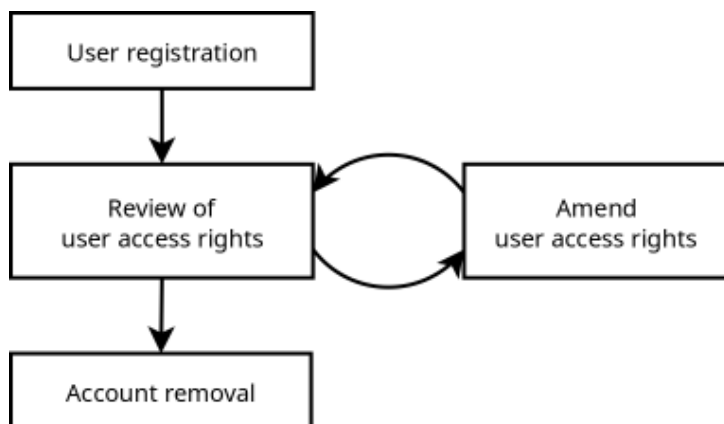
- The '*need-to-know*' principle – restricting access to information based on a business requirement.
- *Non-repudiation* of User actions –holding a User accountable for their actions on an IT system.
- The '*least privilege*' principle – assigning the least number of privileges required to fulfil their work.

At a high level, access control in MoJ 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 MoJ 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 (see [here](#) for 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 MoJ 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 MoJ member of staff this is confirmed by MoJ HR;
- The access rights required must be supplied (for example, the list of RBAC groups and/or applications);
- Confirmation of clearance level (see [here](#) for further details);
- The application for User registration must be authorised by a MoJ 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 MoJ 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 MoJ IT systems, application and information. Temporary use of a MoJ IT system may be permitted where a specific business need exists (e.g. to allow an external trainer to train MoJ staff in a new application) subject to clearance checks and a Non-Disclosure Agreement (NDA). A MoJ senior manager must assume total responsibility for the actions undertaken by that temporary User while they are using a MoJ IT system using a temporary account.

Minimum user clearance requirements

Most MoJ 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
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 MoJ IT system. Most job roles at the MoJ 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 MoJ 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 MoJ 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

MoJ 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 MoJ 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 MoJ, 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 MoJ 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 MoJ senior manager or Senior Civil Servant (SCS). Further advice must be sought from the MoJ ITSO.

Access to knowledge repositories

Knowledge repositories such as TRIM, are intended to host generally accessible information (but still internal to the MoJ), 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 MoJ 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 MoJ 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 above 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 MoJ 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 MoJ 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 MoJ 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 MoJ HR to identify which accounts can be removed (as the User has left the MoJ) or require deactivation (as the User is on long term leave).	Every 3 months
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 MoJ 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 Ministry of Justice (MoJ) has published the [MoJ Password Standard](#).

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 keypairs 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).

MoJ 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

Introduction

This guide provides information on the authentication methods which should be used to manage user access to systems and information in the Ministry of Justice (MoJ). This is a sub-page to the [Access Control Guide](#).

Managing access to MoJ systems

The following methods can be used to manage access to the MoJ'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. See the [GDS guide](#) for more information.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Minimum User Clearance Requirements Guide

Introduction

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 [Access Control Guide](#).

Security clearance levels

The Ministry of Justice (MoJ) 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 MoJ IT systems are able to process OFFICIAL information. Therefore all roles in the MoJ require staff to attain BPSS clearance as a minimum to be granted access rights to view OFFICIAL 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 MoJ 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 above tasks, then BPSS, DBS or Enhanced Check is sufficient.

The MoJ 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 Cyber Assistance Team and refer to the [Vetting Policy](#) for further information.

Checking someone's clearance status

To check someone's clearance status, collect the following information:

- Their firstname.
- Their lastname.
- Their date of birth.

Send this information to the MoJ Group Security Team, by emailing: mojgroupsecurity@justice.gov.uk. The team will check with the Cluster, to determine the individual's clearance status, if any. If you are authorised to receive the answer, the team will reply to you with the answer.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Multi-Factor Authentication (MFA) Guide

Introduction

This Multi-Factor Authentication (MFA) guide explains how MFA can be used to ensure that users are only granted access to Ministry of Justice (MoJ) information once their identity is confirmed. This is a sub-page to the [Access Control Guide](#).

MFA

Users should have their identity authenticated through the following methods:

- something they know (such as a password)
- something they have (such as a mobile phone or smart card), and/or
- something they are (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 should be taken to ensure true MFA. For example, password and security questions are both dependent 'something the user knows' and therefore are just one factor of authentication.

The list below identifies the MoJ's preference for MFA methods, with 1 ranked the highest. These methods can be used for 2, 3, 4, or 5 Factor Authentication as required.

Note:

- MFA Type 1 may not be suitable for all systems. In that case, other methods of delivering MFA should be considered to provide additional protection beyond single sign on.
- MFA types 5 and 8 should only be used when no other MFA method is appropriate as these methods can be easily spoofed or circumvented.

Preference	Type
1.	Hardware-based (for example, Yubikeys or TPM enabled devices)
2.	Software-based (for example, Google Prompt on a 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 factor information)
5.	Certificate-based (a digital certificate used to authenticate a user)
6.	Email-based (a one-time code/link sent to the registered on-file email address)
7.	SMS-based (a one-time code sent via SMS)
8.	Phone-call based (a phone call providing a one-time code or password)

The [MoJ Password Guide](#) provides more information on the use of MFA.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Privileged Account Management Guide

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 Ministry of Justice (MoJ) systems. The MoJ 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
<p># 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.</p> <p># 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 MoJ. This should be enforced through the principle of least privilege.</p> <p># 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. See 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.</p> <p># 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.</p> <p># 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.</p> <p># Ensure that default passwords are managed securely and safely, as described in the Password Manager guidance.</p>
DON'T
<p># 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'.</p> <p># Leave default or factory set passwords for any accounts but particularly for privileged system accounts, social media accounts and infrastructure.</p> <p># Allow a user to have a privileged account, unless they are a service provider and require a privileged account for that specific service.</p>

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

User responsibilities

Protecting Social Media Accounts

Summary

Hostile attacks on Social Media accounts pose a serious threat to the Ministry of Justice (MoJ) 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 see 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.

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](#)
- [Twitter](#)
- [Instagram](#)

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 MoJ 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 through social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

For more information, read [this article](#) on the MoJ 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.

Cyber Security Advice

Cyber Consultants & Risk Advisors

- Email: security@justice.gov.uk
- Slack: #security

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, see 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 Ministry of Justice (MoJ) 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.

Account lockouts

Account lockouts must be implemented within MoJ 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 Technology Service Desk.

Unsuccessful connection attempts.

Allow no more than 10 consecutive login attempts before logout.

Forgotten passwords.

All MoJ 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 MoJ, 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 timeframes:

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 MoJ 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 MoJ revokes user accounts in alignment with the [Access Control Guide](#).

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

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 (PoLP; 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 who has higher levels of access or control than a required for day to day operation.

Examples include those with high privileges on a Ministry of Justice (MoJ) github.com repository and credentials to the MoJ 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 privileged configurations.

Where possible, IAM Roles should be used.

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.

H/T <https://medium.com/@joelgsamuel/ip-address-access-control-lists-are-not-as-great-as-you-think-they-are-4176b7d68f20>

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, see 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 Ministry of Justice (MoJ) 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 MoJ.

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 Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

- 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, see 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 MoJ 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Password Creation and Authentication Guide

Introduction

This guide sets out considerations for creating passwords and authenticating users for access to Ministry of Justice (MoJ) systems. This includes ensuring that there are appropriate authentication methods for information, accounts and systems. For more information, see 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 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, see the [Passwords](#) guidance.

Password history and block listing

The MoJ 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 MoJ 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 MoJ 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 MoJ 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 OFFICIAL 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 in progress for a privileged account.

Further guidance around the use of Multi-Factor Authentication can be found in the [Authentication](#) guide.

Single-Sign On

MoJ SSO solutions include Office 365, and Digital and Technology G-Suite. SSO solutions must be integrated within the MoJ application development and service delivery environment, to improve user experience by authenticating to systems using existing MoJ 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 MoJ 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Password Management Guide

Introduction

This guide sets out the roles and requirements for setting and maintaining strong passwords across Ministry of Justice (MoJ) systems.

The information is aimed at two audiences:

- The in-house MoJ 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 MoJ 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.

Roles and responsibilities

All MoJ 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 leveraged by the MoJ.
- 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 MoJ.

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 MoJ 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 MoJ. 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.

Related guides

Further guidance around the management of passwords at the MoJ is available:

- The [Account management](#) guide explains why you might need to change your password. It also addresses when and how you should change your password.
- The [Multi-User Accounts and Public-Facing Service Accounts Guide](#) explains when you should use a multi-user account and how you should authenticate a service account.
- The [Password Creation and Authentication Guide](#) helps ensure you choose the correct passwords and authentication tools to protect information in line with its security classifications.
- The [Password Storage and Management Guide](#) provides help on storing and sharing passwords securely.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Password Managers

Overview

[Ministry of Justice \(MoJ\) 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 MoJ.

What is a password manager/vault?

A password manager stores sensitive information in an encrypted form. Password managers are sometimes called password vaults.

In the MoJ, '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 do you 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.
System access, no human use	Password vault	Some MoJ 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 MoJ, as much of our IT Policy and guidance derives from NCSC best practices.

What makes a good password manager?

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 should I 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 MoJ guidance.

There are several password managers used within the MoJ. [LastPass](#) and [1Password](#) are probably the most popular for personal or team passwords. Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at LastPass and 1Password. See which one you like best, and 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?".

See also [Using LastPass Enterprise](#).

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Passwords

Overview

This article provides guidance on passwords within the Ministry of Justice (MoJ). It helps you protect MoJ IT systems by telling you about choosing and using passwords. Whenever you see 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 password guidance is for all users. It also includes more detail for system administrators or developers.

Best practices for everyone

The MoJ 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.

If a system or another person provides you with a password, change it before doing any MoJ 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 must 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 must 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

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 MoJ 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 MoJ 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 MoJ Digital & Technology use [LastPass](#).

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 MoJ 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 must ensure that systems support the password requirements. Systems must be able to issue, change, reset, and revoke passwords. This must be possible using well-defined and fully-described processes. Supply enough information and procedures to fulfil MoJ 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.

Related guides

Further guidance around the management of passwords at the MoJ is available:

- The [Account management](#) guide explains why you might need to change your password. It also addresses when and how you should change your password.
- The [Multi-User Accounts and Public-Facing Service Accounts Guide](#) explains when you should use a multi-user account and how you should authenticate a service account.
- The [Password Creation and Authentication Guide](#) helps ensure you choose the correct passwords and authentication tools to protect information in line with its security classifications.
- The [Password Storage and Management Guide](#) provides help on storing and sharing passwords securely.

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 must 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, see the [Multi-user accounts and Public-Facing Service Accounts Guide](#).

Service Accounts

System and application authentication must 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 must:

- 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, see 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 MoJ work.

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.

Use MFA in systems for privileged or important step confirmation. For example, the user must enter their MFA code when deleting a record.

Follow the [NCSC guidance](#) for enabling MFA.

Use [Time-based One-Time Password Algorithm \(TOTP\)](#) or hardware and software tokens. 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 must 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.

For more information, see the [Multi-Factor Authentication \(MFA\) Guide](#).

Extra measures

Check that a system, service, or information protected by a password is not [classified](#) as SECRET or TOP SECRET. 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 must remember. For more information about authentication, see 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 must 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 Cyber consulting team: CyberConsultancy@digital.justice.gov.uk, or the security team: security@justice.gov.uk

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 MoJ Service Desk. 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 must 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 must 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, see 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 must immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they must 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 must 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, see 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 MoJ 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 MoJ credentials.

For more information, see 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, see the [Account management](#) guide.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Password Storage and Management Guide

Introduction

Do not attempt to implement your own password storage mechanism. Always use an existing, approved Ministry of Justice (MoJ) password storage solution.

This guide sets out how passwords must be stored securely to prevent unauthorised access or compromise. The MoJ encourages the use of password managers to reduce the burden on users for maintaining password security. For more information, see the [Password Management Guide](#).

This guide has been written in alignment with [NCSC guidance](#).

Password storage

Passwords must be securely stored within MoJ approved storage tools. The following tool is approved and preferred for use:

- [LastPass](#)

Contact the Cyber Assistance Team (CyberConsultancy@digital.justice.gov.uk) 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 MoJ prefers [LastPass](#) 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, see the [Password Creation and Authentication Guide](#). Contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk if you have a specialised need to use a different password manager or vault.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

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 CyberConsultancy@digital.justice.gov.uk.

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 Chief Information Security Office (CISO) for the Ministry of Justice (MoJ).
- The MoJ 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 CyberConsultancy@digital.justice.gov.uk.

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 Chief Information Security Office (CISO) for the Ministry of Justice (MoJ).

- The MoJ Digital Information Assurance Lead.

Actions:

1. Creating a Mac account for a non MoJ 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 Operational Security Team (OperationalSecurityTeam@justice.gov.uk) and inform MoJ security (security@justice.gov.uk) and the MoJ CISO when leaving Staff have not returned all MoJ 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 CyberConsultancy@digital.justice.gov.uk.

How to use this document

This policy applies to all staff and contractors who work for the Ministry of Justice (MoJ).

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	<p>Start-up:</p> <ul style="list-style-type: none"> • 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. <p>Shut-down:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 (see 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	<ul style="list-style-type: none"> • When visitors are present, ensure that they are only able to see 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 Service Desk.
System Use	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<p>In the event of a User suspecting a virus attack on the network, they must carry out the following steps:</p> <ul style="list-style-type: none"> • 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 Information Technology (IT) Helpdesk who will provide assistance.
Removable media	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> 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] OST 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	<ul style="list-style-type: none"> All requests for IT support and all reports of IT failures must be logged with the IT Helpdesk. 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] Operational Security Team (OST). Any loss of IT equipment, [ORGANISATION] or personal data should be reported. Report also to the Users' line manager, the OST (OperationalSecurityTeam@justice.gov.uk) and to the Data Access & Compliance Unit (DACU). <p>To ensure a quick response all emails must be marked Urgent and have 'Data Incident' in the title/subject heading.</p>

By signing below I acknowledge that I have read the Security Operating Procedures (SyOPs) and agree to be bound by them.

Name:

Date:

Signature:

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: #security

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk

- Tel: 0203 334 0324

Using LastPass Enterprise

What is LastPass?

LastPass 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.

LastPass is available as a browser extension for popular browsers and as well as a full software suite (for use outside of browsers) for Microsoft Windows and Apple macOS.

LastPass will securely save your credentials in your own LastPass 'Vault' and then offer to autofill those credentials the next time you need them.

The Ministry of Justice (MoJ) has the Enterprise tier of LastPass.

Who should use it?

MoJ LastPass accounts can be requested by anyone in MoJ Digital & Technology.

At the moment, rollout is limited to technical service/operation teams but we're working on license funding to make it available to everyone in D&T.

How to get it

Email lastpass-admins@digital.justice.gov.uk to request access.

Make sure you include in the email:

- which team you're in
- your role in your team / why you need access
- if there were any credentials within Rattic that you need access to based on this [shared spreadsheet of old Rattic credentials](#)

What it can be used for

LastPass can be used for storing usernames and passwords that are specific to you (for example, your MoJ Google account details).

LastPass can also 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.

Personal use

You could use your MoJ LastPass account to store personal non-work information but as it is a work account belonging to the MoJ you may lose access if you change role and will lose access entirely if you leave the MoJ.

MoJ LastPass administrators cannot routinely access the contents of LastPass Vaults but can reset accounts to gain access if there is a good reason to do so.

What it shouldn't be used for

LastPass should not be used for storing MoJ documents - you must use existing MoJ services such as Office 365 or Google Workspace for that.

You shouldn't use LastPass for 'secrets' that belong to systems, only credentials to be used by humans. There is separate guidance on how to handle [secrets](#).

How to use it

Getting started

You will be sent an email to your MoJ work email account inviting you to create your LastPass account. LastPass 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 must be at least 12 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](#) on the MoJ intranet.

Your primary password **must** be unique and you should **never** use it anywhere else (including a similar version, for example, by simply adding numbers to the end)

Multi-Factor Authentication

You **must** setup multi-factor authentication (MFA, sometimes known as 2FA) for your MoJ LastPass account.

LastPass has a [guide on setting up MFA](#).

The MoJ 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 MoJ-issued work smartphone you may use a personal device for MFA.

Sharing passwords

To share a password [create a 'shared folder' in the LastPass Vault](#).

You should make sure the credentials you're sharing are only available to the people who need to access them for MoJ work. It is your responsibility to remove items or people from shared folders when access to the credential(s) is no longer required.

(You must not share your LastPass main password with anyone, even your line manager or MoJ security.)

Using it overseas

Taking a device (such as personal smartphone) that has MoJ LastPass installed counts as travelling overseas with MoJ information.

The MoJ has existing [policies on travelling abroad on the MoJ intranet](#) which require various approvals before travel.

It may be simpler to 'log out' of the LastPass applications or uninstall/delete them before travelling outside of the UK and reinstalling when you get back.

Keeping LastPass update to date

Like all software, it is important to keep the software up to date (sometimes known as 'patching'). LastPass software generally should self-update to the latest version by itself however make sure you approve or apply any updates if LastPass asks you to.

Need help?

If you need help *installing* LastPass contact the relevant MoJ IT Service Desk.

If you need help using LastPass such as getting access to shared folders or resetting your primary password as you have forgotten it, contact lastpass-admins@digital.justice.gov.uk

Cryptography

Cryptographic controls

Automated certificate renewal

Where technically suitable, all new Ministry of Justice (MoJ) domains **must** use automated certificate techniques and services, such as [AWS Certificate Manager](#) (most preferred) or [LetsEncrypt](#) (uses [ACME](#))

Over time, existing MoJ 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 MoJ 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 MoJ 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 MoJ employee e.g. 3rd party supplier), to certificates@digital.justice.gov.uk.

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 compatiability)

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 against 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 manage 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-manage 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 Ministry of Justice (MoJ) 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 utilise 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 [MoJ Password Standard](#) has a section on hashing as part of password storage.

HMG Cryptography Business Continuity Management Standard

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESC (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Introduction

Scope

This Business continuity plan is limited to all HMG cryptographic material procured by the Ministry of Justice (MoJ) Crypto Custodian for and on behalf of any part of the MoJ with the exception of BRENT encryption requirements.

Who needs to read this document

This document is for the MoJ 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 MoJ Crypto Custodian is stored.

Background

All HMG encryption is procured from CESC 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 MoJ 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, Eclipt and Bitlocker are procured and distributed to by suppliers through the MoJ 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 MoJ Crypto Custodian and distributed to suppliers as and when necessary and returned to the MoJ 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 MoJ Crypto Custodian holds any others. All supplier crypto deployment environments are not at the same site as the MoJ Crypto Custodian and this provides natural segregation of the editions.

Eclipt 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. Above the safe is a fire suppressant sprinkler system.

Access to the safe is strictly limited to the MoJ 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 MoJ Custodian works is open plan in an accredited IL3 environment. The DSO has further accredited the immediate area surrounding the MoJ 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 MoJ:

- 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@cesg.gsi.gov.uk
and a copy to the Operational Security Team: OperationalSecurityTeam@justice.gov.uk
- 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

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Introduction

Scope

Within the Ministry of Justice (MoJ), 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 MoJ Crypto Custodian.

Out of Scope

Any information or component, which operates at SECRET or TOP SECRET (e.g. Private Keys with a classification above OFFICIAL-SENSITIVE) 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	<p>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.</p> <p>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.</p>
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.
- Departmental Security Officer (DSO) – 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 MoJ 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 MoJ Crypto Custodian, then ComSO, then DSO then SIRO. Escalation to CINRAS and other external bodies shall only be performed by the ComSO, DSO 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 MoJ, 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 [MoJ 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 DSO 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 MoJ 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 MoJ Crypto Custodian reserves the right to audit equipment and processes used in the delivery of PKI Services. The MoJ Crypto Custodian requires that all cryptographic components are managed and processed in accordance with HMG Standard IAS4.
2. Any remedial action required by the MoJ Crypto Custodian, to meet the requirements of HMG IAS4, must be agreed and implemented within reasonable timescales set by the MoJ 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 MoJ 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 OFFICIAL and OFFICIAL-SENSITIVE material, recognised assurances are stated below:
 - 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 MoJ 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 MoJ 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 be 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 MoJ 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, see [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 OFFICIAL and OFFICIAL-SENSITIVE material, assurance preferences are stated below:
 - 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 be 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 be 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, DSO.

Physical Security Policy

1. The PKI Services shall be located in an HMG Government building or Supplier building with appropriate physical controls for OFFICIAL-SENSITIVE information, as assessed by the Authority's DSO 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 DSO, and their delegated representatives, shall know the combination. The ComSO and DSO 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 DSO, 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 MoJ and made available to the MoJ.
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 DSO.

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 <ul style="list-style-type: none"> • 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

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

About this document

This document is the Ministry of Justice (MoJ) 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 below:

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 MoJ 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 MoJ IT system and/or where HMG cryptographic material is obtained through the MoJ.

Purpose

MoJ 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 (see 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 MoJ 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 e-mail methods are GSi, xGSi and CJSM accounts. All queries towards CESG must be forwarded to the MoJ 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 MoJ 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 MoJ Crypto Custodian in order for the form to be sent to CESG for processing.

If any of the conditions above have not been met the form cannot be processed and this may cause delays.

Further processing is required by the MoJ Crypto Custodian and upon dispatch to CESG the MoJ 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 MoJ Crypto Custodian.

The MoJ Crypto Custodian will forward the approved form to CESG for processing and any notifications from CESG will be advised by the MoJ Crypto Custodian to the applicant.

Authority to Operate Certificate

The MoJ 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 MoJ 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 through the MoJ 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 MoJ Crypto Custodian.

Any subject who handles Key Variables for the MoJ must be SC cleared and CRYPTO or ACCSEC authorised initially by the MoJ 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, they 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 MoJ Crypto Custodian or Authority.

Delivery of Key Variables

When Key Variables arrives and has been checked and recorded by the MoJ 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 MoJ 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 MoJ Crypto Custodian.

POL.CRYPTO.008

The applicant **must agree** with the MoJ 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 MoJ HQ and issued out for a short period of time in order to encrypt the system and then returned to MoJ HQ for storage.

Key Variables distribution as follows (in order of preference);

1. Collected from and returned to MoJ 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 IS4 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 MoJ Crypto Custodian for destruction.

Business continuity**POL.CRYPTO.011**

The MoJ 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 MoJ 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

Secure areas

Physical Security Policy**Audience**

This policy compliments the Ministry of Justice (MoJ) overall security policy.

Physical security is the practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (tangible, real-world) environment.

This Physical Security Policy 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, MoJ-occupied premises.

Executive Agencies and Arm's Length Bodies (ALBs) are expected to comply with this corporate framework, but might establish their own arrangements tailored to operational needs, and should therefore supplement this policy with local policy or guidance for any business-specific risk.

Objective

This content provides employees, contractors, partners and other interested parties with a clear policy direction. It requires them to ensure that all necessary physical protective security measures are in place to prevent attack, unauthorised access, damage, or interference (malicious or otherwise) to MoJ assets, and most importantly to prevent physical harm to our people and the public.

Scope and Definition

Physical Security refers to measures that are designed to protect physical locations and the assets, information, and personnel contained within.

This policy sets out the approach to be adopted to manage, develop, improve and assure Physical Security across the MoJ.

It is essential that MoJ business is conducted in an environment where potential threats - including those from both natural and human-made hazards, terrorism, crime, and insider threats - to MoJ assets, information, and personnel have been identified, risk assessed and appropriately mitigated to prevent interference, loss, or compromise (malicious or otherwise). This includes ensuring physical perimeters are protected, and entry controls are in place to provide proportionate protection against natural disasters and terrorist attacks.

Context

This policy sets out a framework to follow a “layered” approach to physical security. It provides suitably secure environments from which the MoJ can operate, to achieve its strategic aims and objectives by implementing security measures in layers, to appropriately protect personnel and assets, including material of differing levels of sensitivity.

This policy provides a high-level organisational objective for the MoJ with regards to Physical Security, supported by **MANDATORY** Physical Security Standards which **MUST** be followed to ensure compliance, as they represent the minimum measures required to protect the security of assets, information and people.

Responsibilities

All employees, contractors, partners, service providers and employees of other organisations who are on MoJ premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues and the protection of Departmental Assets.

The most senior grade based at each site, or in “Moderate Risk” and larger sites the Senior Responsible Officer (SRO), has responsibility for ensuring physical security risk assessments are conducted annually. They **MUST** ensure the action plans created to address identified risks and instigate business continuity activities are up-to-date, clearly communicated, regularly rehearsed, implemented effectively, and readily available, in accordance with their significance, importance, or classification.

Managing the physical security controls of sites occupied by MoJ employees is the responsibility of a contracted provider. The physical security controls include, for example:

- Perimeter control.
- Guarding.
- Site access.

The controls are measured in the form of Physical Security Reviews, as undertaken by the Group Security and Governance Team.

It is the responsibility of those procuring supplier contracts for such physical security measures to ensure that the most up-to-date technical and industry standards are met, and that the technology and processes in place are regularly reviewed to ensure that the security controls remain effective and fit for purpose. This includes technical and industry standards for Closed Circuit Television, Access Controls, Intruder Detection Systems, and any other relevant alarm systems which are managed by a contracted supplier.

Policy statements

Physical Security controls **MUST** be implemented that are proportionate to the risk appetite of the MoJ, and in adherence with the Information Security Policy and Acceptable Use Policy and other appropriate personnel and information security standards, including successful completion of the [Baseline Personnel Security Standard](#).

All employees must ensure they remain observant, report any suspicious behaviour, and highlight non-compliance. This vigilance will help deter, delay, prevent, or detect unauthorised access to, or attack on, a location, and mitigate the impact should they occur.

Each MoJ occupied premises presents unique physical security challenges. The measures introduced to protect each site **MUST** take into account the risk categorisation and the physical composition of that site. Effective approaches to Physical Security **MUST** follow the **MANDATORY** Physical Security Standards.

The most senior grade manager, or SRO in “Moderate Risk” and larger locations, **MUST** ensure that their site adheres to the Response Level Security Measures Policy, and ensure physical security risk assessment activity is conducted annually, and that the action plans created to address identified risks are implemented.

Compliance

The level of risk and potential impact to MoJ information, assets and people determines the controls to be applied, and the degree of assurance required. The MoJ **MUST** ensure 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 change in the Government Response Level.

The implementation of all security measures **MUST** 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 Centre for the Protection of National Infrastructure, and [Government Functional Standard - GovS 007: Security](#).

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, as warranted.

Physical security advice

Physical security advice can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Equipment

Clear Screen and Desk

Clear Screen

Users shall comply with the following:

- Digital Services equipment shall not be left logged on when unattended. Users shall ensure that password-protected screensavers are activated when any equipment is left unattended.
- Computer screens shall be angled away from the view of unauthorised persons.
- Computer security locks shall be set to activate when there is no activity for a short pre-determined period of time (set to 5 minutes by default). This can be manually activated when required.
- Computer security locks shall require passwords to be re-entered to reactivate the computer.
- Desktops and laptops should be shutdown if you expect to be away from them for more than half an hour.
- Users shall log off or lock their computers when they leave the room.

Clear Desk

Users shall comply with the following:

- Where possible, paper and computer media shall 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 etc. are not available, doors must be locked if rooms are left unattended. At the end of each session all OFFICIAL and OFFICIAL-SENSITIVE information shall be removed from the work place and stored in a locked area.
- When handling OFFICIAL documents security shall follow the requirements laid down in the Government Classification Scheme (GCS).
- OFFICIAL or OFFICIAL-SENSITIVE information, when printed, should be cleared from printers immediately.

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.

Laptops

Related information

[Lost devices or other IT security incidents](#) on page 317

Storing data on laptops

The guidance applies to all Ministry of Justice (MoJ) staff.

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 MoJ shared drive.
3. Your MoJ-provided 'home' drive.

Do this as soon as you can next connect to the MoJ network.

Where should I save data 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 MoJ 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 MoJ shared drive.
3. Your MoJ-provided 'home' drive.

There is a better chance of recovering lost data if you have saved it to the MoJ network, as data stored on the MoJ network is backed up daily.

What is 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 MoJ, 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 [IT Service Desk](#). 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 IT Service Desk. Once your identity is confirmed, your password will be reset and you will quickly regain access to your laptop.

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Locking and shutdown

General

The Ministry of Justice (MoJ) has made a commitment towards sustainable IT. The intentions are:

- To reduce overall power consumption for the MoJ by switching off machines and saving energy.
- To reduce the MoJ's overall carbon footprint.

How do I shutdown my 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.

What are 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.

What if there are any 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 [IT Service Desk](#) 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 MoJ 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 see 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 Background

All MoJ 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.

Incident

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 MoJ premises is not sufficient to guarantee the equipment's security. Laptop losses do sometimes occur within MoJ 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.

What you need to do

- 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](#).

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Policies for MacBook Users

Any User of an Ministry of Justice (MoJ)-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 MoJ 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 MoJ 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 MoJ equipment at all times.

If you don't think you should do something, you probably shouldn't. If in doubt, [always seek advice](#).

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

System Lockdown and Hardening Standard

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.

- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI ([Centre for the Protection of the National Infrastructure](#)), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Overview

This standard is designed to help protect Ministry of Justice (MoJ) IT systems by providing basis configuration details for how IT systems should be hardened to defend against malicious attack.

[HMG Security Policy Framework](#) mandatory requirement (MR) 9 concerns technical security controls. To comply with MR 7, the MoJ needs to ensure that it has:

Lockdown policy to restrict unnecessary services;

The lockdown policy itself is covered in the IT Security – Technical Controls Policy whilst this document sets out the MoJ standard for its application.

Scope

This standard provides some high level guidance on IT system hardening with which applied to all MoJ IT systems.

Note: This standard is a generic standard designed to provide high level direction. This standard does not replace the Government Assurance Pack (GAP) which must be considered for MS Windows based systems. The hardening of an IT system will be considered during the Accreditation process where the exact specification for the system will be considered and agreed. For further details on the Accreditation process see.

This standard must be read in conjunction with CESG GPG No.35 and the MoJ Security Architecture Framework.

Demonstration of Compliance

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

Generic hardening standard

Table 1 below provides a generic set of hardening procedures designed to guide IT system development and supplement the [IT Security – Technical Controls Policy](#).

Those configuring MoJ IT systems must consider additional sources of reference such as the Government Assurance Pack (GAP) for MS Windows based systems; Microsoft TechNet and NIST to ensure that specific systems (e.g. SQL server or a UNIX based server) are built to a secure standard. A selection of external reference sources can be found below.

Where this standard provides a generic set of hardening procedures, The MoJ Security Architecture Framework provides a set of vendor and system specific hardening guides which have been approved for use in MoJ IT systems.

The secure configuration of an IT system will be examined during the Accreditation process for further details). This may include an IT Health Check (ITHC) and a review of the system's build configuration.

Table 1 is split into 5 sections:

- 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

Name	Description
BIOS Lockdown	Access to the BIOS must be restricted to system administrators only.
Removal of unnecessary applications and services	All applications and system services which are not required must be uninstalled or disabled.
Auto-run of data on remote media devices	Auto-run must be disabled.
Screen lockout	Desktops and servers must be configured to lock after 5 minutes of inactivity. Unlock must be by password only.
Time and Date	The Time and Date setting must be configured to central synchronisation servers which synchronises with the GSi time server.
System Preferences	<p>Non-system administrative Users must not have access to change:</p> <ul style="list-style-type: none"> • The desktop background or screensaver setting; • The date or time; • Network settings or internet browser settings; • System security settings or group policy settings. <p>Non-system administrative Users must not have access to the following system settings / utilities:</p> <ul style="list-style-type: none"> • The system registry; • Access to operating system directories and files; • Access to CMD / Command Line Prompt and local system utilities such as disk defragmenter and disk cleanup.

External Devices

Name	Description
Bluetooth	Bluetooth must be disabled by default. If required due to business need, Bluetooth devices must be set to not be 'discoverable'.
Webcam	The webcam lens must be obstructed when not in use.
Infrared receiver	The IR receiver must be disabled, ideally at the hardware level (by physically disconnecting the component).

Name	Description
Sound input (microphone)	Sound input from a microphone must be kept at zero level when not in use.
Media drives and external data ports (e.g. USB, FireWire, CD/DVD drive, ...)	All media drives and external data ports must be disabled. Where there is a business justification to allow access, that access must be audited and restricted to an individual User (for example using a technical control such as Lumension).

Account Log-on

Name	Description
Passwords	All passwords must conform to the password guidance .
Guest and 'null' accounts	Guest and 'null' accounts (accounts with a blank username and password) must be disabled and removed where possible.
Fast User Switching	Fast User Switching must be disabled.
Login failure logging	Failed logins must be logged after the 1st failed attempt.
Automatic log in	Any automatic log in feature must be disabled. This does not include Single Sign On functionality where a User has already authenticated themselves to the system.
User list	The option to display a set of usernames list or the previous logged in User's username at logon must be disabled.
Logon Banner	The standard MoJ login banner must be displayed at login, both locally and remotely, see Appendix A .

Services, security and networking applications

Name	Description
Firewalls	An Application Firewall should be installed which: <ul style="list-style-type: none"> • Must be configured to 'allow only essential services'; • Must log Firewall activity; • Must operate in 'stealth mode' (undiscoverable).
Anonymous FTP	Anonymous FTP must be disabled. Where there is a business requirement for FTP, FTP(S) or SFTP must be used.
Simple Network Management Protocol (SNMP)	Where SNMP is required, v2.0 must be used.
Cisco Discovery Protocol (CDP)	CDP must be disabled.
Telnet based administration interface	Telnet access must be disabled.
SSH based administration interface	SSH access must 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) must be encrypted for the entire session using SSL version 3 or TLS version 1.0 or above.
Connection Timeouts	Idle connections must be dropped after a default period.
ICMP Redirects	ICMP redirects must be disabled.

Clear text authentication protocols	All plain-text authentication protocols must be disabled and their functionality replaced with encrypted alternatives.
-------------------------------------	--

Server specific

Name	Description
Internet access from web browsers	External Internet access from web browsers must be disabled.
Example, test and temporary installation files.	All example, test and temporary installation files must be deleted when no longer required.
File share access control	Server file shares must be subject to access control restrictions.

External reference sources

In addition to CESG GPG No.35, 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 MoJ login banner must be displayed at login. A copy of the banner is as follows:

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 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 Ministry of Justice (MoJ) **must** be added to Mail Check under at least the central MoJ 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 MoJ 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](#).

MoJ is permitted to use the service for free as a central government organisation, but suppliers to MoJ currently are not.

Get started

Contact the MoJ Cybersecurity team to be added into MoJ's subscription of the service.

Offshoring Guide

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).

- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Introduction

Document Purpose

This document is the Ministry of Justice (MoJ) IT Information Assurance (IA) Policy and Guidance for offshoring of MoJ 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 MoJ 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 MoJ.

The target audience for this document includes MoJ personnel with a requirement to make offshoring decisions; and MoJ suppliers who are considering, or currently engaged in, delivery of MoJ 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 MoJ. 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 MoJ will face when engaging an offshore supplier directly; it is also an issue that MoJ's suppliers will face, but may not be aware of, when subcontracting elements of delivery.

Risk to "UK PLC"

Many MoJ information systems handle HMG Protectively Marked and/or personal and sensitive personal data. These add a number of specific risks over-and-above 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 MoJ 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 MoJ capabilities from non-UK locations and/or by non-UK Nationals.
- Other provision of support to the MoJ from non-UK locations and/or by non-UK Nationals.

The scenarios which are to be treated as offshoring are set out in the bulleted list below. This is not necessarily an exhaustive list; in case of uncertainty please contact MoJ IT IA for advice: security@justice.gov.uk.

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 MoJ legal team, the MoJ Data Access and Compliance Unit (DACU), and the MoJ Data Protection EU and International Policy Teams must be consulted on legal issues. Contact privacy@justice.gov.uk 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 MoJ 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 MoJ 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 MoJ Accreditor or with MoJ IT IA, who will be able to provide tailored guidance to support individual decisions; it is intended more as general guidance on MoJ 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 MoJ. The MoJ 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 MoJ 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 MoJ 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 MoJ legal experts.

If a capability is delivered late, is substandard, fails completely or is compromised, then the MoJ 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 MoJ may find itself financially or legally liable for shortcomings in supplier subcontracts. Also, the MoJ rather than the supplier will almost certainly suffer the brunt of any bad publicity.

The core function of the MoJ 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 MoJ 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 MoJ 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 Departmental Security Officer (DSO), IT Security Officer (ITSO), Information Asset Owners (IAOs), supported by the Lead Accreditor.

REQUIREMENT 2: The MoJ 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 MoJ Accreditor, MoJ 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 MoJ 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 MoJ Accreditor. [HMG security policy](#) requires that the SIRO must personally 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 MoJ Accreditor, MoJ 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 MoJ Accreditor and MoJ 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 MoJ as the owner of the threat and the risk.

REQUIREMENT 3: All MoJ 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 MoJ 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 [REQUIREMENT 5](#) below.

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 MoJ "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, see [this guidance](#).

- Effective application development may require knowledge of real configuration information to support pre-integration-testing activities, or of broader MoJ 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 MoJ 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 MoJ 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 MoJ that Protectively Marked or otherwise sensitive MoJ 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 MoJ ITSO can provide further details of these, on a need-to-know basis, in response to specific requests. It is the policy of the MoJ that activities involving Protectively Marked or otherwise sensitive MoJ 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 MoJ 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: MoJ 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-above-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 above baseline. Also, as discussed above, 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 above, 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 above, 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 MoJ 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 MoJ 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 MoJ. 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 MoJ.

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 MoJ. 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 MoJ. 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 MoJ 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 MoJ 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 MoJ 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 MoJ, 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 MoJ contracts must flow up to the MoJ. All MoJ information, including vestidual information, which is held on a supplier's physical assets, must be erased and/or disposed of to the satisfaction of MoJ 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 above issues with contractual flow-down of responsibilities and flow-up of ownership are best managed if the MoJ retains control of the subcontract chain. Ideally, wherever practicable, MoJ supplier contracts should only allow further subcontracts to be let with the explicit permission of the MoJ. 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 MoJ 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 MoJ 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 MoJ applications must not be offshored. For other elements of application code which process, store and transmit sensitive MoJ information assets, an onshore security code review must be conducted. This should be to a level that is agreed by MoJ 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 MoJ must retain executive control over the testing process, maintaining visibility of all test results and progress on remedial activities. This includes control by MoJ IT IA over security elements of testing. The MoJ 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 MoJ, 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 MoJ 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 MoJ. If the supplier is not making an acceptable profit on a contract, then relationships between the supplier and the MoJ 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 below expectations 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 MoJ 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 over-and-above 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 MoJ 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 below.

REQUIREMENT 1 and REQUIREMENT 2

Project Scoping & Supplier Selection

MoJ Project Team:

- Ensure that the MoJ SIRO, MoJ Accreditor, MoJ IT IA and MoJ 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 MoJ Legal functions, DACU, and the MoJ Accreditor and MoJ IT IA. Ensure that these parties are key reviewers for all tender requirements.
- On the advice of the Accreditor, DACU, MoJ IT IA, and MoJ 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 MoJ IT IA effort requirement to address offshore elements of the proposal, as per [Requirement 11](#) below.
- Reject any bids that do not meet IA, DACU or Legal requirements for offshoring.

MoJ 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 MoJ Project Team on the suitability of offshoring proposals.

Note: MoJ IA includes both MoJ IT IA and the MoJ Central IA team. Both IA functions should be kept informed and engaged about offshoring proposals.

Contract Award

MoJ 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 MoJ Accreditor and MoJ 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 MoJ IT IA to advise and liaise with the SIRO.

MoJ Accreditor/IA:

- Provide review support and remedial input to the MoJ Project Team.

Development

MoJ 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 MoJ IT IA to advise and liaise with the SIRO.

MoJ Accreditor/IA:

- Provide review support, remedial input and recommendations to the MoJ Project Team.

In-Service & Beyond

MoJ 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 MoJ IT IA to advise and liaise with the SIRO.

MoJ Accreditor/IA:

- Provide review support, remedial input and recommendations to the MoJ 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 MoJ and HMG guidance.
- Asset valuations for all hardware and software assets must be clearly justified in the proposal documentation, and submitted to the MoJ Accreditor for review.

MoJ 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 MoJ IT IA are engaged on an on-going basis.
- Reject any proposals that do not meet with Requirement 3.

MoJ 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

MoJ 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 MoJ standard format, or in an equivalent format which contains (as a minimum) all of the information in the MoJ 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 MoJ. 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.)

MoJ Service Management:

- Maintain a MoJ 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 MoJ standard format, or in an equivalent format which contains (as a minimum) all of the information in the MoJ standard format.

MoJ Project Team:

- Maintain visibility of the hardware, software and information asset registers. Ensure that there is a regular joint (supplier/MoJ) 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.

MoJ 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 MoJ standard format, or in an equivalent format which contains (as a minimum) all of the information in the MoJ standard format.

MoJ Service Management:

- Maintain visibility of the hardware, software and information asset registers. Ensure that there is a regular joint (supplier/MoJ) 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.

MoJ 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 MoJ as part of the tender response.

MoJ 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 MoJ Legal advisors are aware of any potential requirements to offshore elements of the delivery.
- Work with the Accreditor and MoJ 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 MoJ 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 MoJ exposed to any additional legal liability.
- Reject any proposals that do not meet with Requirement 4 or Requirement 5.

MoJ Accreditor/IA

- Advise the project team on any potential offshoring problems and unacceptable offshoring proposals, and recommend mitigation options where necessary.

Contract Award

MoJ 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 MoJ before offshoring any elements of the delivery except where explicitly set out in the contract.
- Ensure that the Accreditor and MoJ IT IA are critical reviewers for all supplier contracts with an offshoring requirement.

MoJ Accreditor/IA:

- Advise the MoJ 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 MoJ.

MoJ Project Team:

- Deal with any emerging requirements on a case-by-case basis, through engagement with the Accreditor, the IA Team, DACU and MoJ 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 MoJ.

MoJ Service Management:

- Deal with any emerging requirements on a case-by-case basis, through engagement with the Accreditor, the IA Team, DACU and MoJ Legal advisors, and Information Asset Owners.

REQUIREMENT 6*Project Scoping & Supplier Selection*

Supplier:

- Conduct an initial IS1 Risk Assessment, In line with the MoJ-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.

MoJ 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 MoJ Accreditor, or MoJ 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 MoJ Accreditor and MoJ IT IA to be inadequate.
- Reject any proposals where the mitigations proposed in the Risk Management Plan are deemed by the MoJ Accreditor and MoJ IT IA to be inadequate, or the costs of implementing those mitigations are deemed by the MoJ Security Architecture Team to be unrealistic.

MoJ 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

MoJ 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 MoJ) for any contract change and as part of the acceptance criteria for each distinct phase of the development.

- Ensure that the Accreditor and MoJ 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.

MoJ 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.

MoJ Project Team:

- Ensure that suppliers meet their contractual obligations regarding risk assessment and PIA.

MoJ 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.

MoJ Service Management:

- Ensure that suppliers meet their contractual obligations regarding risk assessment and PIA.

MoJ 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.)

MoJ Project Team:

- Ensure that supplier proposals to deliver a capability are demonstrably compliant with offshoring security requirements.
- Reject any proposals that the MoJ Accreditor and MoJ IT IA deem to either not address security requirements comprehensively enough or not give sufficient weighting to these requirements.

MoJ Accreditor/IA:

- Engage with the MoJ Project Team and the supplier to support development and assessment of MoJ security requirements, including offshoring requirements, for the capability.

Contract Award

MoJ 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.

MoJ Accreditor/IA

- Support the MoJ Project Team in the development of contractual requirements around offshoring. Review contractual clauses relating to offshoring.

Development

Supplier:

- Inform the MoJ 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 MoJ Project Team, the MoJ Accreditor and MoJ IT IA. Work with MoJ to ensure that this can be managed in a secure way.

MoJ Project Team:

- Retain engagement with the MoJ Accreditor and MoJ IT IA for all aspects of the project development relating to offshoring.

MoJ Accreditor/IA:

- Provide support to the MoJ Project Team on offshoring, including direction for audit, remediation and emerging requirements as necessary.

In-Service & Beyond

Supplier:

- Inform the MoJ 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 MoJ Project Team, the MoJ Accreditor and MoJ IT IA. Work with MoJ to ensure that this can be managed in a secure way.

MoJ Service Management:

- Retain engagement with the MoJ Accreditor and MoJ IT IA for all aspects of ongoing development (e.g. third-line support) relating to offshoring.

MoJ Accreditor/IA:

- Provide support to the MoJ 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 MoJ 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.

MoJ Project Team:

- Ensure that MoJ 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.

MoJ Accreditor/IA:

- Engage with the MoJ Project Team and Supplier security resource to review supplier bids for compliance with HMG IA requirements and documentation (including offshoring requirements).

Contract Award

MoJ 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.

MoJ Procurement:

- Support the MoJ 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 [Requirement 7](#), above.

In-Service & Beyond

All:

- As per [Requirement 7](#), above.

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.

MoJ 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.

MoJ Accreditor/IA:

- Support assessment of functional and security testing proposals.

Contract Award

MoJ 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 MoJ before the start of testing. The MoJ must be contractually entitled to visibility of all test results and progress on remedial activities to the MoJ. 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 MoJ, with the ability to reject substandard delivery, require remediation and enforce contractual penalty clauses.

MoJ 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 MoJ Project Team to discuss progress against test requirements and milestones, exceptions and remedial planning.

MoJ Project Team:

- Ensure that the Accreditor and MoJ IT IA are involved in test forum(s) during development. Proactively track progress of remedial action against test defects.

MoJ Accreditor/IA:

- Support test review and remedial activities.

In-Service & Beyond

Supplier:

- Maintain a regular forum with the MoJ Project Team to discuss progress against test requirements and milestones, exceptions and remedial planning.

MoJ Service Management:

- Ensure that the Accreditor and MoJ IT IA are involved in test forum(s) during development. Proactively track progress of remedial action against test defects.

MoJ 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.

MoJ Project Team:

- In liaison with the MoJ Accreditor and MoJ 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.

MoJ 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.

MoJ 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.

MoJ 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 MoJ immediately if resource requirements change.

MoJ Project Team:

- Ensure that the MoJ Accreditor and MoJ 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.

MoJ Accreditor/IA

- Ensure that the MoJ 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 MoJ immediately if resource requirements change.

MoJ Service Management:

- Ensure that the MoJ Accreditor and MoJ 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 MoJ "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, see [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 MoJ 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.

MoJ IA includes both MoJ IT IA and the MoJ 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 Ministry of Justice (MoJ) is permitted to use the service for free as a central government organisation, but suppliers to MoJ currently are not.

Get started

Contact the MoJ Cybersecurity team (security@justice.gov.uk) to be added into MoJ'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 Ministry of Justice (MoJ) **must** be added to Web Check under at least the central MoJ 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 MoJ is permitted to use the service for free as a central government organisation, but suppliers to MoJ currently are not.

Get started

[Contact](#) the MoJ Cybersecurity team to be added into MoJ's subscription of the service.

Cyber Security Advice

Cyber Consultants & Risk Advisors

- Email: security@justice.gov.uk
- Slack: #security

Protection from malware

Malware Protection Guide - Overview

Introduction

This guide introduces the information which explains your responsibilities in helping the Ministry of Justice (MoJ) to prevent, detect and recover from malware. The MoJ 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.

Detailed information

For further guidance around implementing the three lines of defence to protect the MoJ from Malware, see the guides below.

- [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 MoJ'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 MoJ'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 MoJ 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 MoJ 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 MoJ 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 MoJ.

Contact details

- Contact the Cyber Assistance Team for advice on protecting against malware: CyberConsultancy@digital.justice.gov.uk.
- Contact the Technology Service Desk to report suspected malware: Telephone: 0800 917 5148.
- Contact the Operational Security Team (OST): OperationalSecurityTeam@justice.gov.uk>

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 Ministry of Justice (MoJ) 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 MoJ 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 MoJ 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 MoJ, will also find this information helpful.

Defensive Layer 1: Preventing malicious code from being delivered to devices

<p>Do</p> <ul style="list-style-type: none"> # Ensure that all public facing URLs that are assigned to services owned or managed on behalf of the MoJ 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 MoJ 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 MoJ, of the cloud service provider and any other supplier. For guidance on what responsibilities to consider, see 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 MoJ are scanned for malware. For Microsoft systems this is provided by Office 365 which quarantines any suspected malware. # 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. See 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. See 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 Operational Security Team (OST) 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 Cyber Assistance Team for help with this.
<p>Don't</p> <ul style="list-style-type: none"> # Allow externally obtained (from outside the MoJ) 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 MoJ from malware.

Don't

Connect any devices not procured and/or managed by the MoJ to trusted networks. Devices connected to MoJ trusted networks must be under MoJ management.

Contact details

- Contact the Cyber Assistance Team for advice on protecting against malware:
CyberConsultancy@digital.justice.gov.uk.
- Contact the Technology Service Desk to report suspected malware: Telephone: 0800 917 5148.
- Contact the Operational Security Team (OST): OperationalSecurityTeam@justice.gov.uk>

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 Ministry of Justice (MoJ) 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 MoJ 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 MoJ, 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 MoJ devices at some point. The next layer of protection prevents malicious code from taking effect. The tables below outlines ways in which you can help prevent malicious code from executing.

Do

Ensure that all systems and endpoints are scanned by anti-malware software. See [Note 1](#) for more details.

Ensure that if you are developing a new Microsoft Windows based system, that the MoJ's Windows Defender enterprise anti-malware software for Microsoft environments is configured to regularly scan it. Contact the OST 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 [Cyber Assistance Team](#) and the [Operational Security Team \(OST\)](#). See [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 [Cyber Assistance Team](#) for more information.

If you are developing or modifying networks, you should consider what protective monitoring is required. Contact the [OST](#) 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 MoJ OST's central monitoring capability.

When developing new systems and services, or updating or maintaining them, ensure that you refer to the security requirements detailed in the MoJ Software Development Lifecycle (SDLC) guidance. Contact the [Cyber Assistance 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 MoJ'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. See 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 [Cyber Assistance Team](#). Macros should be disabled by default.

Design systems to use multiple consecutive firewalls for systems processing OFFICIAL 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. See the [NCSC guidance](#) for further information.

Delay implementing security patches on infrastructure when possible. See 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 [Technology Service Desk](#) and the [Operational Security Team \(OST\)](#).

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

Contact details

- Contact the Cyber Assistance Team for advice on protecting against malware:
CyberConsultancy@digital.justice.gov.uk.

- Contact the Technology Service Desk to report suspected malware: Telephone: 0800 917 5148.
- Contact the Operational Security Team (OST): OperationalSecurityTeam@justice.gov.uk>

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 Ministry of Justice (MoJ) 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 MoJ 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 MoJ, 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 MoJ 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 MoJ 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. See 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 MoJ network. This includes firewalls and any device on the network boundary. See 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 MoJ 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. See the [Vulnerability Scanning and Patch Management Guide](#) for further information.

Delay if you suspect a malware incident has occurred. Make sure you contact the [Technology Service Desk](#) 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).

An IRAR is normally completed by Security Architects and Risk Assessors, in conversation with the system architects, designers and developers. The IRAR document must also be agreed with the Business Continuity Team. For more information regarding IRARs, and how to create and maintain them, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

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 tables below.

Do

Make sure user credentials are protected. Do this using strong passwords which are stored securely. See the [Password Manager Guide](#) for further information.

Ensure that effective access controls are designed and implemented in MoJ systems. Use [Multi-Factor Authentication \(MFA\)](#) wherever possible. See the [Access Control Guide](#) for further information.

Make sure you protect highly privileged accounts, by applying the principle of least privilege. See the [Access Control Guide](#) for further information.

Ensure that any system or application running on the MoJ's networks can collect and share system logs with the Operational Security Team's (OST) central monitoring function. This allows the MoJ 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.

In the exceptional circumstances where Bring your Own Device (BYOD) is permitted to access MoJ information, make sure your device runs anti-malware software and follows the requirements in [BYOD](#) guidance. Also ensure that users can only access MoJ 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 MoJ.
- # 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. See the Privileged User guidance for further details.

The NCSC provides helpful guidance on preventing [lateral movement](#) across networks.

Contact details

- Contact the Cyber Assistance Team for advice on protecting against malware:
CyberConsultancy@digital.justice.gov.uk.
- Contact the Technology Service Desk to report suspected malware: Telephone: 0800 917 5148.
- Contact the Operational Security Team (OST): OperationalSecurityTeam@justice.gov.uk>

Backup

System Backup Guidance

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI ([Centre for the Protection of the National Infrastructure](#)), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Backing up information

Backing up is an essential part of protecting Ministry of Justice (MoJ) Information and Communication Technology (IT) resources. This guide document provides an overview of backup concepts, and why backup is important for the MoJ.

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 than 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 MoJ 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 MoJ backup policy and standard both comply with access control assurance.

More information about how the MoJ 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 MoJ IT systems, including systems hosted by third party suppliers for the MoJ.

To decide if backup is required for a specific system, ask the question: "how long can the MoJ 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 MoJ 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 MoJ 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

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.

- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI ([Centre for the Protection of the National Infrastructure](#)), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

System recovery

Backing up is an essential part of protecting Ministry of Justice (MoJ) 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.

All systems MUST comply with the [HMG Security Policy Framework](#). To address this need, these statements from the MoJ [Technical Controls Policy](#) apply:

POL.TCP.108

All systems MUST have recovery procedures to maintain the integrity and availability of all Information Assets held. The recovery time will vary based on the system and data involved.

POL.TCP.109

A log MUST be kept of all back-ups taken for an IT system.

POL.TCP.110

Back-up data MUST be stored and handled in a manner appropriate to the sensitivity of the Information Assets stored.

POL.TCP.111

All IT systems MUST check all historic back-ups regularly to ensure that they can be relied upon. This includes the testing of any backup media used, such as tape or hard disks.

POL.TCP.112

All systems MUST have a recovery procedure which is tested regularly. Ideally, the testing will take place automatically.

POL.TCP.113

The retention period for historic back-ups MUST align to the retention period of the Information Assets held.

POL.TCP.114

All IT systems MUST conform to the [IT Security - System Backup Standard](#).

All IT systems **MUST** 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 **MUST** 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.

Use of the word **MUST** in this document complies with [RFC 2119](#).

System Backup Standard

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Backing up information

Backing up is one of the most important methods of system recovery. It protects Ministry of Justice (MoJ) 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 MoJ, see the [IT Security - System Backup Guide](#).

For details of what backups must do, see the [System backup requirements](#) section.

For details of how backups are implemented, see 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 MoJ 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 MoJ 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 be 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 MoJ 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 $365 \times 2 = 720$ 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 MoJ system is agreed between the business and the Departmental Library and Records Management Service: Records_Retention_@justice.gov.uk.

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 table above.
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 `SECRET`, then the entire backup medium must be protected to meet `SECRET` requirements.

The [protective marking level](#) for a backup is determined during the BIA process, and is described in the MoJ 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 `SECRET`.

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 generalistic 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 Ministry of Justice (MoJ).

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)
- Google Workspace (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 MoJ Google Workspace 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 Ministry of Justice (MoJ) 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)
- Google Workspace (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

Related information

[Security Log Collection](#) on page 189

Overview

The Ministry of Justice (MoJ) monitors the use of services, by recording (logging) event information.

This is permitted under data protection legislation, to help defend MoJ 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 MoJ processes this type of data for this purpose.

This is why the MoJ can log and monitor external interactions with its services, looking for evidence of cyber security attacks. It also allows the MoJ to act to protect those services. For example, the MoJ 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 MoJ is careful not to “over-retain” log information, or to share it with those who do not need to see it, without lawful justification. The MoJ must always act in a proportionate way with this data.

The MoJ Chief Information Security Office (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.

Log retention

By default, the MoJ retains raw logs in direct relation to security logging and monitoring purposes for at least 90 days, and for a maximum of 2 years.

The variation in between is as defined and required by legislation, regulation (such as the Law Enforcement Directive) or certification compliance (such as [PCI-DSS](#)). Retention for periods longer than 2 years requires MoJ CISO approval.

Logs for web-facing services should normally be kept for 90 days.

Logs for internal-only services should normally be kept for 13 months.

Aggregate data from logging systems, such as the number of particular types of events, the total numbers of visits to sites, and so on, can be retained indefinitely, so long as care has been taken to remove potentially unique or identifying information from the retained information set.

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 MoJ's security operations team (OperationalSecurityTeam@justice.gov.uk), 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 MoJ CISO.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Online identifiers in security logging and monitoring 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 for the Ministry of Justice (MoJ) during design, implementation, and operation of MoJ online services. Put simply, it is easiest for the MoJ 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 MoJ online services. This can include, for example:

- IP addresses.
- Cookies that the MoJ or authorised 3rd parties set on devices.
- Information placed into local storage on devices.
- Usernames or other IDs associated with MoJ services.
- Third-party authentication tokens.

Online identifiers could also include metadata captured about a device interacting with MoJ 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 MoJ 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 MoJ 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, see 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 MoJ services?

It is important to think carefully about:

- What metadata is captured during a user's interaction with MoJ services.
- How long information is retained.
- Who has access to the information.

MoJ 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 MoJ 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Protective Monitoring Guide

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: itpolicycontent@digital.justice.gov.uk

This policy applies to all staff and contractors who work for the Ministry of Justice (MoJ).

This document is the MoJ IT Security – Protective Monitoring Guide. It is designed to help protect MoJ 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 MoJ 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 MoJ guidance for its implementation.

Scope

This guide applies to all MoJ ICT systems including ICT systems hosted by third party suppliers on behalf of the MoJ.

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 MoJ 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 commensurate 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 Management 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 below 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).
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.

Protective Monitoring Control	Objective
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 (see [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.
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?

Control	Baseline Control	Notes
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; see [IT Security - Incident Management 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 above 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	<i>Insert Risk level</i>		
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		<i>Insert Risk level</i>	
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	<i>Insert Risk level</i>		
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	<i>Insert Risk level</i>		
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	<i>Insert Risk level</i>		
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	<i>Insert Risk level</i>		
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	<i>Insert Risk level</i>		
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	<i>Insert Risk level</i>		
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](#), a template table is provided below.

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](#); a template table is provided below:

Risk Level	Log Retention Period	Log Checks	Console Manning	Compliance Review Period	Report Production

Accounting items

The table below 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 in	Include on report	Alert on event	Method	Notes in Environment PM in policy	Accounting items and notes in GPG13)	Single and application requirement	Logging application	Tags	Predicates	Specific Events: Audit	Specific Events: Errors & Warnings	Specific Events: Protocol errors

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Security Log Collection

Security Log Collection

Ministry of Justice (MoJ) 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 172

MoJ Cyber Security Logging Platform

The MoJ 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 MoJ 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 MoJ. If you have any questions or comments, get in touch: security@justice.gov.uk.

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 MoJ Cyber Security Logging Platform*

- a: All log data must be sent to the MoJ 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) above is true, the MoJ Cyber Security team will advise in context what information must be sent from the in-place SIEM to the MoJ 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 Google Workspace 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 ultimately 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 logout
- 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 containerised 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)
- Google Workspace (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 ultimately 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 unsuccess 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 in 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

Ministry of Justice (MoJ) 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 \(MCSS\)](#).

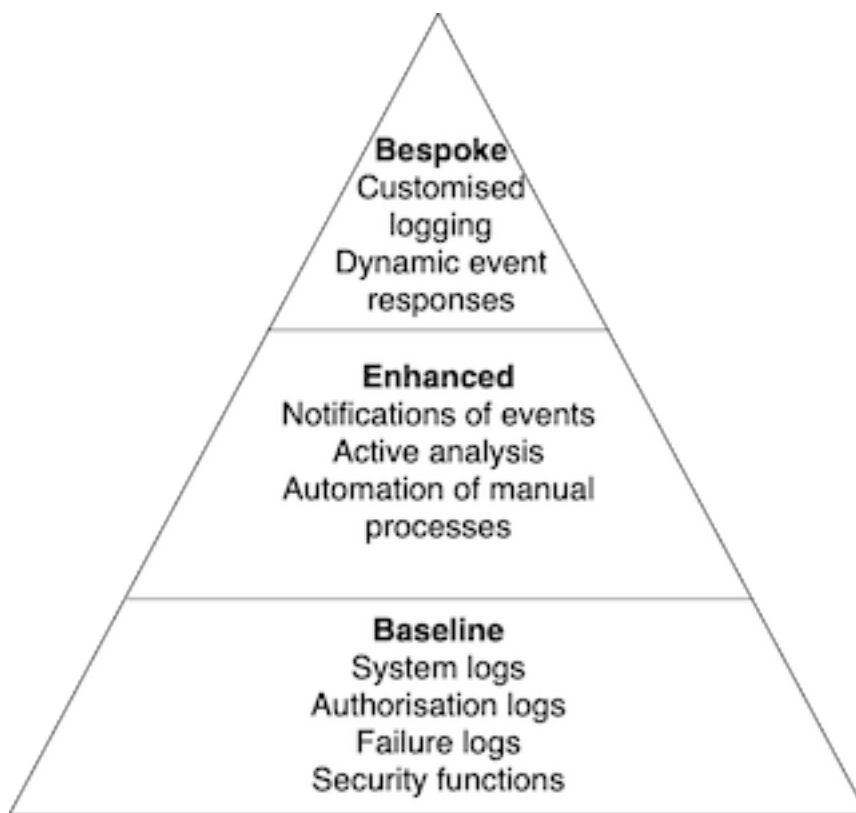
Three tiers have been developed to reflect the breadth and complexity of collecting and forwarding log data.

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 MoJ 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 MoJ, 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 MoJ 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Control of operational software

Guidance for using Open Internet Tools

This information applies to all staff and contractors who work for the Ministry of Justice (MoJ).

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 MoJ Intranet

Overview

Open Internet Tools (OITs) are applications or services from suppliers outside the MoJ. They often have the following characteristics:

- they are general purpose. This means they are not specific to the MoJ. 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 MoJ task, consider the following questions:

- is the task information subject to specific rules or requirements in your part of the MoJ?
- is the task information classified as anything other than OFFICIAL or OFFICIAL-SENSITIVE?
- does the task information include any data identifiable as being about someone?
- is this the first time anyone has used the tool for MoJ business?
- does the tool need access to your account or other data you can access? For example, does it ask to use your MoJ 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 MoJ, 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 MoJ-specific requirements

But as long you consider the threats or risks, and address them, OITs provide many benefits for you and the MoJ.

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: privacy@justice.gov.uk

Classification and security

An OIT can only store or process information [classified](#) at OFFICIAL level.

Think about the MoJ 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 MoJ 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 MoJ trusts you to work with OFFICIAL 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 MoJ IT Security, look on the MoJ Intranet [here](#).

Storage and data retention

Laws and regulations make the MoJ 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 MoJ 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 MoJ information in MoJ systems. If you use an OIT, make sure the key information is also stored in an appropriate MoJ system. Guidance on what you must keep is available [here](#). At regular and convenient intervals, transfer the information to an appropriate MoJ 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 MoJ 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 [MoJ 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 MoJ 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 MoJ cannot provide technical support for OITs.

Common OITs

There are already many OITs used across the MoJ. Permission to use an OIT might vary, depending on where you work in the MoJ. 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.

Requesting that an app be approved for use

If there is an application or service that is not currently approved, but which you would like to use, you can request a security review.

Begin the request by filling in [this form](#), as best you can. The more information you provide, the better. But don't worry if you have to leave some bits of the form blank.

When you submit the form, it is passed to the security team. The app is reviewed, to check things like how safe it is to use, and whether there are any Data Privacy implications. The security team will respond to you with an answer as quickly as possible.

Note: You should submit the request, and wait for a formal 'approval' response, *before* you install or use the app on MoJ equipment or information.

If you have any questions about the process, contact the security team: security@justice.gov.uk.

Getting help

For further help about aspects of using OITs within the MoJ, contact:

Subject	Contact
Classification and Security	MoJ 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 Ministry of Justice (MoJ) is primarily responsible for cyber security **must** redirect the `/.well-known/security.txt` location to the central `security.txt` file.

This redirection should be accessible from the public Internet whether or not the underlying applications/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` should still be accessible without authentication.

security.txt

`/.well-known/security.txt` must HTTP 301 (permanent redirect) to `https://raw.githubusercontent.com/ministryofjustice/security-guidance/main/contact/vulnerability-disclosure-security.txt`.

For example, `https://www.prisonvisits.service.gov.uk/.well-known/security.txt` must HTTP 301 to `https://raw.githubusercontent.com/ministryofjustice/security-guidance/main/contact/vulnerability-disclosure-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) should also implement `security.txt` as described above.

Non-production domains

Non-production domains resolvable from the public Internet (for example, a demo deployment of a MoJ digital service or prototype) should also implement `security.txt` as described above.

Vulnerability Disclosure Policy

The [Ministry of Justice \(MoJ\) Security Vulnerability Disclosure Policy](#) is published as part of the [MoJ 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 [MoJ Digital & Technology blog](#).

Feedback

If you wish to provide feedback or suggestions on the [MoJ 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 Ministry of Justice (MoJ) 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 MoJ.

Who is this for?

This guide is aimed at two audiences:

1. The in-house MoJ 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 MoJ 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.

Related guides

Further guidance on vulnerability scanning and patch management can be found in the following guides below:

- The [Vulnerability Scanning Guide](#) explains the scanning requirements for the MoJ systems.
- The [Patch Management Guide](#) explains the patching requirements for the MoJ.

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 MoJ.
- **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 MoJ 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 MoJ digital services. Many services make use of third-party software libraries and imported code.
- **Applications:** All applications hosted on MoJ 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 MoJ must be:

- Fully compliant with applicable Licenses and Terms of Use.
- Supported by applicable supplier packages (but see the note below).
- 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.

Cyber Security Advice

Cyber Consultants & Risk Advisors

- Email: security@justice.gov.uk
- Slack: #security

Vulnerability Scanning Guide Introduction

This guide explains the scanning requirements for Ministry of Justice (MoJ) systems.

This guide is a sub-page to the [Vulnerability Scanning and Patch Management Guide](#).

Scanning requirements

The MoJ should conduct the scanning activities outlined below 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).

An IRAR is normally completed by Security Architects and Risk Assessors, in conversation with the system architects, designers and developers. The IRAR document must also be agreed with the Business Continuity Team. For more information regarding IRARs, and how to create and maintain them, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

- 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 [Cyber Assistance 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 MoJ. Web Check continuously scans these websites and provides regular reports to the Operational Security Team (OST). If you are responsible for developing or running a website for the MoJ, you must:

- Ensure that it is added to the MoJ HQ Web Check Account. [Contact](#) the MoJ Cybersecurity team to be added to the MoJ 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 indicative schedule below 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 MoJ OST/SOC (OperationalSecurityTeam@justice.gov.uk) 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 [Operational Security Team](#).

These vulnerability alerts must contain as a minimum:

- An alert identifier.
- A cross-reference to known vulnerabilities.
- A risk rating (see the [Vulnerability risk ratings](#) section below).
- 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 MoJ. 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.

Rating (Severity)	Values on CVSS	Definition
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 see 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 MoJ and the vendor.

The schedules for vendors to conduct vulnerability scanning and issue vulnerability alerts to the MoJ are outlined below.

- 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 MoJ 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 MoJ 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 Cyber Assistance Team for advice on risk, scanning and patching: CyberConsultancy@digital.justice.gov.uk.
- Contact the Operational Security Team to report a vulnerability alert, or to add a URL to the MoJ Web Check system: OperationalSecurityTeam@justice.gov.uk.

Patch Management Guide

Introduction

This guide explains the patching requirements for Ministry of Justice (MoJ) 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 MoJ systems because of vulnerabilities.

Patching of MoJ systems and equipment

This guidance must be followed for all systems and services developed or procured by the MoJ. 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, described [below](#).

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 MoJ 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.

MoJ Digital services

For systems or services developed by the MoJ, 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](#) 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).

An IRAR is normally completed by Security Architects and Risk Assessors, in conversation with the system architects, designers and developers. The IRAR document must also be agreed with the Business Continuity Team. For more information regarding IRARs, and how to create and maintain them, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

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

Rating (Severity)	Infrastructure Devices; Server Applications; Digital Services	End User Client Devices	Web Check Reporting
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 MoJ.

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 MoJ 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 (contacted through email: CyberConsultancy@digital.justice.gov.uk) 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 MoJ in-house project teams

Where services and applications are developed by MoJ 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 [Cyber Assistance 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 [Cyber Assistance 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: CyberConsultancy@digital.justice.gov.uk) 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 Cyber Assistance Team for advice on risk, scanning and patching: CyberConsultancy@digital.justice.gov.uk.
- Contact the Operational Security Team to report a vulnerability alert, or to add a URL to the MoJ Web Check system: OperationalSecurityTeam@justice.gov.uk.

Communications security

Network security management

Code of connection standard

This standard is designed to help protect Ministry of Justice (MoJ) IT systems by providing a standard for the connection of a 3rd party IT system to a MoJ IT system.

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

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 MoJ on the security measures to be applied by that 3rd party prior to and during any electronic

connection with a MoJ 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 MoJ standard for its implementation.

Scope

This guide applies to all MoJ IT systems including IT systems hosted by third party suppliers on behalf of the MoJ 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 MoJ 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 MoJ that a connecting 3rd party understands the security controls and procedures required to connect to a MoJ 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 MoJ 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 sought from the IT Security Officer (ITSO) and system Accreditor.

A generic CoCo (based on the note above) is provided in Appendix A; it is split into two sections:

- basic requirement (see 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 (see 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 MoJ 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 MoJ 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 MoJ 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 (see 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 (see Appendix A) provides a baseline by which a 3rd party IT system's connection to a MoJ IT system will be assessed. The MoJ 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 MoJ 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 MoJ 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 MoJ 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 MoJ 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 MoJ 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 [MoJ IT Security Policy](#) and the IT Security Policy for the “ORGANISATION NAME FOR 3rd PARTY IT SYSTEM” are the primary polices which apply to this CoCo.

Any 3rd party IT system connecting to a MoJ IT system must have a current and relevant IT Security Policy which is accepted by the MoJ ITSO and system Accreditor. If any aspects of the data to be exchanged require special handling measures or are particularly sensitive, the MoJ 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 MoJ 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 MoJ 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 (see 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 MoJ 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 MoJ 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 MoJ 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 MoJ 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 MoJ IT SYSTEM” and its onward connections. All such connections must be identified in this document (see 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 above RESTRICTED should be exchanged over this connection.
CoCo-5	All points of connection to the “NAME OF MoJ 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, see A.2) and all have individual unique user accounts.

Condition	Description
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 MoJ IT SYSTEM” must be reported to MoJ 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 (see A.1.2.1).
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 MoJ IT SYSTEM”:

- The “NAME OF MoJ IT SYSTEM” is Accredited by the MoJ to process data up to and including RESTRICTED-IL3 for Confidentiality, Integrity and Availability;
- The security regime within the “NAME OF MoJ 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 MoJ 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 MoJ 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 MoJ 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 MoJ INFORMATION ASSET OWNER	Signature
MoJ Information Asset Owner	
	Date
NAME OF MoJ SYSTEM ACCREDITOR	Signature
MoJ System Accreditor	Date

A.2 Supporting compliance statement

This compliance statement provides a check list which will enable the MoJ 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 MoJ 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)			

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
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?			<i>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.</i>
A.6	Security Organisation			
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?			<i>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.</i>
A.6.1.3	Allocation of Information Security Responsibilities - Are “ORGANISATION NAME FOR 3rd PARTY” information security responsibilities allocated and documented?			<i>Have information security responsibilities been documented and communicated to all staff? If so, how?</i>

Ref.	Control	Compliance (Applicability) Y/N/ P/N/A	Process Owner/ Reference	Solution/Comments
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?			<i>Do confidentiality agreements state your requirements for security? Provide a copy of your agreement with this statement if possible.</i>
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?			<i>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.</i>
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?			<i>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</i>

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?			<i>Need to provide detail of any security requirements?</i>
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?			<i>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.</i>
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?			<i>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.</i>
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?			<i>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.</i>
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?			<i>How do management ensure that staff and contractors are aware and comply with their responsibilities for security?</i>
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?			<i>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?</i>
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?			<i>Details should be provided on the process for removing access rights on termination of employment.</i>
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?			<i>Describe the physical security barriers, e.g. walls, alarm systems, doors/gates, fencing, etc, where applicable.</i>
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?			<i>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?</i>

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?			<i>Describe the controls limiting access from public access, delivery and loading areas to the areas housing the IT services used to support this connection.</i>
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 MoJ IT SYSTEM”?			<i>Are operating procedures documented? A copy of the document or Table of Contents will suffice.</i>
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 MoJ IT SYSTEM”?			<i>*Describe the change management process.</i>

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?			<i>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?</i>
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?			<i>What measures are in place to control against malicious software/code? Describe the process for detection and removal of malware if detected.</i>
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.			<i>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.</i>
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 MoJ 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 above (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?			<i>How is the system documentation prevented from unauthorised access?</i>
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?			<i>Please provide any policies or an Information Sharing Agreement.</i>
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?			<i>Describe the registration and deregistration process. Are the user registration procedures documented?</i>
A.11.2.2	Privilege Management - Does the “NAME of 3rd PARTY IT SYSTEM” restrict the allocation and use of privileges?			<i>Who has (or will be given) privileged access to the MoJ IT System – roles will suffice? How will this access be restricted to just those named roles?</i>
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?			<i>Describe the process for allocating new passwords, the password policy and any control used to enforce it?</i>
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”?			<i>Describe the process for regularly reviewing access rights</i>
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"?			<i>What is the timeout process?</i>
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?			<i>Describe how users are limited to those services that they are only authorised to use. Is there a policy covering access to network services?</i>
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? See Control A.11.2.3 above.			<i>What security safeguards are in place to control access by remote users?</i>
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?			<i>Provide an overview of the secure log-on process.</i>

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?			<i>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.</i>
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?			<i>What procedures do you have in place to restrict access to system utility programs?</i>
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			<i>Check with the MoJ system Accreditor on whether any cryptographic controls are required in this connection.</i>

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"?			<i>Provide details on the controls put in place on the implementation of operational software.</i>
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 MoJ system Accreditor.			<i>Is there a documented Change Control procedure? Details should be provided.</i>
A.12.5.4	Information Leakage - Are there controls in place to reduce the likelihood of information leakage (compromise of MoJ)?			<i>What controls are in place to detect, deter or prevent information leakage?</i>
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 MoJ ITSO and system Accreditor as soon as possible?			<i>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 MoJ.</i>
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 MoJ.			<i>All IT Security incidents should be reported to MoJ Operational Security Team.</i>
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?			<i>Reference relevant documentation that details the procedures for adhering to privacy and protection of personal information. Provide documentation to support this if available.</i>
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?			<i>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?</i>
A.15.2.2	Technical Compliance Checking			<i>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?</i>
A.15.3	System Audit Consideration			

Defensive domain registrations

The Ministry of Justice (MoJ) 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 MoJ organisation **must** identify a core set of internet domains it considers critical to its internet identity. Each MoJ 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:dmarc-rua@dmarc.service.gov.uk;
```

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

MoJ 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 MoJ, 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.

Internet -v- PSN

The internet is 'ok'

The Ministry of Justice (MoJ) prefers the use of public commodity networks (such as the Internet) over the use of dedicated or private network links.

Networks are bearers

The MoJ 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 Ministry of Justice (MoJ) does **not** consider its IP address, DNS or architectural information to be `SENSITIVE` (a handling caveat within the `OFFICIAL` 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 MoJ 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 `OFFICIAL` the Ministry of Justice (MoJ) 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

Introduction

This guidance helps you use Bluetooth enabled devices and peripheral devices.

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 Ministry of Justice (MoJ) 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 MoJ 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.

Contact the Cyber Assistance Team by email: CyberConsultancy@digital.justice.gov.uk

Bluetooth devices and risks

Examples of Bluetooth devices, and whether they might be used for business purposes, are as follows:

Bluetooth device	Suitable for MoJ 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 MoJ-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

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 see 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.

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 accessed 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 see what Bluetooth devices you are using?
- Is the material you are working with OFFICIAL-SENSITIVE 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 undetectable if you can. Only make the device discoverable when you need to connect to a trusted device.

At regular intervals, check to see 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 see what Bluetooth devices you have, or are using, they might try and use one of their devices 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 OFFICIAL 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 OFFICIAL-SENSITIVE or higher material.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Criminal Justice Secure Mail

The Ministry of Justice (MoJ) operates the CJSJ 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 MoJ does **not** require the use of CJSJ 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 OFFICIAL data, including where the SENSITIVE handling caveat has been applied.

Data sovereignty

The Ministry of Justice (MoJ) Senior Security Adviser, Chief Information Security Officer (CISO), Chief Technical Officer (CTO) and Data Protection Officer (DPO) have issued this guidance for MoJ business units and third-party partners across the MoJ supported by Digital & Technology and/or within scope of the MoJ Data Protection Officer (DPO) to explain the MoJ's position on 'data sovereignty' (where the processing of data, including personal data, may take place).

Summary

At OFFICIAL 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 SENSITIVE (marked as OFFICIAL-SENSITIVE) 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 OFFICIAL.

The MoJ 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 questions above 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 MoJ 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 MoJ's position.

The MoJ has no plans to inshore data (i.e. limiting and / or returning data to the UK) for privacy or security reasons, nor is the MoJ asking its partners (for example, commercial suppliers) to do so.

Where to get help

In the first instance, contact the MoJ's Data Protection Officer - privacy@justice.gov.uk.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Email

For general assistance on Ministry of Justice (MoJ) security matters, email security@justice.gov.uk.

For Cyber Security assistance or consulting, email CyberConsultancy@digital.justice.gov.uk.

Suppliers to the MoJ should primarily contact your usual MoJ points of contact.

General Apps Guidance

Overview

When working from home, you still need to communicate with Ministry of Justice (MoJ) colleagues. You'll also need to work with people outside the MoJ. 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 MoJ.

Some ALBs, Agencies, or other large groups within the MoJ might have their own, specific guidance regarding how to use certain Video and Messaging apps for different purposes.

Access to tools

You can access tools that are provided through your MoJ provided devices by downloading from:

- The Software Centre application on your device (for Dom1 equipment).
- The Self Service application on your Mac (for Digital Service Desk (DSD) managed MacBook laptops).

Currently, access to the tools mentioned in this document is not available from Quantum devices.

For other MoJ provided devices, seek help from your Line Manager in the first instance.

Corporate, work and personal accounts

- A corporate account is for making official MoJ statements and providing official views. Only a small number of authorised people can use it.
- A work account is your normal MoJ 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.

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 MoJ. 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 MoJ. When working with a personal account, you are speaking and acting as an MoJ employee and a civil servant.

Always follow all [MoJ policies and guidelines regarding public information, including social media \(to access this information you'll need to be connected to the MoJ Intranet\)](#). In particular, follow the [Civil Service Code of Conduct](#).

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).

MoJ Policy and guidance

OFFICIAL and OFFICIAL-SENSITIVE Information

OFFICIAL 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.

OFFICIAL-SENSITIVE is not a classification. SENSITIVE is a handling caveat for a small subset of information marked OFFICIAL 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: privacy@justice.gov.uk
- Slack: #securityprivacyteam
- 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 OFFICIAL.

Think about the MoJ 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 MoJ trusts you to work with OFFICIAL

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 MoJ-provided work tool.

Remember that it is impossible to delete information after it's released in public.

For more information about MoJ IT Security, look on the MoJ Intranet [here](#).

Storage and data retention

Laws and regulations make the MoJ 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 MoJ 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 MoJ information in MoJ systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate MoJ system. Guidance on what you must keep is available on the Intranet [here](#). At regular and convenient intervals, transfer the information to an appropriate MoJ 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 MoJ system.

Many tools let you export your data. You can then store it on an appropriate MoJ 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 MoJ 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	MoJ use approved	Digital Service Desk controlled Mac - Self service, Web browser.	Internal/ External

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Microsoft Teams	Communication and collaboration tool: Video and/or voice	MoJ use approved	Dom1 Software centre, Digital Service Desk 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	MoJ use approved	Dom1 Software centre, Digital Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Slack	Text messaging, Voice/ Video calls, etc.	Avoid personal or sensitive data	Digital Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Slido	Q&A tool during presentations	Avoid personal or sensitive data	Web browser.	Internal
Twitter	Text Messaging, Video transmission	Approved for MoJ 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	External meetings

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 MoJ 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 MoJ devices. Installation might not be possible, for example on Quantum smartphones.

You might have both a personal and an MoJ 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 MoJ 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 above, please consult our [Guidance for using Open Internet Tools](#) and [speak to us for help](#).

Requesting that an app be approved for use

If there is an application or service that is not currently approved, but which you would like to use, you can request a security review.

Begin the request by filling in [this form](#), as best you can. The more information you provide, the better. But don't worry if you have to leave some bits of the form blank.

When you submit the form, it is passed to the security team. The app is reviewed, to check things like how safe it is to use, and whether there are any Data Privacy implications. The security team will respond to you with an answer as quickly as possible.

Note: You should submit the request, and wait for a formal 'approval' response, *before* you install or use the app on MoJ equipment or information.

If you have any questions about the process, contact the security team: security@justice.gov.uk.

Other information

Government policy and guidance

[GDS Social Media Playbook](#)

NCSC

[Video conferencing services: using them securely](#)

[Secure communications principles](#)

[Using third-party applications](#)

Web Browsing

The Ministry of Justice (MoJ) provides access to the Intranet and Internet for business use. The access helps you to do your job effectively and efficiently. MoJ 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 [Service Desk](#).

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 can I access?

The MoJ'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 MoJ 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 [Service Desk](#).

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 Service Desk 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, Operational Security 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 [Service Desk](#).

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 Service Desk via a local or area IT Manager.
- HMPPS Probation - Log an incident with your [Service Desk](#).
- All other teams, contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk

- Slack: #digitalservicedesk

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

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

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 Ministry of Justice (MoJ) or on its behalf. This guide aligns with [NIST 800-53](#) and the NCSC [Cyber Assessment Framework \(CAF\)](#). The guidance provides the MoJ with 3 phases or layers of defence. These controls must be implemented to ensure the MoJ's network infrastructure is secure.

Who is this guide for?

This guide has two audiences:

1. The in-house MoJ 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 MoJ 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 MoJ '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, see 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 Ministry of Justice (MoJ) 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, above 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 MoJ.

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 Ministry of Justice (MoJ) 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 Operational Security Team (OST).

Have the capability to respond to alerts generated by the monitoring system or by users and discuss options with OST.

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, see the [Data Security & 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 the above.

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 MoJ. Contact the Cyber Assistance Team (CAT) for advice at CyberConsultancy@digital.justice.gov.uk.

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 MoJ-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 maintaince 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 implementating 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 Ministry of Justice (MoJ) 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 commoly accepted best practices
- upgrading from SSLv3 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 principles above can generally be applied in most scenarios however interpretation and applicability in context can vary - the Ministry of Justice (MoJ) Cybersecurity 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 Ministry of Justice (MoJ). In particular, it applies to product owners, technical architects, security architects, and developers.

MoJ policy about making source code developed by the MoJ available complies with [UK Government guidance](#).

By default, MoJ developers **MUST** 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](#).

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

System Test Standard

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.

- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

About this document

This document is the Ministry of Justice (MoJ) System Test Standard. It is designed to help protect MoJ 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 MoJ 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 MoJ standard for system test implementation from a security perspective.

Scope

This standard is concerned with the security testing of all MoJ IT systems including IT systems hosted by third party suppliers on behalf of the MoJ.

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 MoJ will need to demonstrate compliance with in the MoJ IAMM return to Cabinet Office.

Testing approach

This standard outlines at a high level the security testing which must be applied to all MoJ 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 MoJ policy that system testing **MUST NOT** 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 (see [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 MoJ IT Security Officer (ITSO), system assurer, and Information Asset Owner (IAO). Further information can be obtained from the MoJ 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. See [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 section below ([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 are many different types of penetration test. For most MoJ 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 MoJ 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 MoJ [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 below 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.	See 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.	See 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 (see System Configuration Tests). Vulnerability scan (see Vulnerability Scanning). Compliance scan (see 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.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Test data

Using Live Data for Testing purposes

Summary

This document describes the use of live data during testing of Ministry of Justice (MoJ) systems. In general, using live data for testing purposes is considered bad practice. By default, the MoJ 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 MoJ Digital and Technology staff who are responsible for testing systems as part of technical design, development, system integration and operation.
2. Any other MoJ 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.

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 MoJ 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](#).

Data Privacy considerations

The use of live data for testing, where the data contains personal information, is almost certainly incompatible with the initial specified, explicit and legitimate purpose(s) known to data subjects. In effect, the data subject didn't know that their data would be used for test purposes.

There are sometimes valid reasons when you do need to use live data for test purposes but they are normally the exception rather than the norm and typically looked at on a case by case basis where appropriate risk management calls can be taken.

Looking at datasets being pulled out of databases are a prime example of where you may need to use live data to make sure that a software application is functioning correctly. For some things it is not always possible to use synthetic data.

Where a project is considering the use of live data for test purposes, it is essential to understand the data first, to be clear about what GDPR related factors apply.

You might need to look at fair processing notices and take these into account around the context of the tests being performed.

Note: It may actually be illegal to perform planned tests if fair processing notices do not allow using the data for test purposes.

Where the data involves personal information, help must be obtained from the MoJ Data Privacy team. At the very least, you must revisit or update an existing Data Protection Impact Assessment.

If there is no option apart from using live data, some of the things that should be considered will include the following:

- How will the data be extracted or obtained, and who will perform or oversee the extraction? What clearance do they have?
- What controls are in place to extract the data?
- Where is the data going to be extracted to? In other words, what media or mechanism will be used? For example, is the data extracted using electronic means such as SFTP, or is the data extracted to removable media, or does it remain 'in situ'?
- How is this data going to be protected at rest and during transit?
- What systems will the data be copied to, and in what environments?
- What systems will the data be processed by?
- How will access to this information be controlled both at rest and during transit for all systems that are involved in processing it?
- What access controls are in place end to end?
- Once testing is complete how will the data be removed/destroyed? What assurances do you have over this?

If live data is being used for test purposes within the Production environment, then backups are key and the testing to make sure that backups can be quickly restored is a must. There needs to be a good rollback plan in place. There also has to be an appetite for risk acceptance.

Ensuring test data is GDPR compliant

If you are intending to seek a special exception for using live data, or if you have anonymised the data but still want to have a satisfactory level of Data Privacy consideration, the follow points will help. Ensure that your test model has:

- Well-defined documentation of personal data information in all test environments.
- Effective data discovery to understand and unearth sensitive data information.
- Implemented a test data management process for the entire data life cycle that includes profiling, sub setting, masking, provisioning and archiving data in test environments.
- An irreversible 'on-the-fly' data masking process for production data within a repository.
- Permission and alerts in place for data exports and access outside the region, as this is restricted.
- Controls to prevent access to personal data from unauthorised access points, devices, or locations.

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 see 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 above](#). 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 Ministry of Justice (MoJ) 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 MoJ utilises 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 MoJ.

Accreditation

The MoJ no longer accredits new systems or suppliers (as defined by CESG Information Assurance Standard 1&2).

The MoJ maintains accreditations where committed to by existing contract.

Commodity digital technology

MoJ assesses commodity digital technology supply chain such as Software-as-a-Service (SaaS) tools such as Google Workspace, Microsoft Office 365, Trello and AtlassianCloud based on the [Cloud Security Principles](#), information risk assessment techniques and shared data within HMG.

Contractual promises

The Ministry of Justice (MoJ) embeds data governance and security-related clauses and schedules with contracts.

The MoJ is in the process of standardising and commoditising comprehensive clauses and schedules and will implement them over time.

Security Aspects Letters

Purpose

The Ministry of Justice (MoJ) will issue a Security Aspect Letter (SAL) where appropriate.

SALs are generally not required at OFFICIAL but MoJ 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 SENSITIVE handling caveat.

All information must be considered OFFICIAL 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 SENSITIVE 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 OFFICIAL 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 OFFICIAL.

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 OFFICIAL 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 above 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 declaration below 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 Ministry of Justice (MoJ) does **not** by default prohibit the use of supplier organisation corporate IT for the processing of MoJ data on the basis that the corporate IT environment is well designed, maintained, governed and defended in line with large scale commercial threat models.

Subject to the suitability described, the MoJ does **not** require suppliers to create or maintain dedicated or segregated IT solutions for the processing of MoJ data classified at OFFICIAL.

Technical security

Supplier corporate IT systems are expected to maintain appropriate levels of technical security defences to proportionally defend all types of data within whether the supplier's own corporate data through to MoJ data being processed.

This will range (but not be limited to) the use of modern Transport Layer Security or IPSec for in-transit encryption through to modern hashing and cryptography mechanisms for data stored at-rest, whether a data entry in a database or the entire storage drive in a laptop.

Supplier systems are expected to be proportionally resilient to malware, ensuring segregation between systems, users and data and employ adequate commodity measures (such as email attachment scanning/filtering).

Email security

Supplier corporate email systems processing MoJ data are expected to align to the [UK government secure email policy](#) which summarily requires widely accepted best practices.

Supplier corporate email systems are *not* required to technically integrate to the Public Services Network (PSN).

Data Governance

Data offshoring

Supplier's may process MoJ data (including Personal Data for which the MoJ is responsible) outside of the United Kingdom, subject to the maintenance of adequate information controls and governance.

MoJ data must not routinely be processed within an incompatible legal framework to the United Kingdom.

Working overseas

Supplier staff are **not** prohibited from working overseas while processing MoJ data on the basis that adequate information controls and governance are maintained.

When working overseas, this may include limiting access to information while the user travels or using secondary temporary accounts to avoid primary account compromise.

Data backups

Supplier corporate IT systems may backup data for extended retention times (for example, keeping archived or deleted emails for an additional few months). Backup systems may also exist in such a way that individual backup items cannot be individually deleted, and are subject to a system-wide backup rotation/retention schedule.

Subject to appropriate data governance, the MoJ acknowledges these cases.

Local end-user device data

The MoJ acknowledges that corporate users typically 'download' files (from local email client caching to file downloads via a web browser) that can remain within 'Downloads' folders until explicitly deleted by the user.

MoJ expects suppliers to consider these types of data locations in data governance regimes, however it is appreciated that data destruction may be guidance based from the supplier organisation to supplier staff.

Supplier service delivery management

Baseline for Amazon Web Services accounts

The Ministry of Justice (MoJ) has a 'lowest common denominator' for security-related promises, capabilities and configurations of MoJ Amazon Web Services (AWS) accounts.

The baseline is not a holistic list of dos and don'ts, but a *minimum* line in the sand for what 'at least' **must** be done.

The base principle

All MoJ AWS accounts **must** utilise 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 MoJ Cyber 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.

Security incidents

The CyberSecurity 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: Operational Security Team
- Title: Mx
- Email Address: OperationalSecurityTeam@justice.gov.uk

Baseline

IAM Access Analyzer

Utilise [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

Leverage 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 MoJ AWS account. Alerts fire for at least HIGH and above (or some version of) GuardDuty matches.	GuardDuty is automatically re-enabled.

CloudTrail

Leverage 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 MoJ AWS account.	CloudTrail is automatically re-enabled.

Config

Leverage 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 CyberSecurity via CloudTrail.	Alerts fire when Config is not enabled in an MoJ 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 MoJ 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 utilisation.

For more information on MFA, see the [Multi-Factor Authentication guidance](#).

Encryption

Leverage 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 MoJ Cyber 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 MoJ Cyber Security. After 7 days, the S3 object permissions are forcefully and automatically changed to remove 'world' access.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
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 MoJ Cyber 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 leverage 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 MoJ AWS account.	Security Hub is automatically re-enabled.

Implementation

Various [AWS account baseline templates](#) have been developed and published for use.

Information security incident management

Management of information security incidents and lost devices

Forensic Principles

Overview

The [Forensic Readiness Policy](#) states the Ministry of Justice (MoJ) requirements on the need for IT forensics. Each MoJ IT system or IT domain **MUST** have, or be explicitly covered by, a Forensic Readiness Plan. The policy also outlines four principles which must be followed. For reference, these are:

- Preservation of Evidence - the forensic investigation process **SHALL** preserve the integrity of original evidence by providing sufficient security, legal advice and procedural measures to ensure that evidential requirements are met. Any processes applied to copies of evidence must be repeatable and achieve the same results.
- Aptitude for task - any task in a forensic investigation **WILL** be conducted by a person assessed to be suitably trained and competent to carry out that task.
- Documented Methodology – all investigations **WILL** follow the documented methodology outlined in the forensic readiness plan, with an audit trail of all processes applied to evidence. A chain of evidence **WILL** be created and preserved demonstrating where evidence has been stored and whose care the evidence has been in from point of capture until presentation.

- Conformance - investigations **WILL** be conducted in a manner which respects MoJ policies and assumes full cooperation from all internal and external staff members.

People and resources

The MoJ Operational Security Team (OST) is responsible for the IT Security Incident Management Process and charged with responding to all IT security incidents. The team can be contacted by email: OperationalSecurityTeam@justice.gov.uk.

The MoJ intends to use a mix of internal and external resources to ensure that its forensic investigation capability can quickly and efficiently react to potentially incidents thereby minimising disruption to business.

Note: The [Forensic Readiness Policy](#) states that each forensic investigation must have a named Forensic Investigation Owner.

Incident management and forensic investigation process

The [IT Incident Management Policy](#) sets out the MoJ requirement for incident management where forensics investigation form part of the incident management process. As such, the forensic incident management process is an extension of the overall incident management process.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Forensic Readiness Guide About this document

This document is the Ministry of Justice (MoJ) IT Security Forensic Readiness Guide. It is designed to help protect MoJ IT systems by providing guidance on how to develop a Forensic Readiness Plan.

How to use this document

The purpose of this guide is to provide a consistent approach to forensic readiness across all MoJ IT systems and designed to supplement the guidance provided in [CESG GPG No.18](#).

Overview

Introduction

[HMG Security Policy Framework \(SPF\)](#) Mandatory Requirement (MR) 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.

To comply with this requirement, the MoJ **MUST**:

Have a forensic readiness policy that **WILL** maximise the ability to preserve and analyse data generated by an IT system that may be required for legal and management purposes

The policy on forensic readiness is covered in the [Forensic Readiness Policy](#) document. This document sets out the MoJ guidance on implementing that policy and developing a Forensic Readiness Plan.

Scope

This document is intended to provide guidance on the development of a Forensic Readiness Plan for MoJ IT Systems, including IT systems hosted by third party suppliers on behalf of the MoJ.

This guide is designed to supplement [CESG GPG No.18](#) and [CESG Implementation Guide No. 18](#), and is an extension of the [Incident Management Plan and Process Guide](#).

Readers of this guide who are developing a Forensic Readiness Plan **MUST** ensure it complies with [Forensic Readiness Policy](#) document and is written in accordance with [CESG GPG No.18](#).

Demonstration of Compliance

The [CESG Information Assurance Maturity Model \(IAMM\)](#) sets out the minimum maturity level Government departments should attain. Forensic readiness is captured as a basic requirement in Level 1 and the MoJ need to demonstrate compliance against this requirement.

Outline

This document is split into three sections:

- Definition of capability and requirement – this section provides guidance on the type of forensic capability which should be provided and the high level requirements associated with delivering a forensic capability which can support the implementation of a Forensic Readiness Plan;
- Developing a Forensic Readiness Plan – this section provides guidance on developing a Forensic Readiness Plan for an IT system or IT domain.
- Staff, education, training and awareness – this section provides guidance on what staff training and awareness should be made available in-order to support the implementation of the Forensic Readiness Plan.

A template Forensic Readiness Plan is available in Appendix D.

Definition of capability and requirement

Forensic principles

The [Forensic Readiness Policy](#) document states the MoJ requirements on the need for IT forensics; each MoJ IT system or IT domain **MUST** have or be explicitly covered by a Forensic Readiness Plan. The policy also outlines four principles which **MUST** be followed. For reference, these are:

- Preservation of Evidence - the forensic investigation process **SHALL** preserve the integrity of original evidence by providing sufficient security, legal advice and procedural measures to ensure that evidential requirements are met. Any processes applied to copies of evidence must be repeatable and achieve the same results.
- Aptitude for task - any task in a forensic investigation **WILL** be conducted by a person assessed to be suitably trained and competent to carry out that task.
- Documented Methodology – all investigations **WILL** follow the documented methodology outlined in the forensic readiness plan, with an audit trail of all processes applied to evidence. A chain of evidence **WILL** be created and preserved demonstrating where evidence has been stored and whose care the evidence has been in from point of capture until presentation.
- Conformance - investigations **WILL** be conducted in a manner which respects MoJ policies and assumes full cooperation from all internal and external staff members.

Resources and capability

Capability

[CESG GPG No.18](#) provides guidance on the level of forensic capability that should be developed commensurate to the Segmentation Model and Business Impact Levels (BILs) of the IT system or IT domain in question.

Most MoJ IT systems attract a BIL of 3 for Confidentiality, Integrity and Availability and are classified as ‘Deter’ in the segmentation model. As such, [CESG GPG No.18](#) considers that a Forensic Readiness Plan developed to capability level 2 is sufficient. It is anticipated that the majority of MoJ IT systems will fall into this capability level; however, this must be assessed on a system by system basis as part of the system Accreditation process. Further details on the process can be found in the [Accreditation Framework](#).

People and resources

The MoJ IT Operational Security Team (OST) is responsible for the IT Security Incident Management Process and charged with responding to all IT security incidents.

The MoJ intends to use a mix of internal and external resources to ensure that its forensic investigation capability can quickly and efficiently react to potentially incidents thereby minimising disruption to business.

Note: The [Forensic Readiness Policy](#) states that each forensic investigation must have named Forensic Investigation Owner.

Evidence collection and storage

The responsibility for the collection and management of evidence is likely to be split between the MoJ, IT service providers and an external forensics provider. At all stages of a forensic investigation process (see [here](#)), all evidential items collected from MoJ sites (or from MoJ IT equipment) must be managed and under the control of the Forensic Investigation Owner. Using [CESG GPG No.18](#), it is important to ensure that the procedures are laid out in the Forensic Readiness Plan.

Internal and external reporting and communication

The [Forensic Readiness Policy](#) outlines the need to ensure appropriate internal and external reporting. To ensure consistency of approach, as the Forensic Readiness Plan sits within IT Security Incident Management, the trigger points for internal and external reporting must align with the relevant Incident Management Plan; see [Incident Management Plan and Process Guide](#) for further details.

Note: Responsibility for escalation normally resides with the Information Asset Owner (IAO) and/or the Forensic Investigation Owner. Where responsibility for an investigation has been escalated to the Departmental Security Officer (DSO) or Senior Information Risk Owner (SIRO), further escalation responsibility will also reside with them.

The impact upon any ongoing operational activity must be considered before external reporting and escalation is invoked. The forensic investigation process (see [here](#)) must allow for the chain of evidence to be passed to any authorised outside agencies (e.g. Law Enforcement) where applicable.

Building an evidence-based case

A forensic investigation needs to go beyond identifying a wrongdoer or discovering how an incident occurred; it is required to provide a body of evidence that can stand up to detailed scrutiny, possibly by outside authorities. An investigation may involve many separate facts, both technical and testimonial, that are gathered together and presented as a logical argument.

A forensic case consists of:

1. The use of a technical forensic investigation methodology to build a consistent body of evidence that is applicable to its context e.g. presentation to a court of law or disciplinary hearing.
2. The ability to record testimonial evidence, including witness statements attesting to the facts around an incident and its investigation by a forensic expert.
3. The presentation of available facts in a logical, unbiased argument.

The forensic investigative capability of the selected external provider must follow a predefined forensic methodology to acquire evidence in a consistent manner, suitably transport and preserve it, and present it as legally admissible in any subsequent proceedings.

Developing a forensic readiness plan

Scenario based planning

It is important to consider the circumstances in which a Forensic Readiness Plan will be invoked. Scenario-based planning is all about examining the different circumstances and incident types which are likely to result in a forensic investigation, then building the forensic readiness plan around those scenarios.

Table 1 provides a list scenario class types which are detailed in [CESG Implementation Guide No. 18](#). It is anticipated that for the MoJ, the most pertinent classes are class 1, 2, and 3; record management systems may also need to consider class 5.

Table 5: Table 1 – Classification of forensic scenarios

Class	Scenario
Class 1 - Crime	Scenarios involving criminal offences and law enforcement.
Class 2 - Internal	Scenarios relating to internal (e.g. disciplinary or audit) investigations.
Class 3 - External	Scenarios relating to external attack (e.g. by a hacker).
Class 4 – Civil Dispute	Scenarios involving civil disputes (e.g. over a contract).

Class	Scenario
Class 5 – Regulatory Compliance	Scenarios where information is to be provided in compliance with a regulatory requirement (e.g. under the Freedom of Information Act).

Each scenario should be documented in full with a summary contained in the Forensic Readiness Plan (see Appendix D). Table 2 provides an outline for how each scenario should be documented. It is recommended that this is included as an appendix to the Forensic Readiness Plan.

Table 6: Table 2 – Layout for a forensic investigation scenario

Section	Description
Scenario	Scenario name and brief description.
Typical Synopsis	Provide an example(s) of the scenario type. This is not meant to be exhaustive and there can be many variations on a theme.
Typical Diagnostic Indicators	Produce a list of possible sources that may first raise suspicion that an incident of that scenario type has occurred. See Appendix A for possible incidents.
Typical Digital Evidence Sources	Generate a checklist of potential initial sources (in approximate order of significance) of evidence that would be useful to an investigation in that scenario type. See Appendix B for guidance on digital evidence sources.
Typical Workflow	Generate a workflow checklist of activities which should be followed. This does not need to be a precise list as each incident may have unique characteristics and take the investigation in unpredictable directions. See here for further details.
Typical Desired Outcomes	A checklist of the outcomes / outputs of conducting a forensic investigation.

Criteria for conducting a forensic investigation

The decision to conduct a forensic investigation is a risk management decision, set against a cost/benefit analysis and any obligations stemming from any legal or regulatory requirements.

Developing forensic scenarios (see [here](#)) plays an important role in understanding the inputs into the decision making process. Table 3 outlines the decision making criteria along with the considerations which should be applied.

Table 7: Table 3 – Criteria for conducting a forensic investigation

Criteria	Consideration
Risk Management	It is important to ascertain the risk and issues associated with any incident and consider whether the impact of conducting a forensic investigation will have a detrimental effect on MoJ IT systems or business processes.

Criteria	Consideration
Cost/Benefit Analysis	The costs associated with conducting a forensic investigation might outweigh the benefits of the desired outcomes. There may be a requirement to discuss those outcomes with the MoJ ITSO and/or external forensic provider to understand the options available.
Legal / Regulatory requirement	Where there is a legal or regulatory requirement to conduct a forensic investigation, this must be fed into the decision making process along with an analysis of what level of forensic investigation is required to satisfy that requirement.
MoJ Authorisation	The decision to conduct a forensic investigation resides with the IAO and/or ITSO.

Incident management and forensic investigation process

The [IT Incident Management Policy](#) sets out the MoJ requirement for incident management where forensics investigation form part of the incident management process. As such, the forensic incident management process is an extension of the overall incident management process.

[CESG Implementation Guide No. 18](#) provides a generic forensic investigation process flow. Table 4 lists the step-by-step forensic investigation activities which are expected to be included in the Forensic Readiness Plan (see Appendix D), along with the role/s responsible for completing each activity.

Table 8: Table 4 – Forensic investigation activities

Step	Activity	Role/s responsible
1	Decision to conduct a Forensic Investigation	MoJ OST / MoJ ITSO
2	Agree the scope of the forensic investigation	MoJ ITSO
3	Provide a Single Point of Contact (SPOC) for incident management and co-ordinate forensic activities	Forensic Investigation Owner
4	Establish a forensic investigation	Forensic Investigation Owner / MoJ IT System Manager / External Forensics provider
5	Collection of evidence	MoJ IT System Manager / External Forensics provider
6	Analysis of evidence	Forensic Investigation Owner / MoJ IT System Manager / External Forensics provider
7	Production of forensic reports	Forensic Investigation Owner / External Forensics provider
8	Approval of forensic reports	SIRO / IAO / MoJ ITSO
9	Long term storage of evidence if required	MoJ IT System Manager / MoJ ITSO
10	Provide specialist digital forensics legal advice to investigations	External Forensics provider

Step	Activity	Role/s responsible
11	External reporting and liaising	MoJ OST / MoJ ITSO
12	Act as Expert Witness for legal proceedings (if required)	External Forensics provider
13	Post incident remediation analysis including production of lessons learned	Forensic Investigation Owner / External Forensics provider
14	Approval of post incident remediation	SIRO / IAO / MoJ ITSO
15	Implement required changes to support investigation and post incident activities	MoJ IT System Manager / IAO

Note: The Forensic Readiness Plan and associated investigation process should align with the relevant business continuity plan and MoJ policy on records management.

Procedures

When the decision is made to conduct a forensic investigation or preserve evidence in a manner which does not preclude a forensic investigation, it is vital that a clear set of procedures are included within the Forensic Readiness Plan to ensure evidence is not lost or tampered with.

Appendix C contains a generic set of procedures which are designed to be enacted during the first stages of a forensic investigation (steps 1 to 4 in Table 4) to ensure information is stored in a forensically safe manner. Each Forensic Readiness Plan (see Appendix D) must contain a set of forensic procedures.

Performance monitoring

Each Forensic Readiness Plan must consider the Key Performance Indicators (KPIs) and Service Level Agreements (SLAs) required. This ensures that when required, the Forensic Readiness Plan can be executed in a timely and efficient manner.

To support continuous improvement, the Forensic Readiness Plan must be updated annually with the following information:

- Current and target forensic capability levels;
- Status of the plan and associated scenarios;
- Status of any exercise and feedback from those exercises;
- Status of staff or external provider competency levels (including register of formal certifications);
- Current and past investigation knowledgebase and active issues (to be managed by MoJ OST);
- Status of the current review cycle.

Staff, education, training and awareness

Good information usage and risk management practice demands appropriate training of all individuals coming into contact with MoJ IT systems; this must include relevant aspects of the Forensic Readiness Plan.

Ongoing general MoJ IT security awareness training must integrate forensic readiness awareness into the existing courses, and ensure at least annual refreshment for all staff on the current policy and procedures. This includes the communication of any required incident response procedures to ensure admissibility of evidence.

For the roles outlined [here](#), more in depth forensic readiness training may be required. This must be considered during the development of the Forensic Readiness Plan. It may involve utilising external training courses and material to train first responders and other key individuals involved in developing and delivering the Forensic Readiness Plan.

Appendix A. Guidance on risks and incidents

Business risks that require reduction or mitigation through the use of forensics come from a variety of sources and cover several different types of incident/crime.

Table 5 provides some examples of incidents which may require a forensic investigation:

Table 9: Table 5 – Incident categories and associated risks

Incident Category	Nature of Incident
Creation or planting of viruses or malware	The deliberate introduction of these files could pose a major threat to MoJ information security. Infiltration of systems in this way potentially causes issues such as downtime, unpredictable behaviour and/or data non-availability.
Damage or modifications to computer equipment or data	The deliberate or incidental damage of a computer system may disguise unauthorised activity previously carried out on that device. Examining modifications of equipment may reveal planted devices, such as key loggers or modems used to bypass normal security mechanisms.
Disciplinary issues through inappropriate use of MoJ IT systems	This could include: the storage of pornographic or other images or files; email abuse such as SPAM; connecting systems to unofficial networks; attempted unauthorised access to computer data or programs; or unapproved upload/download of information to the Internet. See Acceptable Use Policy for further details.
Email SPAM/Denial of Service Attacks	Internal connections may be used to attack other internal or external targets. An investigation may look for evidence of the tools used by hackers.
Financial crimes, identity theft, fraud, forgery, theft of funds, blackmail or extortion	The misuse of a computer to steal people's identity for financial or other gain may leave evidence in IT systems or on portable media. A forensic study of disks, equipment, logs and email records plus other devices (e.g. mobile phones) and non-digital evidence (e.g. printed documents, written notes) may provide investigators with evidence to prosecute individuals.
External	Many outside parties, from teenagers acting alone to hostile foreign governments, may attempt to compromise the security of MoJ IT systems.
Internal Authorised	Authorised users may abuse MoJ IT systems by conducting unauthorised or illegal actions. These could include storage of offensive material, stealing information for an outside agent, providing (or selling) information to someone external to the organisation, the unapproved upload/download of information to the Internet or internal illegal file-sharing.
Internal to External	Users may use MoJ IT facilities to facilitate crimes against external parties. Examples would include mass emailing, hosting illicit Peer-to-Peer (P2P) clients (for music propagation etc) or launching attacks against websites.
Internal Unauthorised	Staff members may attempt to circumvent controls to gain access to material they do not have authorisation to view. A cleaner attempting to access a restricted file system would be an example of this.

Incident Category	Nature of Incident
Target Systems	If a MoJ IT system has been compromised through a security incident it may be necessary to collect evidence from that system to understand the method and source of the attack.
Telecommunications Crime/Hacking	The use of a computer to attempt unauthorised access to computers or networks is common. A forensic investigation might gather evidence from multiple devices, including router and firewall logs to establish the source and perpetrator of the attack.
Theft of intellectual Property/Protected Data	The unauthorised copying or removal of programs or sensitive data may involve the use of removable disks or other storage, such as a media player. Copyright theft would be an example of such a crime. Forensics can be used to prove a particular piece of equipment was used in such an incident, even if the perpetrator has attempted to cover their tracks.

Appendix B. Guidance on sources and forms of digital evidence

Computers, networks, storage devices and their peripherals may be used in the commission of various incidents or crimes, or can themselves be the target of an attack. As a result, digital evidence may be collected from a variety of sources. Table 6 and Table 7 below provide a set of examples:

Hardware artefacts:

Table 10: Table 6 – Sources and forms of digital evidence - Hardware

Artefact	Relevant Aspects
Backup media (tapes, disks, etc.)	Actions that took place over a period of time, or in the past, might be recreated using backup media, or backup (archive) files stored on a device.
CD-ROM / DVD / memory sticks / floppy disks	Storage media are often used for stealing data or intellectual property. An understanding of storage techniques, and protective / concealing technologies such as encryption is required to reveal hidden data.
Digital cameras and video devices including CCTV	Increasingly, camera and video images are used as evidence. An investigation must handle this media appropriately to preserve evidence. Such systems need to have the same time source as IT for synchronisation purposes, as should Access Control systems. Ministry of Justice personnel are responsible for the upkeep of CCTV on MoJ sites.
Hard disks (internal and external)	Hard disks or removable media devices or phones may contain evidence in deleted or hidden files, folders or partitions not normally visible to users.
Media players / games consoles	These devices appear to be innocent entertainment devices, but may be used as mass storage or wireless transmission devices and include PC synchronisation capabilities. Recent generations of this type of technology have extremely large storage capacity in a physically small device.

Artefact	Relevant Aspects
Mobile Phones	Modern mobile phones contain contact information and call logs (inbound and outbound). They also have significant data storage capability, and the ability to synchronise data with a PC. They can also be used to wirelessly connect a PC to the Internet or simply connect directly to the Internet, often with the majority of functionality of a PC both online and off.
PC	This is the main unit which contains the hard disks and motherboard. Investigations may include: Copying volatile memory; Copying the BIOS; Examining hardware for unauthorised modification; Examining seals and asset tags.
Routers / Modems / Bridges / Firewalls	Configurable network devices often contain logs which can be used to attribute a machine to a course of action, and generally contain configuration information showing how the device was connected at a given time. It should be noted that a well known issue with device-specific logs such as these is that they do not record the system operating context within which they have been deployed and used. As this context changes dynamically and drifts away from any notional configuration over time, it is generally thought that examining such logs more than six months after an incident is of very little value.
USB / Firewire devices / Wireless cards, PCMCIA cards, and 'flash' memory cards	An array of devices can be connected to PCs through these ports and may need investigating. Interactions via this route can be subtle, and either innocuous or malicious. For example, some modern mobile phones charge themselves via the USB connection – and it can be difficult to distinguish this type of use from an inappropriate data upload/download. Furthermore, many USB connected devices automatically synchronise selected data with the PC, so a user may not be aware of the data transfer that has actually taken place. Memory sticks (or memory keys) are another class of USB device where care must be taken as their small physical size allows them to be used covertly with ease, and the latest generation of these devices includes the facility to automatically invoked data capture.

Software and other artefacts:

Table 11: Table 7 – Sources and forms of digital evidence – Software and other artefacts

Artefact	Relevant Aspects
Application software	Some applications, such as accounting packages, may hold records of fraud or employee records and activities.

Artefact	Relevant Aspects
Operating System (OS) components and the registry	The OS is the software which controls the operation of the PC or phone. Security is enforced by the operating system, so attempts to subvert a PC frequently, starting with an attack on the operating system files. The registry is specific to Windows-based PCs and is the central repository of system management information. Examination of the registry can reveal: What devices have been connected; What application software has been installed and uninstalled; Usage history for applications; The state (configuration) of operating system components.
Application and Middleware Log Files	Many applications and middleware (particularly the large enterprise varieties) produce their own log files for various activities. An investigation may involve the detailed study of this information, or of the servers holding this information. Investigators need to be aware of any attempt to subvert log files in support of malicious activity.
Email records	IT systems can hold records of recent email activity, and mail servers retain extensive logs and records[1]. Organisation policy may dictate an email retention period, such as seven years for everything. An investigation may involve the detailed study of this information, or of the servers holding this information.
System Log Files	IT systems produce log files for various activities. An investigation may involve the detailed study of this information, or of the servers holding this information. Investigators need to be aware of any attempt to subvert log files in support of malicious activity.

Note: Different evidence sources require specific handling and documentation. This will need to be managed by the Forensic Investigation Owner.

Appendix C. Forensic procedures

This section contains a set of forensic procedures which should be enacted in addition to contacting the relevant IAO/ Line Manager and the IT Security Manager when an incident occurs.

These procedures are designed to ensure as much evidence is preserved as possible, and to facilitate the transfer of equipment and material to a forensic investigator for further inspections.

As outlined [here](#), consideration must be given to the strength of case required to proceed; therefore, a preliminary business impact assessment should be made based on whether any of the following are present:

- Evidence of a reported crime.
- Evidence of internal fraud, theft or other loss.
- Estimate of possible damages (a threshold may induce an escalation trigger).
- Potential for embarrassment/reputation loss.
- Any immediate impact on customers, business partners or profitability.
- Recovery plans have been enacted or are required.
- The incident is reported under a compliance regime.

For computer equipment which is switched on, the following process must be applied:

1. Secure the area containing the equipment.

2. Move people away from the computer and power supplies.
3. If attached, disconnect any modem.
4. If the computer is attached to the network remove the network cable from the data point.
5. Do not touch the keyboard or mouse.
6. Do not take advice from the computer's user/owner.
7. Allow any printers to finish printing (further evidence may be printing).

If equipment is removed before the investigator arrives then the following steps must be performed:

1. Record what is on the screen and take photographs if possible.
2. Switch off the computer by pulling the power cable from the computer, not from the power socket.

Note: For laptops, remove the battery before pulling the power cable.

When removing the power supply always remove the end attached to the computer and not the socket. This will avoid data being written to the hard drive if an uninterruptable power supply is fitted. Then:

- a. If possible, label and photograph all the components in situ. If no camera is available draw a sketch plan;
- b. Label the ports and cables so that the computer can be reconstructed at a later date;
- c. Carefully remove the equipment and record serial numbers/asset tags;
- d. Ensure all items have been signed and completed exhibit labels attached;
- e. Search the immediate area for diaries, notebooks or pieces of paper that may contain passwords;
- f. Consider asking the user if there are any passwords, and if given, record them accurately;
- g. Make detailed notes of all actions in relation to the seizure of the computer equipment;
- h. Remove the computer equipment to a secure location.

For computer equipment which is switched off, the following process must be applied:

1. DO NOT switch the computer on.
2. Secure and take control of the area controlling the equipment.
3. Move people away from the computers and power supplies.
4. Confirm the computer is actually switched off – some screen savers can give the appearance that the computer is switched off. Check the hard drive and monitor lights to confirm this.
5. Be aware that some laptops may power up by opening the lid.
6. Remove the battery from laptops.
7. Unplug the power supply from the computer. A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of data.

Appendix D: Forensic Readiness Plan template

IT Security – Forensic Readiness Plan	
System Details	
IT System / IT Domain Name	[Enter the name of the IT system or domain.]
System Description and Scope	[This section should describe the name and purpose of the system, including the protective marking level of the information it holds. Diagrams may prove useful where there is a complex interaction between systems covered in this statement/standard. It is important to include notes of where a part of a system is excluded from the scope of this plan e.g. an application which is managed by another function.]

IT Security – Forensic Readiness Plan	
Responsibilities and Ownership	[Complete a statement detailing who has ownership and who will be responsible for the administration of this plan. Where a third-party or managed service provider is responsible for all or just a component of the plan, a clear reference should be made to contractual responsibilities. Points of contact regarding forensic readiness should also be noted.] [Note: Each role outlined here must be named in this section.]
Forensic scenarios	
[Name of Scenario 1]	[A summary of each scenario developed must be contained in this section, with full details provided as an appendix to the plan. See here for further details.]
Process and procedures	
Process	[This section must contain a step-by-step plan of activities to be followed during a forensic investigation. See here for further details.]
Procedures	[This section must contain details on the initial forensic procedures which should be followed once the decision to undertake a forensic investigation has been made. See here for further details]
Performance Monitoring	
KPIs / Performance measures	[Include details on the KPIs and SLAs associated with this plan. See here for further details]
Continuous improvement	[Include details on the continuous improvement measures associated with this plan. See here for further details]
Training and awareness	
Capability and staff training	[Include details of how staff training measure outlined here are met.]
Plan Approval	
IT System Manager	[Enter the name of the IT System Manager.] [DATE OF APPROVAL]
Information Asset Owner	[Enter the name of the Information Asset Owner.] [DATE OF APPROVAL]
System Accreditor	[Enter the name of the system Accreditor.] [DATE OF APPROVAL]

Note: It is a legal requirement in the UK to hold communication logs for up to 12 months from the date the communication took place (although not the content).

Forensic Readiness Policy

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESC (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

About this document

This document is the Ministry of Justice (MoJ) IT Security – Forensic Readiness Policy. It provides the core set of IT security principles, expectations, roles and responsibilities for the capture and preservation of digital evidence.

How to use this document

Each policy statement outlines a security requirement and where applicable, a reference is provided to further material. A unique identify is associated with each statement for easy reference. The format of each statement is illustrated below:

POL.FRP.XXX

Policy statement text.

The policies outlined in this document form the baseline standard. Where exceptions are required, this is captured on a case by case basis in Tier 4, where approval is required from both the business group SIRO and MoJ ITSO.

Forensics Readiness Policy

Introduction

The aims of this policy are to:

- Maximise the effectiveness of any digital incident investigation which may be required, normally as a result of a security incident;
- Help protect MoJ information assets through the application of best practice in IT Forensics;
- Minimise the cost and impact on the business of a forensic investigation;
- Manage the risks associated with forensic investigations, and, the risks inherent in the incident(s) that occurred, necessitating the investigation.

IT forensics is the application of techniques to detect and react to types of security incidents that require the collection, storage, analysis and preparation of digital evidence that may be required in legal or disciplinary proceedings.

The use of IT forensics as a course of action is linked to decisions made during an IT security incident. As such, this policy is linked to, and should be read in conjunction with, the [IT Security - IT Incident Management Policy](#).

This policy outlines the requirements to collect, preserve and analyse data in a systematic, standardised and legally compliant fashion to ensure the admissibility of evidence in a legal case, dispute or disciplinary hearing relating to an incident.

POL.FRP.001

Each IT system or IT domain **must have** (or be explicitly covered by) a Forensic Readiness Plan which implements this policy.

Note: In general, where an IT system (or IT domain) has an IT Security Incident Management Plan, there should be a corresponding Forensic Readiness Plan.

A template Forensic Readiness Plan is [available](#) with further guidance provided in [IT Security - Forensics Readiness Guide](#).

Scope

This Policy applies to all users of MoJ IT systems; this includes contractors and third parties who have access to MoJ information assets or IT systems.

Planning principles

Detection

Skilled perpetrators may attempt to cover up their unauthorised or malicious actions. An investigator, using IT forensic tools, can detect these actions and take suitable actions to limit the risk exposure from an incident.

POL.FRP.002

The MoJ **must have** the capacity to conduct a forensic investigation (as required), whether it involves the use of internal or external capability and resource.

Deterrence

IT Security awareness training ensures staff are aware of the [IT Security Acceptable Use Policy](#) and that the MoJ has the right and ability to monitor all IT systems for conformance to this policy. This may deter staff from inappropriate, illegal or malicious actions. Additionally, external awareness of MoJ system monitoring capability may also deter unauthorised users from attempting to access or attack MoJ facilities and IT systems.

POL.FRP.003

All users of an IT system **must be** made aware that their access is monitored and that as part of an investigation into a security incident, IT forensic techniques may be used to capture evidence.

Consistency

An IT Security Incident Management Plan documents a set of pre-planned procedures and methods for instigating and conducting an investigation. Part of this plan is concerned with the criteria for forensic monitoring and investigation. This is to ensure that all forensic investigations are conducted in a consistent, repeatable fashion.

POL.FRP.004

Each IT security incident management plan **must outline** the criteria for initiating a forensic investigation.

POL.FRP.005

A Forensic Readiness Plan **must contain** a defined set of procedures and methods for conducting a forensic investigation.

Business continuity

It is essential that the MoJ is able to resume or continue business operations after an IT security incident event. It is therefore important that a forensic investigation is conducted in a manner that supports the restoration of IT services. For example, a forensic investigation may involve the removal of hardware assets; steps should be taken to inform the relevant IT supplier to ensure replacement assets are installed.

POL.FRP.006

The procedures and methods outlined in a Forensic Readiness Plan **must consider** the business continuity

arrangements required to support the restoration of IT services.

Evidential ownership and responsibility

Digital evidence can be exceptionally fragile and must be handled extremely carefully to remain admissible. It is essential that at all stages of an incident's investigation, there is a clearly documented chain of custody for all evidential items, including a clear record of who was responsible for carrying out actions upon these evidential items.

POL.FRP.007

For all stages of a forensic investigation, there **must be** a clearly documented chain of custody for all evidential items captured.

POL.FRP.008

Each forensic investigation **must have** a named forensic investigation owner who is responsible for conducting the investigation and the integrity of any evidence captured.

POL.FRP.009

Any investigative action taken on an evidential item (e.g. an analysis of a hard drive) **must be** captured and recorded. This record **must include** details of the action taken and the person responsible for undertaking that action. Responsibility for the integrity of evidence resides with the Forensic Investigation Owner and MoJ Operational Security Team (OST). In addition, responsibility for any evidence captured, by or passed to an external forensic provider at the start of an investigation, resides with the MoJ and the Forensic Investigation Owner.

POL.FRP.010

Admissibility of evidence in a court of law varies with the method of capture. Advice **must be** sought from the MoJ legal team and forensic investigation provider prior to capture if required.

POL.FRP.011

Each Forensic Readiness Plan must include details of how any IT assets used or captured as part of a forensic investigation are securely disposed when they are no longer required. This must be in line with IT Security – IT Asset Disposal Guide [IT Security – IT Asset Disposal Guide].

Enforcement and escalation

Forensic investigations are closely related to MoJ IT security incident management processes. Clear, predefined roles and escalation points will assist in reducing the impact of an incident and allow the business to recover more quickly.

POL.FRP.012

Each Forensic Readiness Plan **must have** an escalation path to raise issues identified as part of an investigation as required.

Note: The escalation path outlined in a Forensic Readiness Plan should align with the escalation path in the corresponding IT Security Incident Management Plan.

Legality

Consideration must be taken in account of the legal and regulatory constraints which apply to the MoJ, which may differ from region to region.

BS 10008 is the British Standard regarding legal admissibility of evidence. This standard provides the foundation for the capture of evidential data (including capture from IT systems).

POL.FRP.013

All investigations **must be** conducted in line with MoJ IT Security Policies, specifically [IT Security - Acceptable Use Policy](#).

POL.FRP.014

The capture of evidence during a forensic investigation **must be** in accordance to [BS 10008](#).

POL.FRP.015

All IT systems **must consider**, in their design, the need to capture evidence in an evidential way following [BS 10008](#).

Note: Guidance on evidential capture in accordance to [BS 10008](#) is provided in [IT Security - Forensics Readiness Guide](#).

The need for IT Forensics*Business risks that require digital evidence collection*

It is necessary, as part of incident management, to have the ability to collect and analyse data held on a variety of electronic devices or storage media that may be used as evidence in some future investigation.

The decision to conduct a forensic investigation

Other than as required by the MoJ's obligations under UK law, all decisions to forensically monitor or investigate a potential security incident must be justified by a risk analysis relating to the need to obtain forensically sound evidence, followed by a cost benefit analysis of how much the required evidence will cost to collect, and what benefit it provides.

POL.FRP.016

Unless required by UK law or requested by UK law enforcement, a cost benefit analysis **must be** undertaken before a forensic investigation is launched.

All investigations will either be:

- Proactive forensic monitoring - As part of an identified MoJ security control, where the appropriateness, legality and costs have been assessed and accepted by the relevant business unit or risk owner.
- A reactive investigation - Where a suspicious incident has been identified (or reported). These investigations require the appropriateness, legality, effects of business disruption, cost and availability of key resources to be considered before the investigation is started.

Forensic investigations are only to be carried out under the following circumstances:

- Risk Management of a system has revealed a particularly sensitive/vulnerable area which needs to be proactively monitored. Any discovered security incidents would then be escalated through the IT security incident management process.
- A business function has issued a request to gather forensic investigation evidence directly to the MoJ Defensive Security Operations Team (DSOT). Results of such an investigation will be handed back to the requesting business function. Any request will be processed through the appropriate incident management process and escalated to the ITSO, DSO or SIRO as required.
- An investigation is requested as part of the IT security incident management process. Results of the investigation will be reported back through the incident management process, but other subsidiary processes may also be invoked. Further details available in the [IT Security – Forensic Readiness Guide](#).
- A forensic investigation is requested by the DSO as part of a leak investigation. Results of an investigation under these circumstances will be reported back to the DSO, who will report to the Permanent Secretary. Further information is available from the [Corporate Security and Business Continuity Branch](#).

POL.FRP.017

Each Forensic Readiness Plan **must include**, in the criteria for conducting an investigation:

- An assessment of the risk management benefits;
- The investigation has been authorised by the ITSO, DSO or business group SIRO;

- The consideration of a forensic investigation is in line with the corresponding IT security incident management plan process.

POL.FRP.018

Where a forensic investigation has been requested in response to a leak investigation. This investigation **must be** requested by the DSO where the DSO is responsible for that investigation.

Note: This may fall outside of the IT security incident management process.

Capability to collect evidence

MoJ forensic principles

The following forensic principles are based on [ACPO guidelines](#):

- Preservation of Evidence - The forensic investigation process needs to preserve the integrity of the original evidence by providing sufficient security, legal advice and procedural measures to ensure that evidential requirements are met. Any processes applied to copies of evidence must be repeatable and achieve the same results.
- Aptitude for the task - Any task in a forensic investigation will need to be conducted by a person who is suitably trained and competent to carry out that task.
- Documented Methodology – All investigations need to follow a documented methodology, as outlined in a Forensic Readiness Plan, with an audit trail of all processes applied to collect evidence. A chain of evidence will need to be created and preserved to demonstrate where evidence has been stored and under whose responsibility from capture until presentation. This allows other investigators to repeat those processes to obtain the same results as required.
- Conformance - Investigations need to be conducted in a manner which is inline with MoJ policies (this includes all MoJ corporate policies, not just IT Security policies).

POL.FRP.019

Each forensic investigation **must be** guided by the following principles (further detail is provided in section 4.1):

- Preservation of Evidence;
- Aptitude for the task (i.e. ability and skill to conduct a forensic investigation);
- Documented Methodology (as outlined in a Forensic Readiness Plan);
- Conformance to MoJ policies.

Evidence collection and storage

Collection and management of evidence is the responsibility of the Forensic Investigation Owner for any particular investigation. This may involve the use of an external organisation to conduct the investigation, from the point of capture until presentation back to the MoJ. At all stages of an investigation, all evidential items collected from MoJ sites or IT systems need to be managed according to the applicable Forensic Readiness Plan.

POL.FRP.020

Each Forensic Readiness Plan **must include** a process for the collection and storage of digital evidence (including provision for where this task is conducted by an external organisation).

Internal reporting and communication

For all incidents it is necessary to consider the internal reporting and communication requirements, both from the perspective of informing senior management that an incident is ongoing, and also the danger that such a communication might pre-warn any investigation target that remedial and investigative activity is in hand. Roles where reporting and regular communication should be considered include:

- Senior Management;
- SIRO;
- Corporate IA team;
- HR (where staff related matters are relevant);
- Internal Audit;
- MoJ legal team;
- MoJ Data Access and Compliance Unit (DACU) – where an incident involves personal data.

POL.FRP.021

Each Forensic Readiness Plan **must include** the reporting structure and escalation path which outlines the roles involved and what communications is passed. This must be consistent with reporting structure in the corresponding IT Security Incident Management Plan.

POL.FRP.022

Each Forensic Readiness Plan must name a single point of contact that is responsible to co-ordinating any stakeholders involved in a forensic investigation they may be the Forensic Investigation Owner.

External reporting and escalation

For major incidents it is necessary to consider escalating the forensic investigation process to external bodies, including:

- Other Government Agencies (if common assets are affected, or if there are consequential effects);
- Law Enforcement;
- CESG, including GovCertUK and CINRAS;
- Cabinet Office (as part of the annual returns required by the SPF);
- MoJ legal advisors.

Responsibility for escalation normally resides with the Information Asset Owner (IAO) who may also be in charge of the incident investigation. Where responsibility for an investigation has been escalated to the DSO or SIRO, further escalation responsibility will also reside with them.

The impact upon any relevant ongoing operational activity has to be considered before external reporting and escalation is invoked. The forensic investigation process needs to allow for the chain of evidence to be passed to outside agencies (e.g. a law enforcement agency).

POL.FRP.023

Each Forensic Readiness Plan **must include** details of any external (non MoJ) entities which form part of the reporting structure and escalation path.

References

ID	Title	Version / Issue
1	IT Security - Technical Controls Policy	V1-00
2	IT Security - Acceptable Use Policy	V1-00
3	IT Security - Information Classification and Handling Policy	V1-00
4	IT Security - IT Incident Management Policy	V1-00
5	HMG Security Policy Framework	Version 8, April 2012
6	MoJ Accreditation Framework	V0-01

ID	Title	Version / Issue
7	BS 10008:2008 - Evidential weight and legal admissibility of electronic information	November, 2008
8	Corporate Security and Business Continuity Branch	n/a
9	Good Practice Guide for Computer-Based Electronic Evidence – Published by ACPO.	Version 4, 2008
10	IT Security - Forensics Readiness Guide	V0-01
11	IT Security – IT Asset Disposal Guide	V0-01

Incident Management Plan and Process Guide

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI ([Centre for the Protection of the National Infrastructure](#)), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

About this document

This document is the Ministry of Justice (MoJ) IT Security – Incident Management Plan and Process Guide. It is designed to help protect the information assets of the MoJ through the formal documentation of procedures surrounding the management of IT security incidents.

How to use this document

This document provides guidance on implementing the MoJ [IT Security – Incident Management Policy](#). It should be used to guide the development of a MoJ business group level IT Security Incident Management Plan whose scope covers all IT systems used to support that business group.

For the purposes of this document, the following term will be used:

- **IT Security Incident Management** will be referred to as **ITSIM**.

Overview

Introduction

The ability of the MoJ to react quickly to IT security incidents will ensure that losses are minimised and the business will be able to resume or continue operations as quickly as possible.

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful incident management and all MoJ systems will rely upon the development and implementation of an IT Security Incident Management (ITSIM) plan as described in this guide.

The [HMG Security Policy Framework](#) mandatory requirements 4 states that:

Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business.

The policy on IT Security Incident Management is covered in [IT Security Policy - IT Incident Management Policy](#) while this document set outs the MoJ guidance for creating an ITSIM plan. This guide must be read in conjunction with [CESG GPG No. 24 – Security Incident Management](#).

Aim of this guide

The aim of this guide is to ensure all MoJ business groups develop, implement and maintain an ITSIM plan.

This guide is split up into four sections:

- An overview of principles of IT security management, its lifecycle and stakeholders;
- Planning and preparation;
- Managing an IT security incident and;
- Capturing lessons learnt.

A template ITSIM plan is provided [here](#), this is not designed to be a rigid template and can be flexed to meet the needs of the business.

Demonstration of Compliance

The [CESG Information Assurance Maturity Model \(IAMM\)](#) sets out the minimum maturity level Government departments should attain. IT asset disposal is captured as a basic requirement in Level 1 where the MoJ will need to demonstrate compliance.

Principles of IT Security Incident Management

ITSIM is a combination of people, plans and predefined processes which enables the MoJ to deal with the consequences of an IT security incident. ITSIM at the MoJ follows the following principles:

Consistency

The use of dependable, documented methods ensures that incidents, and the reaction to them, are dealt with systematically and cost-effectively.

Business Continuity

It is essential that the business is able to resume or continue operations as soon as possible after a security incident.

Ownership and Responsibility

IT security incidents can be very distressing times but reacting on impulse often does more damage than the initial incident itself. The purpose of incident management is to ensure that people with the right level of expertise and experience are consulted and take responsibility for decisions made.

Escalation

IT security incidents may require coordination with external agencies such as law enforcement or computer forensic capabilities. Internally, different functions within the MoJ may need to be involved in incident management. ITSIM ensures that communication channels are predefined and appropriate for the categorisation of an incident.

Preservation of MoJ's reputation

Information breaches or IT security incidents are extremely sensitive; both politically and how they viewed by the media and public. When major incidents do occur, as well as escalation within MoJ, there is a public relations requirement to manage how information and questions are dealt with. A good ITSIM should minimise the reputation damage to the MoJ were an incident to occur.

ITSIM Stakeholders**Table 12: IT Security Incident Management Stakeholders**

Stakeholder	Role
All MoJ staff (including contractors and agency staff)	<p>All MoJ staff (including contractors and agency staff) play a role in identifying and reporting IT security incidents.</p> <p>All staff must report any concerns especially when the IT security policy is not being adhered to, or where suspicious activity may indicate a security incident is being (or highly likely to be) committed. Moreover, if there is a strong likelihood that a security incident may occur, this must also be reported.</p>
MoJ Senior Managers	<p>MoJ Senior Managers hold a position of responsibility and can form part of the decision making process during the management of a live IT security incident.</p> <p>MoJ Senior Managers must ensure that all IT security incidents or personal data breaches are taken seriously and sufficiently investigated, and where necessary, corrective, disciplinary and or legal proceedings are actively pursued.</p>

Senior Information Risk Owner (SIRO)	<p>MoJ Business Group SIROs are responsible for implementing and managing information risk in their respective business groups and, reviewing the application of policy and guidance regularly thereafter to ensure it remains appropriate to their business objectives and risk environment.</p> <p>In the context of ITSIM, the SIRO forms part of the escalation path where incidents which are categorised as having a high impact or involve personal data (see here) are reported to the SIRO as a matter of course. They are also responsible for ensuring that their business group has an ITSIM plan.</p>
Information Asset Owner (IAO)	<p>IAOs are senior individuals involved in running business units. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. MoJ IAOs must understand and address risks to the information, and ensure that information is fully used within the relevant laws, and provide written input and assurance to the SIRO annually on the security and use of their asset. They will be informed of any security incidents which compromise any information assets under their ownership.</p>
MoJ IT Security Officer (ITSO)	<p>The MoJ ITSO is responsible for IT security across the MoJ and is the first point of escalation. The ITSO performs two functions with regards to ITSIM; Firstly, a source of advice and guidance on MoJ IT security policy and secondly, forms part of the decision making process during the investigation and resolution phase of an IT security incident.</p>
MoJ Operational Security Team (OST)	<p>The MoJ OST forms the core of the MoJ ITSIM response mechanism. They act as a co-ordinator managing all IT security incidents across the MoJ estate.</p> <p>The OST are responsible for:</p> <ul style="list-style-type: none"> • Incident ownership, monitoring, tracking and communication • Sanctioning enhanced monitoring on IT systems where appropriate • Updating the incident management database with details of all incidents, any investigation conducted and actions undertaken • Carrying out analysis of security incidents as required • Initiating a forensic investigation and commissioning forensic analysis (in accordance with Forensic Readiness Policy) • Providing progress reports on specific incidents to relevant parties.
IT Service Desk	<p>The MoJ IT service desk act as the first point of contact for MoJ IT Users reporting an IT security event. Their function is to ensure that the details of the incident are captured and the OST are informed.</p>

Lifecycle

ITSIM follows a typical risk management lifecycle (see Figure 1) based around:

- Preparation and planning;
- IT Security Incident Management;
- Lessons learnt and continuous improvement.

IT Security

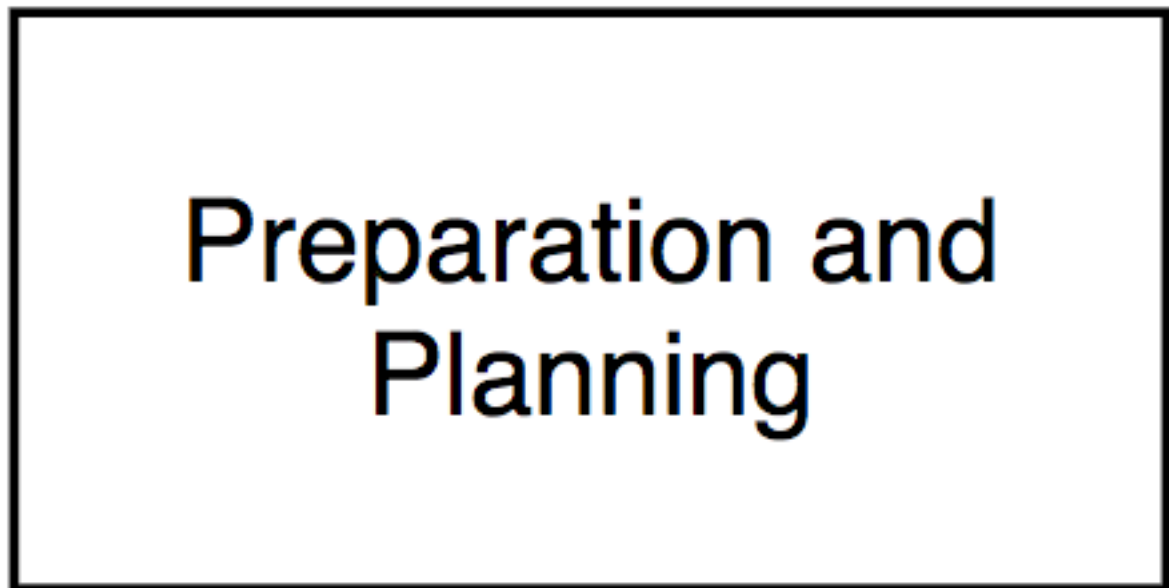


Figure 1 - IT Security Incident Management Lifecycle

The remainder of this guide explores each of these three components and provides guidance on what is required and the activity which must take place in order to create an ITSIM Plan which is fit for purpose.

Preparation and planning

The core of ITSIM is preparation and planning, the plan itself needs to be developed mindful of the environment an IT system operates in including the business context. Figure 2 below represents the flow required to develop and implement an ITSIM plan.

Prepa

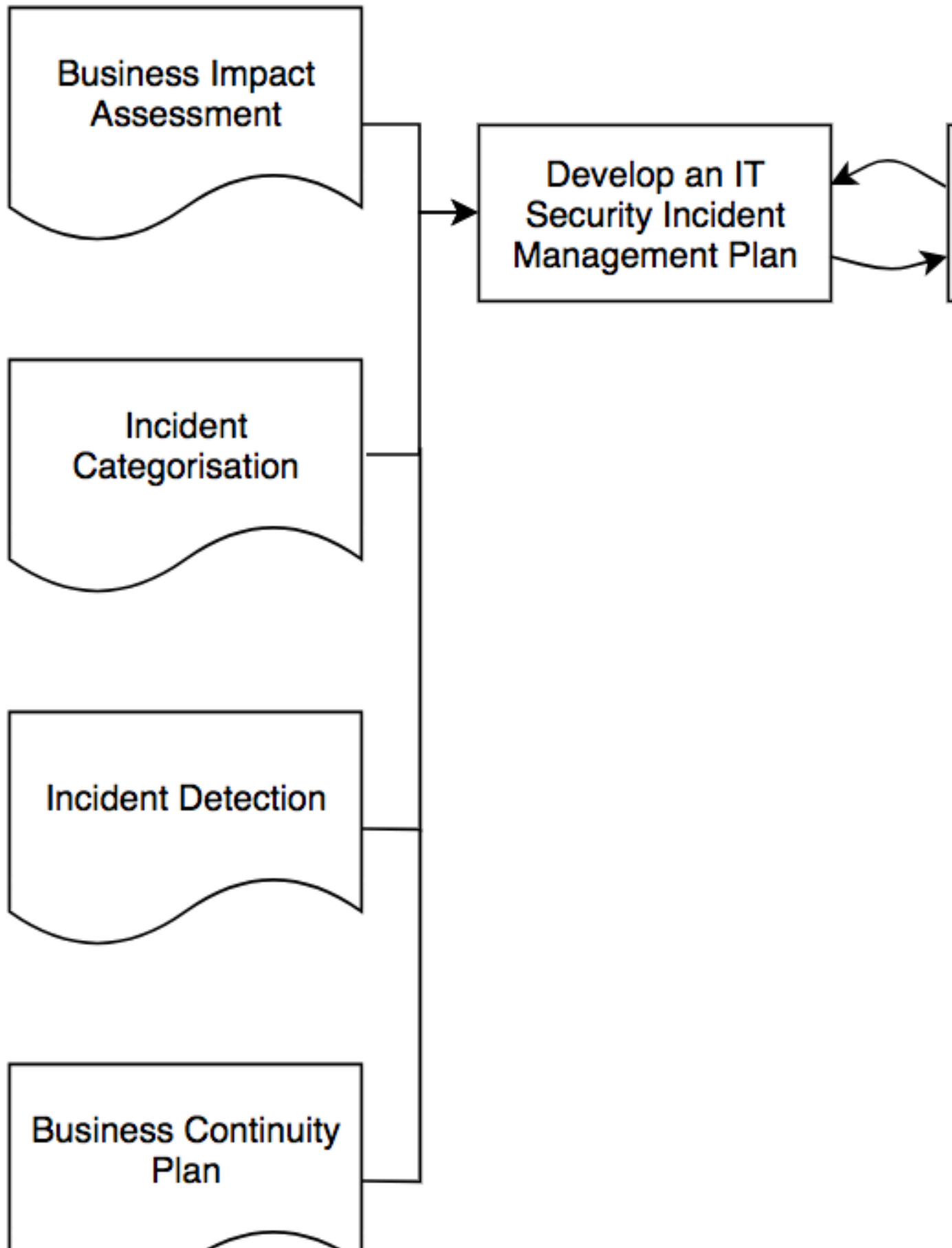


Figure 2 – Preparation and planning

Developing an ITSIM plan

A good ITSIM plan requires a good understanding of the business, the information assets and IT systems involved, the impacts to the business were an incident to occur and the overall business continuity requirement.

Input	Role
Business Impact Assessment (BIA)	The BIA provides the core rational on how the business views the impact to their information assets and services from a loss of Confidentiality, Integrity or Availability. Where this is useful in the development of an ITSIM plan is that the BIA 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.
Incident Categorisation	<p>The IT Security – IT Incident Management Policy and this guide (see here) provides a generic incident categorisation schema. This generic scheme should be used to develop final schema contained within the ITSIM plan. The aim at this phase of developing the ITSIM plan is to:</p> <ul style="list-style-type: none"> • Explore the different types of incidents which could or have occurred. For example a good starting point is a review of relevant system RMADS to identify possible incident types. • Compare the incident types identified with the information assets and services which could be impacted and broadly align each type to impact category (high impact, medium impact or low impact, see here for further details on the response level for each category).
Incident Detection	It is unlikely that an ITSIM plan will be developed in isolation and the IT systems which fall under the scope of the plan will have security controls and procedures which directly or in-directly support incident detections, for example an anti-virus client or intrusion detection system (IDS).
Business Continuity Plan (BCP)	Though the ITSIM plan concentrates on the management of IT security related incidents, ITSIM sits within an overall BCP. It is vital that the relevant BCP is factored in the creation of the ITSIM plan and it is advised that both teams work together as both plans are closely linked and need to be aligned.

Table 2 – Inputs to the IT Security Incident Management plan

Test and refine

Before implementing an ITSIM plan, it is generally good practice to test out as many aspects of the plan as possible in-order to refine its processes and operations. This is likely to involve a number of iterations and include the testing of any automated detection tools.

Implementing the plan

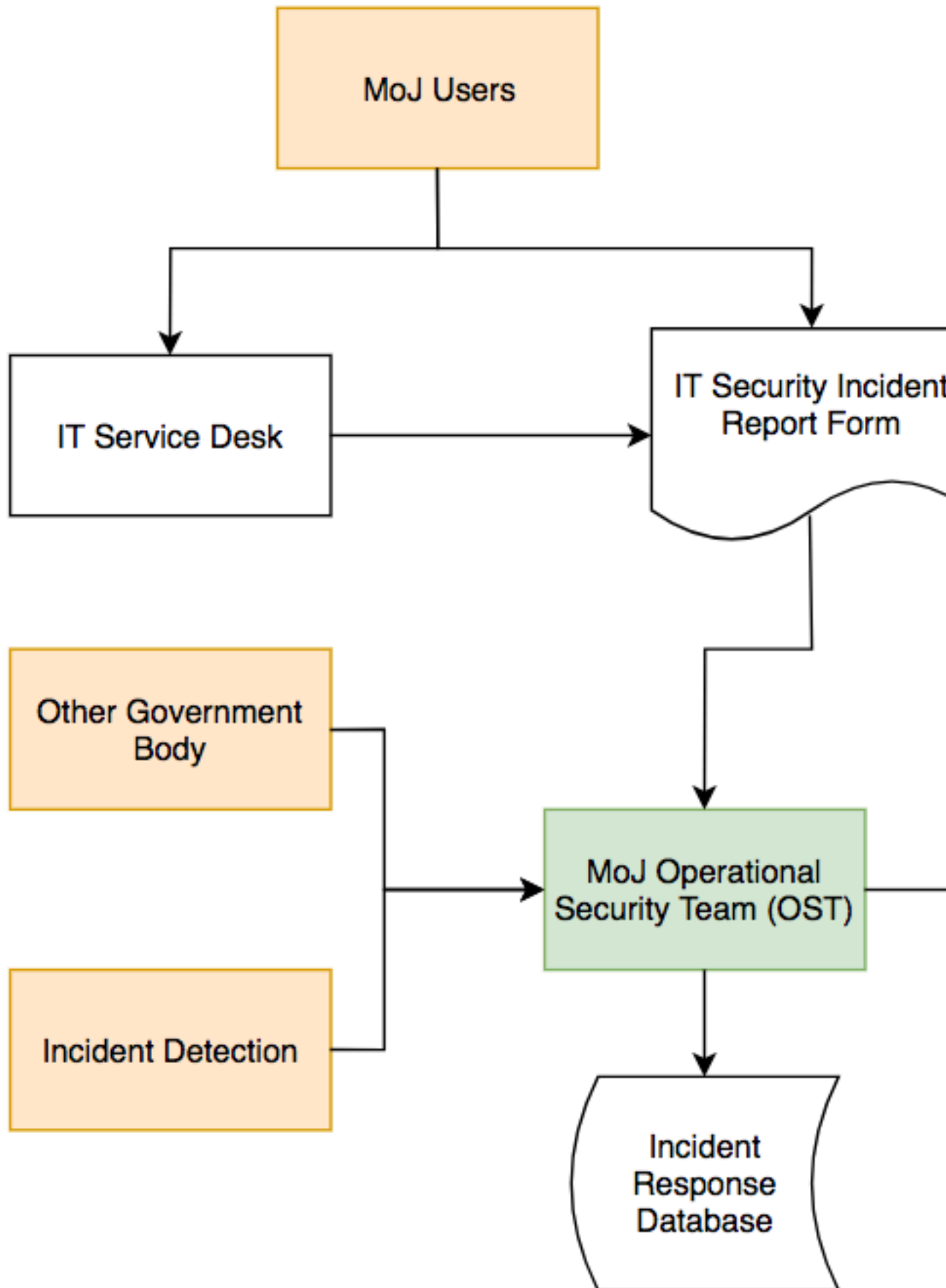
Table 3 below provides a list of the main outputs required to implement an ITSIM plan.

Outputs	Role
IT Security Incident Management Plan	Though obvious, a final released version of the ITSIM plan is the primary output. It must be approved by the business group SIRO and ITSO. It must be released to all Users and stakeholders identified in the plan.
Security Controls	The development of an ITSIM plan may lead to the requirement for further security controls to be introduced. For example the ability to collate anti-virus detections centrally.
Monitoring Services	For an ITSIM plan to be effective, a consummate incident detection and monitoring service must be in place and active. For most MoJ ITSIM plans, this will involve the MoJ Operations Security Team (OST) acting as the centralised monitoring and management service where incident reports are fed to them, for example, from automated security controls (such as virus detection alerts from an anti-virus client) or manually by a User reporting the loss of a MoJ laptop to the IT service desk.
Training and Awareness	All Users must be provided with awareness training which covers the ITSIM plan and their role in incident detection, reporting and management. For those who perform specific roles within the plan such as a Senior Manager, they should undertake additional training to ensure they are prepared to fill their aspects of the plan.

Table 3 – Outputs from implementing the IT Security Incident Management plan

IT Security Incident Management

Incident management requires a variety of decisions to be made, drawing on expertise from a variety of backgrounds, including technical, administrative and managerial depending on the nature of the incident. The incident management process supports the decision making process and subsequent courses of action taken to resolve an incident.



Key



Figure 3 – IT Security Incident Management flow

The ITSIM process essentially consists of three elements:

- Incident reporting – This is shown as a source of incident information on Figure 3. Generally there are three sources, MoJ Users reporting incidents using an IT Security Incident Report Form, alerts from other government bodies such as GovCERT and incident detection controls such as an IT supplier reporting the release of an emergency critical patch or an automated alert from an Intrusion Detection System (IDS).
- Incident management – This is a function performed by the MoJ Operational Security Team (OST), it involves conducting an initial assessment of the incident, incident categorisation and management of the incident escalating where appropriate. Note that the process continually examines the categorisation of an incident as it is being investigated. An incident may move up or down the impact scale as more information is discovered.
- Incident resolution – Where an incident has been through the management process and resolved.

What constitutes an 'incident'?

For the purpose of this document, an incident is defined as any event or action that results in an actual and/or potential compromise of personal and sensitive personal data, MoJ information assets and/or the MoJ IT infrastructure.

Types of Incidents

The list of incident types provided in this section is not exhaustive and mirrors the list provided in the [IT Security – IT Incident Management Policy](#). Each ITSIM plan must contain a definition of what constitutes an incident which results in the plan being activated, this definition can solely refer to the list provided in the policy, however there may be incident types which are specific to a particular business area which need to capture. The list of incident types includes (but is not limited to):

- Breaches of the [IT Security - Acceptable Use Policy](#);
- Detection of malicious code (e.g. a piece of malware);
- Network attacks or Denial of Service (DOS) attacks;
- Scanning and probing of a network (where significant network resources are consumed);
- Inappropriate use of MoJ IT assets as defined in the [IT Security – Acceptable Use Policy](#);
- The discovery of a new network vulnerability or release of a patch or software update which is considered critical or an emergency;
- The results of a penetration test on a live operational IT system that reveals critical vulnerabilities;
- Unauthorised access to an IT system;
- Accidental loss of personal or other information assets;
- Deliberate release of personal or other information assets;
- Compromise of integrity;
- Any alerts or suspicious activity report generated by an IT system that proves to be a real security alert.

Business related IT security incidents include (but is not limited to):

- Harm to an individual as a result of the compromise of MoJ information assets;
- A significant loss of availability at the MoJ site at which processing and storage of MoJ information takes place;
- The theft or loss of MoJ information;
- The likelihood that a MoJ department or function will be brought into disrepute or might suffer reputational damage;
- A significant impact on the ability of the MoJ to perform its duties;
- A long recovery period either in terms of practical matters or reputation;
- An event that is of interest to local/national press;
- Evidence of espionage activities;
- Accidental loss of personal or sensitive personal information;
- Deliberate release of personal or sensitive personal information.

Incident Detection and Recording

Security incidents may come to light from a variety of sources, including through active system monitoring and the MoJ staff reporting suspicious activity or security incidents. All IT security incidents must be reported to the OST, who will conduct an initial assessment and manage the incident through to resolution.

Note – All incidents involving personal data must also be reported to the MoJ Data Access and Compliance Unit (DACU).

The [MoJ IT Security Policy](#) defines the requirements for capturing and recording security events and monitoring them for suspected malicious activity or breaches of security.

The MoJ Operational Security Team (OST) is responsible for maintaining a centralised database and view of all IT security incidents across all MoJ IT systems. This database contains information on:

- Security incident reports;
- An up to date status of all reported security incidents;
- An up to date status of any actions taken with respect to a particular security incident.

This database and the effective reporting of security incidents which populate it are important in managing the MoJ's overall risk exposure. This is both in the short term, to identify any major deficiencies with an IT system which requires immediate remedial action and in the long term, to capture lessons learnt to improve Information Assurance maturity and the ITSIM plan itself.

Categorisation of Incidents

Incidents need to be categorised to assess their impact and the required level of escalation and reporting. This is mainly done to manage resources and make investigations cost effective. The initial assessment for all IT security incidents will be made by the OST with support from the ITSO and the relevant system Accreditor as required. The assessment will be in terms of the potential impact of the incident with each incident categorised in terms of Low, Medium or High impact.

The three sub-sections below provides a description for each category, it is expected that the business group ITSIM plan will contain a tailored version of this description and confirm the escalation route which will be followed.

Low Impact Incident

These would typically be minor such as low level breaches in security through an accident or carelessness, or a minor loss of service from a service provider e.g. temporary loss of power or connectivity.

A low impact personal data incident would typically include an incident where no loss has occurred but a weakness in a system may potentially have led to a loss, and with a small amount of remedial action the weakness in a process can easily be addressed.

Incident categorised as low will be typically managed by the MoJ OST who will engage with the relevant parties within the business and IT supplier community to resolve the incident. Any escalation (see Figure 4) will be predominantly to the level of the MoJ ITSO and relevant system Accreditor.

Medium Impact Incident

Examples of medium impact incidents include (but not limited to):

- Deliberate disregard for the [IT Security Policy](#) leading to minor breach in security or the potential of data loss;
- Inappropriate use of MoJ IT assets as defined in [IT Security - Acceptable Use Policy](#);
- Loss of data or IT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Theft of data or IT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Damage to any MoJ IT asset;
- Connecting unauthorised equipment to an IT system (where there is no intent or suspicion of malicious activity);
- 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;

- Any alert or reported suspicious activity on an IT system (note this may need to be escalated to High Impact upon investigation);
- Compromise of IT system integrity;
- The recognition of a new critical security vulnerability in an IT system (this may be the result of a penetration test);
- The release of a critical patch by an application or IT equipment vendor;
- Localised report of malicious code (e.g. the detection of a virus or malware of a desktop terminal);
- Serious case of equipment theft;
- The theft or loss of HMG cryptographic material.

Medium impact incidents require escalation to the MoJ ITSO who will determine whether the IAO and relevant system Accreditor also need to be informed. In the case of personal or sensitive personal data, the MoJ Data Access and Compliance Unit (DACU) also need to be informed. If deemed appropriate, a forensic investigation will be requested by the MoJ ITSO in line with the [Forensic Readiness Policy](#).

High Impact Incident

High level IT incidents require immediate escalation to the Senior Information Risk Owner (SIRO) and relevant Information Asset Owner/s.

Examples of incidents requiring this level include (but are not limited to):

- Evidence of espionage activities;
- An incident that is of interest to local/national press;
- A significant impact on the ability of the MoJ to perform its duties;
- The likelihood that MoJ function will be brought into disrepute or might suffer reputational damage;
- Any successful network intrusion to MoJ IT facilities;
- Widespread malicious code attacks;
- The release of an emergency patch released by a manufacturer used by the MoJ (as described in the Security Patch Management Policy);
- The loss of a MoJ, or suppliers, site at which processing and storage of MoJ information takes place for more than one working day;
- The theft or loss of MoJ protectively marked information which could include CONFIDENTIAL and above, or a significant quantity of RESTRICTED material.

It is highly likely that an incident of this magnitude would require the MoJ ITSO to instigate a forensic investigation and start collecting evidence.

Further Escalation Requirements

The decision to escalate an incident beyond the MoJ business group SIRO remains with that SIRO where advice will be provided by the MoJ ITSO.

Incidents that require this type of escalation include (but are not limited to):

- Issues of national security;
- If the incident has received local or national press coverage;
- If the incident has caused or might cause harm to MoJ Staff;
- There is a high likelihood the MoJ will be brought into disrepute or might suffer reputational damage;
- If the incident involves (or is suspected to involve) Foreign Intelligence Services (FIS) or Organised Crime;
- Where there is a HMG requirement to report to central incident management bodies, the OST will co-ordinate reporting for example, the reporting of network security incidents to GovCERT;
- Where there is a significant, actual or possible loss of personal data, the Information Commissioner's Office and the Cabinet Office Central Sponsor for Information Assurance need to be informed via the SIRO and ITSO

Investigation and Diagnosis Capability:

The MoJ Operational Security Team (OST) is responsible for organising the investigation of all IT security incidents. Where there is a need for evidence to be gathered for possible disciplinary or legal proceedings, a forensic

investigation may be required. Each impact category should have its own associated management process which consists of the following activities:

- Investigating an incident as directed by the ITSO or SIRO;
- Proactively monitoring any IT system involved in the incident to capture suspicious behaviour;
- Where authorised by the MoJ SIRO, providing evidence to disciplinary hearings, industrial tribunals, civil courts and criminal courts when required;
- Maintaining files on investigations in appropriate security storage and in accordance to privacy laws;
- Conducting investigations into information security incidents at any of the MoJ locations;
- Recovering and securely store evidence when required;

The distinction between the management processes is the priority and level of resources assigned. For example, a low impact incident involving a MoJ user attempting to access a blocked website will be processed at a slower rate than a high impact incident where a confirm and active network intrusion has been detected.

It is important to ensure that a diagnosis of the events surrounding each incident is recorded and shared with the relevant stakeholders.

Where there has been a personal data incident or where possible disciplinary or legal proceedings may be required, the following actions must be taken:

- The relevant MoJ Senior Manager must collect detailed information on the incident;
- Refer any possible disciplinary action to HR;
- Maintain records on the investigation appropriately preserving evidence.

Resolution, Recovery and Closure of Incidents

Based on the investigation and diagnosis of an incident the recovery and closure of the incident can involve many stakeholders. It is important that all stages of resolution are recovered and recorded before an incident is formally closed.

When an IT system has had a significant compromise, that system may require a review of its accreditation status in light of the circumstances of the incident. This is a decision normally made by the relevant system Accreditor.

Lessons learnt and continuous improvement

Adequate information relating to security incidents, such as types, volumes and costs must be recorded in order to identify recurring or high impact incidents or malfunctions. This may indicate the need for additional or enhanced security controls to limit the frequency, damage and cost of future occurrences or may indicate the need for a change in policy, the design of an IT system or implementation of SyOPs.

IT security incident statistics must be presented in conjunction with an assessment of top security risks and details of any significant compliance gaps on a monthly basis to the ITSO to assist risk management. Each ITSIM plan must be reviewed on a yearly basis and re-approved by the SIRO and ITSO.

Appendix A – IT Security Incident Management Plan - Template

IT Security Incident Management Plan	
Overview	
MoJ Business Group	[Enter the name of the MoJ Business Group.]
System Description and Scope	[This section must describe the scope of the ITSIM plan. Diagrams may prove useful where there is a complex interaction between systems and business processes covered by this plan.]

Escalation Path		[This section must describe the escalation path for an IT security incident (see Figure 4).]
Incident Categorisation		
Low Impact Incident	Description	[Provide a description of what a Low impact incident constitutes; see here for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consult the OST and ITSO when completing this section.]
Medium Impact Incident	Description	[Provide a description of what a Medium impact incident constitutes; see here for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consult the OST and ITSO when completing this section.]
High Impact Incident	Description	[Provide a description of what a High impact incident constitutes; see here for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consult the OST and ITSO when completing this section.]
Plan Approval		
Business Group SIRO		[Enter the name of the Business Group SIRO] [DATE OF APPROVAL]
IT Security Officer		[Enter the name of the ITSO] [DATE OF APPROVAL]

Completing this plan can form part of the Accreditation process and must be included and maintained as part of the relevant RMADS.

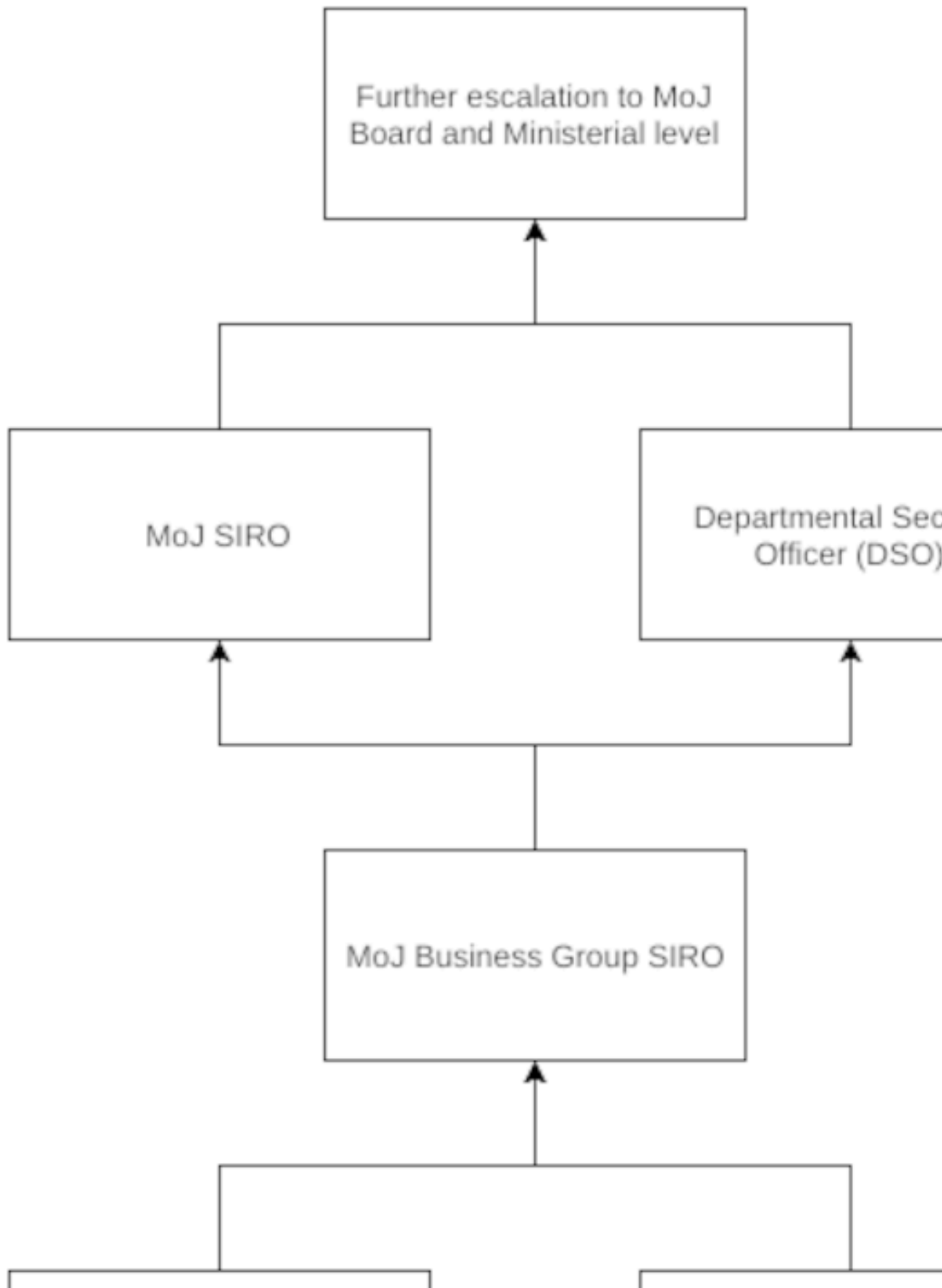
Appendix B – Escalation path

Figure 4 – ITSIM Escalation path

IT Incident Management Policy

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Introduction

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful information security management and all Ministry of Justice (MoJ) systems rely on Incident Management Plans for safe and secure operations.

The aim of this policy is to ensure best practice is followed by all IT systems when dealing with security incidents, in particular, those pertaining to data loss, in a timely and efficient manner.

POL.IMP.001:

Each MoJ Business Group **must have** an IT Security Incident Management Plan which aligns to this policy. This plan must be common to all IT systems within a particular business group.

A template plan and guidance on the construction of an IT Security Incident Management Plan is provided in [IT Security – Incident Management Plan and Process guide](#).

Scope

This policy is concerned with IT related security incidents outlining the roles and responsibilities, escalation path and criteria for escalation.

Relationship with wider MoJ functions

An IT system is one element of a number of supporting elements which sustain MoJ business functions and delivery of services. The MoJ [Corporate Security and Business Continuity Branch](#) is responsible for overall MoJ Incident Management policy and plan. This policy is designed to sit within the overall MoJ incident management structure.

Incident Management Process

An incident management process is a prepared course of actions that will be instigated upon the detection or report of a security incident. Incident management requires a variety of decisions to be made, drawing on the experience of a number of roles, depending on the nature of the incident.

The incident management process supports the making of informed decisions following a consistent approach designed to reduce the consequences of any incident.

Definition of an Incident

For the purposes of this policy, an incident is defined as any event or action which results in an actual and/or potential compromise of a MoJ IT asset or MoJ Information Asset (including personal data).

Such events will result in the MoJ, individuals or IT systems and/or the information held on them being exposed, or potentially exposed, to illegitimate access. As a result, incidents have the potential to compromise MoJ business delivery, the Data Protection Act, as well as the confidentiality, integrity and availability of IT systems and the information held on them. This may, in turn cause harm, distress or other damage to individuals or organisations, and result in operational disruption or reputation damage to the MoJ.

Types of Incidents

IT Security related incidents include (but not limited to):

- Breaches of the [IT Security - Acceptable Use Policy](#);
- Detection of malicious code (e.g. viruses and malware);
- Network attacks or Denial of Service (DOS) attacks;
- Scanning and probing of a network (where significant network resources are consumed);
- In appropriate use of MoJ IT assets as defined in the [IT Security - Acceptable Use Policy](#);
- The discovery of a new network vulnerability or release of a patch or software update which is considered critical or an emergency;
- The results of a penetration test on a live operational IT system that reveals critical vulnerabilities;
- Unauthorised access to an IT system;
- Accidental loss of personal or other information assets;
- Deliberate release of personal or other information assets;
- Compromise of integrity;
- Any alerts or suspicious activity report generated by an IT system that proves to be a real security alert;

Incident Detection and Recording

Security Incidents may come to light from a variety of sources, including through protective monitoring solutions, reports filled by MoJ staff or breaches of the MoJ IT Security Policy detected by an IT system.

The [MoJ IT Security Policy](#) defines the requirements for capturing and recording security events and monitoring them for suspected malicious activity or breaches of security.

This section of the policy is concerned with taking those security events and ensuring that if an event relates to an actual IT Security incident, this incident is appropriately recorded.

POL.IMP.002:

All IT Security incidents or suspected incidents **must be** reported to the MoJ Operational Security Team (OST) within 60 minutes of detection.

POL.IMP.003:

For all incidents involving an IT Security incident, an IT Security Incident Report Form **must be** completed and submitted to the OST ([Reporting an incident or breach](#)). This is irrespective of the reporting route (i.e. a User direct with OST or a user via the IT helpdesk).

POL.IMP.004:

All IT Security incidents involving personal data (or other information assets) **must be** reported to the MoJ Data Access and Compliance Unit: Data.access@justice.gov.uk.

The MoJ Operation Security Team (OST) is responsible for maintaining a centralised database and view of all IT Security incidents across any MoJ IT system. This database contains information on:

- Security incident reports;
- An up to date status of all reported security incidents;
- An up to date status of any actions taken with respect to a particular security incident.

This database and the effective reporting of security incidents which populate it are important in managing the MoJ's overall risk exposure. This is both in the short term, to identify any major deficiencies with an IT system which requires immediate remedial action and in the long term, to capture lessons learnt to improve Information Assurance maturity.

Categorisation of incidents

Security incidents are categorised in order to assess their impact and required level of escalation. This is to ensure that the appropriate resources can be allocated and incident resolution is conducted in a timely manner.

The three categories are:

- Low Impact (see [here](#));
- Medium Impact (see [here](#));
- High Impact (see [here](#)).

POL.IMP.005:

All IT Security incidents **must be** categorised in accordance with this policy.

The nature of an incident may not be immediately obvious when it is first reported; further assessments of its categorisation need to be made as more information is gathered. For example, through conducting an investigation (see Figure 2 which outlines this process flow).

The sub-sections below provide an overview of the three categories with further guidance on its practical application provided in [IT Security – Incident Management Plan and Process Guide](#).

Low impact incident

Low impact incidents would typically be minor internal infractions, such as, a low level breach in IT Security, or, a minor loss of an IT service (e.g. due to a short loss of power).

A low impact personal data incident would typically include an incident where no actual data had been lost but a weakness in an IT system which may have led to a potential loss is discovered where a relatively small amount of remedial action is required to address the vulnerability.

Medium impact incident

Examples of a medium level impact event include (but not limited to):

- Deliberate disregard for the MoJ [IT Security Policy](#) leading to minor breach in security or the potential of data loss;
- Inappropriate use of MoJ IT assets as defined in [IT Security - Acceptable Use Policy](#);
- Loss of data or IT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Theft of data or IT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Damage to any MoJ IT asset;

- Connecting unauthorised equipment to an IT system (where there is no intent or suspicion of malicious activity);
- Prolonged or permanent failure of an IT system;
- Prolonged set of unsuccessfully attempts to scan an IT network or instigate a denial of service attack;
- Any alert or reported suspicious activity on an IT system (note this may need to be escalated to High Impact upon investigation);
- Compromise of integrity;
- The recognition of a new critical security vulnerability in an IT system (this may be the result of a penetration test);
- The release of a critical patch by an application or IT equipment vendor;
- Localised report of malicious code (e.g. the detection of a virus or malware on a desktop terminal);
- Serious case of equipment theft;
- The theft or loss of HMG cryptographic material.

High Impact Incident

IT Security incidents at this level require immediate escalation to the relevant MoJ Business Group Senior Information Risk Owner (SIRO) in addition to the OST and where applicable, the MoJ Data Access and Compliance Unit: Data.access@justice.gov.uk.

Incident at this impact may warrant forensic investigation.

Examples of incidents at the level include (but are not limited to):

- Evident of malicious activity, intent or espionage;
- An incident which comes to the attention of local or national media;
- Any successful network intrusion;
- Widespread malicious code attacks (e.g. a worm spreading across an IT system);
- The release of an emergency patch by an application or IT equipment vendor;
- The theft or loss of personal or protectively marked data from an IT system.

Further escalation requirements

The decisions to escalate an incident irrespective of its impact up through the chain from ITSO, MoJ SIRO, DSO, and above (possible to Ministerial level) may include the following factors:

- Issues of national security;
- If the incident has received local/national press coverage;
- If the incident has caused harm to a member of staff or public;
- There is high likelihood that the MoJ has suffered reputational damage or been brought into disrepute;
- Where there is a HMG requirement to report to another Department or central management function (e.g. GovCERT for network incidents or CINRAS for incidents involving HMG cryptographic material);
- Where there is a significant actual or possible loss of personal information where the Information Commissioner's Office and Cabinet Office need to be informed.

Incident Management Stakeholders

This policy outlines the general incident management stakeholders and escalation path principles. Each MoJ business group implementation of this policy (which is the creation and acceptance of an IT Security Incident Management Plan) will need to consider how this is practically implemented, all the individual stakeholders involved (including others such as IT suppliers), and escalation path.

All MoJ staff (including contractors and agency staff)

It is important that all MoJ staff are aware of what a security incident is and how to correctly report it.

POL.IMP.006:

All MoJ staff **must** report any concerns that the MoJ [IT Security Policy](#) is not being followed to their line manager.

POL.IMP.007:

All MoJ staff **must** report any breach of the MoJ [IT Security Policy](#) as an IT Security incident.

POL.IMP.008:

All MoJ staff must report any suspicious activity which indicates an IT Security incident has occurred.

POL.IMP.009:

All MoJ staff **must** report an IT Security incident either to the IT helpdesk or directly to the MoJ Operational Security Team using an IT Security Incident Report Form.

MoJ Senior Managers

POL.IMP.010:

All MoJ Local Managers **must ensure** that all IT Security or personal data incidents or breaches are reported and taken seriously. These include facilitating any investigation and, where appropriate, pursue disciplinary action and/or legal proceedings.

Senior Information Risk Owner (SIRO)

POL.IMP.011:

Each MoJ business group SIRO **must ensure** that each IT domain (e.g. DISC or OMNI) which fall under their remit has an IT Security Incident Management Plan which implements this policy. A template plan and guidance is available in [IT Security – Incident Management Plan and Process guide](#).

POL.IMP.012:

All High impact IT Security incidents and any IT Security incident involving personal data **must be** reported to the SIRO immediately.

Information Asset Owner (IAO)

The role of an IAO is to understand what information is held, how it's adapted, used, shared and removed from an IT system.

POL.IMP.013:

All IT Security incidents involving the loss, theft or compromise of an Information Asset **must be** reported to the asset's IAO.

MoJ Operational Security Team (OST)

The OST are responsible for:

- Incident ownership, monitoring, tracking and communication
- Sanction enhanced monitoring on IT systems where appropriate
- Update the incident management database with details of all incidents, any investigation conducted and actions undertaken
- Carry out analysis of security incidents as required
- Initiating a forensic investigation and commissioning forensic analysis (in accordance with the [Forensic Readiness Policy](#))
- Providing progress reports on specific incidents to relevant parties.

Helpdesk

The IT helpdesk plays a crucial role in ensuring security incidents are correctly reported and escalated to the OST in a timely manner. The majority of IT Security incident will be reported to the IT helpdesk first. Also, the IT helpdesk can help identify where a user reporting an issue is actually an IT Security incident. It is therefore important that the IT helpdesk recognise this and report it to the OST.

POL.IMP.014:

Where the IT helpdesk receives a report of a security incident, this **must be** reported and escalated to the OST immediately.

Escalation Path

As a rule, all IT Security incidents are reported to OST. As depicted in Figure 2, OST then progress the incident according to its categorisation (see [here](#)). Depending on the category and nature of the incident, this can involve escalating the incident to other stakeholders.

POL.IMP.015:

Each IT Security Incident Management Plan **must include** a pre-arranged escalation path where each stakeholder is named and aware of their role in the Incident Management Plan.

A generic escalation path is provided [here](#). This generic path is intended to provide a starting point where further guidance on tailoring and customisation is provided in the [IT Security – Incident Management Plan and Process Guide](#).

Investigation and Diagnosis capability

The OST is responsible for the investigation of all IT Security incidents. Where evidence gathering is required for possible disciplinary or legal proceedings, a forensic investigation may be required, further details are provided in the [Forensic Readiness Policy](#).

In the course of investigation, the OST may:

- Investigate incidents at the direction of the ITSO;
- Proactively monitor suspected targets or IT systems to capture potential suspicious behaviour for analysis;
- Undertake or oversee an investigation requested by an outside agency (e.g. CESG) where authorised by the ITSO;
- Recover and securely store evidence where required;
- Require a SIRO or Senior Manager to collect more information on an IT Security incident.

POL.ITSEC.016:

The OST **must maintain** files on any investigation undertaken.

POL.ITSEC.017:

Any diagnosis of an IT Security incident and the events surrounding it **must be** shared and reported to relevant stakeholders.

Resolution, Recovery and Incident Closure

Based on the investigation of an IT Security incident, remedial action may be required to ensure appropriate incident resolution and the recovery of any IT services or information assets compromised as a result of the incident.

POL.ITSEC.018:

An IT system which has a significant compromise (Medium or High impact, see [here](#)) **must be** reported to the system Accreditor and a review of that system's risk assessment and accreditation must be conducted.

POL.ITSEC.019:

All IT Security incidents for an IT system **must be** collated and provided to the system Accreditor during the re-accreditation process.

Recovering from an IT Security incident

There may be occasions when it is appropriate to restore a system that has been attacked or compromised from its backup since it might be the only way to ensure system integrity.

Checks must be made to ensure the IT system being restored pre-dates the incident and does not contain any exploitable weaknesses, for example, ensure the IT system is fully patched before it is brought back into service.

POL.ITSEC.020:

The IT Security Incident Management Plan for an IT System or overarching IT Domain **must include** details on how that system or IT domain IT services are restored (or recovered) following an IT Security incident.

Note – The detail of how an IT system recovers from an incident event should be captured in that systems disaster recovery plan. See [IT Security – Disaster Recovery Policy](#) for further information.

Preventing re-occurrences

Once the cause of an IT Security incident has been identified, steps must be taken to reduce the risk of its reoccurrence, for example eradicate any computer viruses, block firewall ports, and install any missing system patches, as necessary.

Learning points

When an IT Security incident has been resolved and closed, a management report needs to be prepared outlining the incident, the outcome of the investigation, actions taken, and recommendations about how to improve the business systems to reduce the likelihood of a reoccurrence.

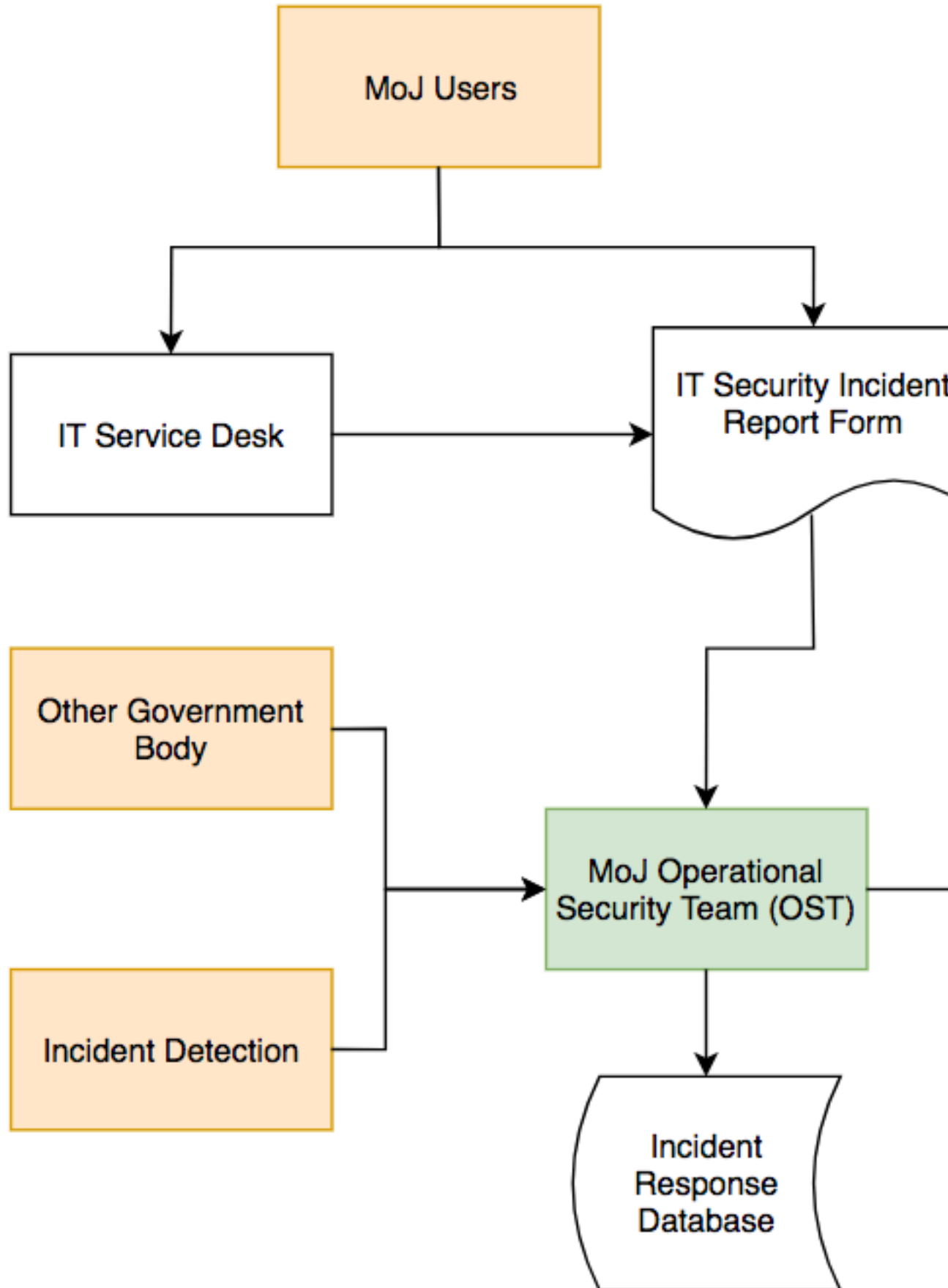
Copies of the report must be sent to the ITSO who has a responsibility for forwarding the report onto any HMG central reporting functions, for example CESG, GovCertUK or CINRAS, as appropriate.

POL.ITSEC.021:

For each Medium and High impact (see [here](#)) IT Security incident, a management report **must be** prepared covering:

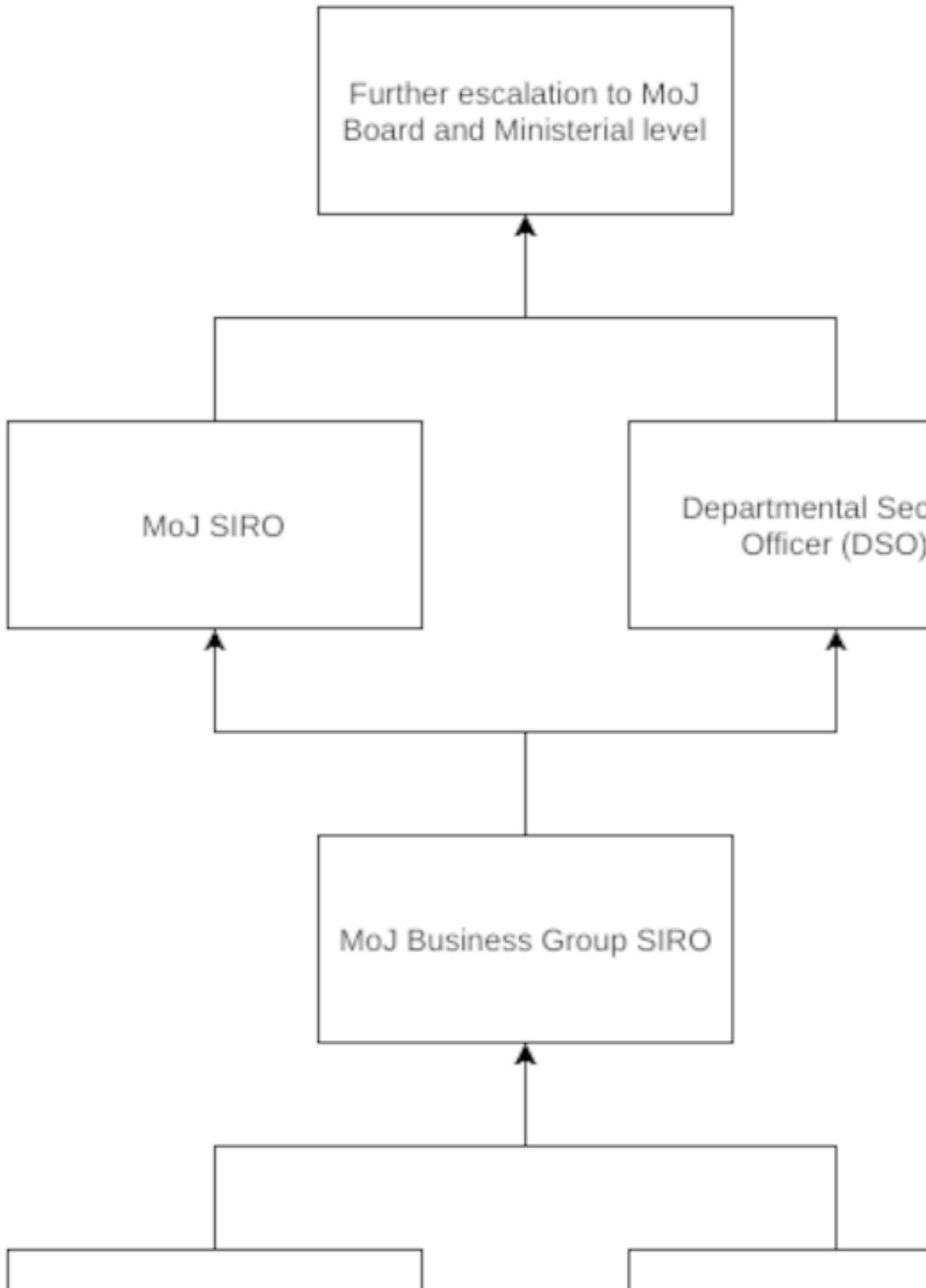
- A description of the incident;
- The outcome of the incident investigation;
- Actions raised (or taken) with associated action owners;
- Any recommendations made.

IT Security Incident Recording and Categorisation

**Key**

IT Security Incident Escalation Path

The following is a generic IT Security incident escalation path which provides a starting point for the creation of a tailored version in an IT Security Incident Management Plan. Further information is provided in the [IT Security – Incident Management Plan and Process Guide](#).



Lost devices or other IT security incidents

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Related information

[Laptops](#) on page 124

What to do if your device is lost, stolen, or compromised

If MoJ 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 MoJ 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 Technology Service Desk. The analyst will ask the relevant questions and note responses on the ticket.

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
 - Slack: #digitalservicedesk
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 [here](#).

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Information security aspects of business continuity management

Information security continuity

IT Disaster Recovery Plan and Process Guide

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESC (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

About this document

This document is the Ministry of Justice (MoJ) IT Security – IT Disaster Recovery Plan and Process Guide. It is designed to help protect the information assets of the MoJ through the formal documentation of procedures surrounding the management of IT disaster events.

How to use this document

This document provides guidance on implementing the MoJ [IT Security – IT Disaster Recovery Policy](#). It should be used to guide the development of a MoJ business group level IT Security Disaster Recovery Plan whose scope covers all IT systems used to support that business group.

For the purposes of this document, the following terms will be used:

- **IT Disaster Recovery** will be referred to as **ITDR**.
- **IT Security Incident Management** will be referred to as **ITSIM**.

Overview

Introduction

The ability of the MoJ to react quickly to ITDR events will ensure that losses are minimised and the business will be able to resume or continue operations as quickly as possible.

ITDR management is the ability to react to ITDR events in a controlled, pre-planned manner. Preparation and planning are key factors to successful incident management and all MoJ systems will rely upon the development and implementation of an ITDR plan as described in this guide.

The HMG Security Policy Framework (SPF) Mandatory Requirement 4 states that:

"Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business."

The policy on IT Disaster Recovery is covered in [IT Security Policy – IT Disaster Recovery Policy](#) while this document sets out the MoJ guidance for creating an ITDR plan. This guide must be read in conjunction with CESG GPG No. 24 – Security Incident Management and [IT Security – Incident Management Plan and Process Guide](#).

Note: The [IT Security Policy – IT Disaster Recovery Policy](#) sets out the roles and responsibilities with respect to ITDR. It states that each IT system must fall under the responsibility of an IT Disaster Recovery Team Leader (ITDRTL) who is responsible for maintaining the ITDR plan.

Aim of this guide

The aim of this guide is to ensure all MoJ business groups develop, implement and maintain an ITDR plan. This guide is split up into four sections:

- Gathering the requirements needed to shape an ITDR plan;
- Guidance on writing an ITDR plan;
- Testing an ITDR plan;
- Training and awareness.

A template ITDR plan is provided [here](#); this is not designed to be a rigid template and can be flexed to meet the needs of the business.

Demonstration of compliance

The [CESG Information Assurance Maturity Model \(IAMM\)](#) sets out the minimum maturity level Government departments should attain. IT asset disposal is captured as a basic requirement in Level 1 where the MoJ will need to demonstrate compliance against.

Relationship to Business Continuity Planning

ITDR is distinct from Business Continuity planning; specifically it:

- Includes planning for resumption of applications, data, hardware, communications (e.g. IT networks) and other IT infrastructure.

The Business Continuity Plan (BCP) is broader than the ITDR in that it puts in place a plan for the recovery of an entire business group's business operation in the event of a disaster. The MoJ's BCP contains the procedures for building, facilities, transport, people, physical information (e.g. paper) disruption and the communication of critical information to employees.

Therefore, an ITDR plans is created:

- To aid the business in returning to normal operations as quickly as possible;
- To ensure the causes of a disastrous event are captured and understood;
- To help avoid similar incidents in the future; and
- To aid the improvement of the ITDR policy and planning.

Link to IT Security Incident Management

The ITDR plan sits under an ITSIM plan. It is important to ensure that the steps encapsulated in the ITDR plan align to the ITSIM plan. Further information on the ITSIM plan can be found in [IT Security – Incident Management Plan and Process Guide](#).

Process

The process for developing a good ITDR plan can be summarised into two stages:

- Firstly a "Requirements and Planning" stage establishes the requirements for the plan.
- Secondly, during "execution" of the ITDR plan, it is important to ensure that ITDR incidents are managed appropriately, the plan is executed effectively, and that any lessons learned are fed back into the process so that future improvements can be made.

The following diagram illustrates this process.

Feedback

Step 1:
Requirements
Gathering

Requirements and Planning

Incident Management

Step A:
Declaring a
Disaster

Step B:
Invoking
p

Gathering requirements for ITDR

The ITDR process is based on understanding the Recovery Time and Point Objectives; these form the basic requirements for ITDR. This section outlines the process to identify a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and the information gathering activities required in order to create an ITDR plan.

ITDR requirements

Recovery Time Objective (RTO)

The RTO is the maximum business-tolerable time that an IT system can be unavailable. This time must be considered from the business' point of view where the RTO covers the entire period from initial failover to successful restoration of the business operations. Simply taking this time to recover a single server is not sufficient.

Recovery Point Objective (RPO)

The RPO is the amount of data loss which can be tolerated by the business after a system failover. As such, a business can either re-type or re-generate this amount of information without a significant impact on their business process.

Information gathering

The following table provides details on the base set of information sources required to support the development of an ITDR plan.

Table 13: Information sources

Information source	Description
ITDR asset register	The group of IT systems that are subject to the ITDR planning process must be captured in an ITDR asset register. The RTO and RPO for each individual IT system must be less than or equal to the overall business group RTO and RPO.
Business Impact Assessment (BIA)	For each IT system identified on the ITDR asset register, a Business Impact Assessment (BIA) is carried out. A BIA considers what impact would occur to the business in the event that the IT systems were unavailable or data were lost. This BIA may be created as part of the Risk Management and Accreditation Document Set (RMADS).

Writing an ITDR plan

This section provides guidance on writing an ITDR plan with a template provided [here](#). Each sub-section is an element of the ITDR plan.

IT System Description

For the purposes of the ITDR plan, an IT system is the collection of applications and supporting infrastructure which provides IT services to a MoJ business group. In turn, this business group supports a number of business processes – it is these processes which must be restored, not just the IT system.

In order to make clear the role of the IT system with relevance to the BCP, this section must clearly list the IT system's constituent components, as well as details of the business processes it supports. This in turn defines the scope of the ITDR plan.

Site List

This section of the ITDR plan must contain details of all the physical sites relevant to the recovery process. It must also include details of any secondary business sites, in case the primary site is affected by a disaster and IT system services need to be made available at a secondary site.

Dependencies

A list of dependencies (internal and external) must be included in the ITDR plan. Restoration of a business process may be more complex than restoration of a single IT system, and the bottlenecks or miscommunications which can

occur here are often the critical points of failure in the process. The impact of the dependency must be captured, in terms of risk, time and cost.

This information can be used in a disaster event to provide an accurate estimate time for recovery.

Internal Dependencies

Internal dependencies are those which may materialise as part of the recovery actions of the ITDR plan itself, for example:

- When a step in the plan must be completed before a subsequent step can be taken, such as restoring access to a database before conducting login testing.
- If the data centre is in a remote part of the country, and so it may take time for staff to reach the location.

External Dependencies

External dependencies are those which may affect the success of an ITDR plan and lie beyond the area of control of the ITDR Team Lead (see [IT Security – IT Disaster Recovery Policy](#) for a role description).

For example:

- Where a previous service, such as power, communication or sanitation facilities, must be restored before this system can be restored;
- Where the recovery of this system must be completed before the Incident Management team can notify staff to return to work at some location.

Invocation

Definition of a 'Disaster'

The ITDR plan must include a clear statement on what set of incidents constitute a disaster. Certain components of the IT system may be replaceable without invocation of the entire ITDR plan, whereas an apparently 'small' incident may have a wider reach which does require the plan to be invoked. This section must clarify the situations in which the ITDR plan will be invoked; it may be useful to reference incidents which may have occurred in the past.

Note: This definition must be consistent with corresponding ITSIM plan.

Invocation

The ITDR plan does not need to be invoked in its entirety. A disaster event may not require the invocation of all the procedures in the plan, and so the level of response must be assessed and clearly communicated and agreed between the business and IT leads before implementation.

This section must list those with authority to invoke the ITDR plan.

Staff Notification

Provisions must be made to inform the correct staff of the need to begin recovery procedures; this should usually be captured in the corresponding ITSIM plan.

IT supplier staff may require a different form of notification, and therefore this procedure should be clearly noted in the ITDR plan if they are not contained within the corresponding ITSIM plan.

Key Contacts

This section of the ITDR plan should detail the individuals who currently hold the roles listed in the previous section. As mentioned above, this information may be better kept in an annex.

Recovery procedures

This section of the ITDR plan must list the functions of the IT system and the business processes it supports, and relate them to a specific set of recovery actions. Functions should be categorised (into primary and secondary functions) allowing for critical business processes to be restored ahead of others.

A generic set of ITDR incident management steps is [provided](#) which should be used as the basis to structure the more granular recovery actions (see [here](#)).

Primary functions

Primary functions are those which **must be** restored in the event of a disaster. The primary functions are the business-centric and mandated processes which must be restored for the business to successfully complete its work.

Secondary functions

Secondary functions are those which **should be** restored in the event of a disaster. Priority should be aimed at the primary functions; secondary functions should be restored only after all the primary functions are restored.

Recovery actions

This section of the ITDR plan should list any actions which are to be used in the recovery effort and where possible should be cross-referenced with the relevant primary and secondary functions. It is recommended that the ITDR plan contains a high level set of actions (e.g. recover file server) with technical details contained in a referenced work instruction or pre-existing operational procedures document.

Review

The ITDR plan is a constantly evolving document, and therefore must be subject to change control and review. This should be in line with the review schedule for the corresponding ITSIM plan.

This section of the ITDR plan must define those responsible for the reviews, as well as the conditions under which the review must be undertaken.

ITDR testing

This section outlines the steps required to develop an effective approach to ITDR testing.

Types of test

There are five main approaches to testing an ITDR plan:

- Paper-based testing
- Walkthrough testing
- Component testing
- Parallel testing
- Cutover testing

Each approach is summarised in the following table.

Table 14: ITDR plan test types

Test type	Description
Paper-based Test	A paper-based test collects together all of the available documentation for the system; most importantly, the ITDR plan for the system. An analyst with experience of conducting ITDR will then ascertain from examining the documented processes and interviews with staff, whether all of the necessary provisions exist to meet the recovery requirements for that IT system.
Walkthrough Test	A walkthrough test is a non-technical, real-time test involving a role-play exercise where all relevant stakeholders walk through an ITDR scenario. All resources need to be available and set aside to test a specific scenario; these include business staff, IT staff and accommodation. Where possible it is recommended that the individuals who would be used in a true disaster scenario are used to conduct the test, with the various parties responding as per their role.
Component Testing	Component testing starts to test individual components of processes and technology that will be identified in an ITDR plan. Component testing provides an opportunity to gain confidence that the individual components of the IT system can be restored successfully. This type of testing often takes place before progressing to an end-to-end form of testing.

Test type	Description
Parallel Testing	Parallel testing involves the use of hardware which has been sourced or set aside for the purposes of testing. Essentially, this form of test is operating a full restoration of an IT system in a non-live setting. In this type of testing, the ITDR process is run in parallel alongside the live system, ensuring that the business process can continue to function, while identifying hardware-based, physical and practical limitations of the plan.
Cutover Testing	Cutover testing focuses upon putting a disaster recovery system into a live setting. Therefore this involves the complete dependence on the backup system rather than the primary. It is strongly recommended that all previous types of tests are considered and undertaken and reviewed or not taken with formally agreed reasoning to assure confidence before adopting this approach. Care must also be taken to ensure that the live service is not affected during the setup and execution of this test. As with any live service testing, it will be imperative that appropriate service or maintenance windows are identified and agreed with the business, in order to minimise risk to business operations.

Planning a test

Objectives

The main objectives of testing an ITDR plan are to determine whether:

- IT services can be recovered after an incident;
- IT continuity provisions can minimise the impact to the business and their operations, in response to an incident;
- The ITDR procedures for a return to 'business as usual' operations are validated;
- Additional factors, such as communication, and incident and alert management are sufficiently robust; and
- To allow staff to become familiar with the ITDR plan.

The test results must show:

- Gaps in the level of service compared to the ITDR requirements (see [here](#)).
- Actions to address these gaps must be identified and assigned to responsible staff.
- A consolidated report for management should be compiled, in order to illustrate the results of the tests, along with actions taken to address any issues that arose.
- The process of examining the results against the requirements should identify 'defects' in the Plan documentation and process. These defects must be identified and fed back into the planning documents.

Success criteria

A test can only be declared a success if the following conditions are met:

- The business processes which are covered by the ITDR plan are proven to be recovered to working use at the end of the test period.
- The entire IT system, including data, can be accessed by users within the period of time specified by the agreed RTO limit (see [here](#)).
- Where applicable, users can access the IT system from a necessary site after the failover has been tested.
- The amount of data loss can be specified exactly, and is within the RPO limit.

Note: This is not an exhaustive list, this should be discussed and criteria should be reviewed and agreed with the business group Senior Information Risk Owner (SIRO) in advance.

Review and update

Subsequent review of the test must be undertaken to ensure that all test results are reflected in the ITDR plan. It is recommended that this be undertaken as soon as possible after the test is completed. It is important that any unexpected results arising from the test, which have not been rectified or are still outstanding issues, are document in the ITDR plan including any actions to rectify any defects or issues.

ITDR Incident management

The following table provides a generic set of incident management steps which should be followed when the ITDR plan is invoked. As the ITDR plan sits under an ITSIM plan, it is important to ensure that the steps encapsulated in the ITDR plan aligns to the ITSIM plan.

Table 15: Information management steps

Step	Name	Description
A	Declaring a Disaster	An incident is declared a 'disaster' which requires the ITDR plan to be invoked.
B	Invoking the ITDR plan	The IT Disaster Recovery Team Lead identifies the critical resources required to manage the disaster, and puts forward a communications strategy to ensure that all personnel can co-ordinate actions appropriately.
C	Executing the DR Plan Procedures	The scope and extent of the disaster is assessed and the ITDR plan is executed following the set of recovery procedures set out in the plan.
D	Status Updates	During the recovery process, regular communication points are recommended as part of the ITDR plan to keep the business updated.
E	Incident Resolution	Once the IT system is considered restored to a sufficient level, a final communication to indicate completion should be made to the business. At this point, it is the responsibility of Service Management to declare the system restored.
F	Review Results	After the incident has been closed off the 'lessons learned' from the recovery procedure must be reviewed and addressed. In some cases defects in the procedure or plan may come to light. The aim and objectives of the invocation and requirements must be analysed in light of the information gathered from conducting the execution of the plan. These results will establish if the aims and objectives were met and whether the response to the outage was sufficient.

Training and awareness Introduction

All staff should be subject to training in order to raise an awareness of the ITDR plan and their individual roles within it.

Staff training requirements

The following table defines several categories of staff and outlines the recommended training and awareness requirements.

Table 16: Staff training requirements

Category	Requirements
General staff awareness	<ul style="list-style-type: none"> To know that an ITDR plan exists. To know how they will be impacted by the range of scenarios covered by the ITDR plan. To know what to do in the event of an incident or invocation.

ITDR Representatives	<p>As for general staff, plus:</p> <ul style="list-style-type: none"> • To know the responsibilities of a ITDR representative. • To know how their departments will be impacted by the range of scenarios covered by the ITDR plan. • To ensure their business requirements are communicated and accommodated within the ITDR plan.
Incident management team	<p>As for general staff, plus:</p> <ul style="list-style-type: none"> • To understand the requirements of the ITSIM and ITDR plans. • To know their roles in the ITSIM and ITDR plans.
ITDR recovery staff	<p>As for general staff, plus:</p> <ul style="list-style-type: none"> • To understand the IT recovery priorities, plans and processes. • To know their roles in the recovery process.

IT Disaster Recovery Plan - Template

IT Disaster Recovery Plan	
Overview	
MoJ Business Group	[Enter the name of the MoJ Business Group.]
System Description and Scope	[This section must describe the scope of the ITDR plan. Diagrams may prove useful where there is a complex interaction between systems and business processes covered by this plan. See here for further details]
Site List	[See here]
Definition of a 'Disaster'	[See here]
Authorised to invoke the plan	[See here]
Staff notification	[Include details of how staff and IT suppliers are notified that ITDR plan has been invoked, see here]
Roles and responsibilities	[For each role outlined in the IT Security – IT Disaster Recovery Policy , a named individual must be entered here.]
Dependencies	
Internal Dependencies	<p>[Include each dependency, recommend the following format:</p> <ul style="list-style-type: none"> • Dependency ID; • Description; • Impact (time, resource, effort). <p>See here]</p>
External Dependencies	<p>[Include each dependency, recommend the following format:</p> <ul style="list-style-type: none"> • Dependency ID; • Description; • Impact (time, resource, effort). <p>See here]</p>

Recovery Procedures	
Primary Functions	<p>[Include each primary function, recommend the following format:</p> <ul style="list-style-type: none"> • Function ID; • Function; • Description. <p>See here]</p>
Secondary Functions	<p>[Include each primary function, recommend the following format:</p> <ul style="list-style-type: none"> • Function ID; • Function; • Description. <p>See here]</p>
Step [X]	<p>[For each step outlined in ITDR Incident Management, list the corresponding recovery procedures in this section; see Recovery procedures for further details.]</p>
Recovery Actions and Review	
Recovery Actions	[See here]
Review	[See here]
Plan Approval	
Business Group SIRO	[Enter the name of the Business Group SIRO] [DATE OF APPROVAL]
IT Security Officer	[Enter the name of the IT Security Officer (ITSO)] [DATE OF APPROVAL]

Completing this plan can form part of the Accreditation process and must be included and maintained as part of the relevant RMADS.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

IT Disaster Recovery Policy

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).

- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF (Security Policy Framework), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Introduction

IT disaster recovery is a crucial element of the Ministry of Justice (MoJ) overall business continuity plans.

Definition of a disaster event

An IT 'disaster' event is defined (for the purposes of this policy) as any incident which results in an actual or potential loss of availability or integrity of an IT system or a business process supported by an IT system. That event would result in a system being unable to operate in an acceptable manner to the business.

POL.ITDR.001:

Each IT system or IT domain **must have** (or be explicitly covered by) an IT Disaster Recovery Plan which implements this policy.

A template Disaster Recovery Plan is available in the [IT Security - IT Disaster Recovery Plan and Process Guide](#).

Note: In general, where an IT system (or IT domain) has an IT Security Incident Management Plan, there should be a corresponding IT Disaster Recovery Plan.

Roles and responsibilities

An effective IT Disaster Recovery Plan requires the clear allocation of responsibility. Defining the roles and responsibilities of those involved with IT disaster recovery is also an important part of the overall recovery effort.

Note - The roles outlined in this policy are aligned with and support the [IT Security – Incident Management Policy](#).

POL.ITDR.002:

Each IT Disaster Recovery Plan **must outline** how the roles and responsibilities in this policy are fulfilled. This includes recording named individuals (and associated contact details) for each role.

POL.ITDR.003:

All staff **must be** made aware of the relevant IT Disaster Recovery Plan/s and where applicable, their role within it.

Note: Further guidance on training and awareness can be found in [IT Security – Disaster Recovery Plan and Process Guide](#).

Senior Information Risk Owner (SIRO)

A SIRO acts as an advocate for managing risk for Business Continuity and IT Disaster recovery.

Departmental Security Officer (DSO)

The Departmental Security Officer is responsible to the Permanent Secretary for:

- Assurance of the management and completion of the Department's Business Continuity Plans.
- The MoJ's assessment of the National Threat Assessment in the context of business continuity planning.
- Setting direction for the MoJ's approach to Business Continuity and agreeing the maintenance and creation of plans across the business.
- The DSO has a MoJ wide view of Business Continuity Plans and is able to report on the maturity of these plans. This IT Disaster Recovery Policy supports these Business Continuity Plans.

Information Asset Owner (IAO)

The IAO's role in IT Disaster Recovery Planning is to understand the risks to the availability of their information assets in the event of a disaster and to ensure that they understand and can execute the relevant IT Disaster Recovery Plan.

Business Continuity Team Leader (BCTL)

The Business Continuity Team Leader is appointed to monitor and manage the MoJ's Business Continuity Plans.

IT Disaster Recovery Team Leader (ITDRTL)

The ITDRTL is responsible for the MoJ's IT Disaster Recovery Plans. This role works with the Business Continuity Team Leader to ensure that MoJ IT systems support MoJ's critical business processes.

The IT Disaster Recovery team leader is responsible for:

- Identifying where the IT Disaster Recovery Plan will need to be updated in line with changes to the MoJ Business Continuity Plan;
- Administering IT disaster recovery testing in accordance with agreed schedules;
- Providing regular reports of the IT disaster recovery status of the MoJ;
- Coordinating regular reviews and updates of IT Disaster Recovery Plans.

IT Security Officer (ITSO)

This role is responsible for identifying and managing Corporate-level IT disaster recovery risks, and maintaining the Corporate IT disaster recovery risk register.

System Accreditor

The role of an Accreditor is to act as an impartial assessor of the risks to information systems. Their function is to assure that systems are sufficiently secure to be placed into operational service. They accredit systems on behalf of the SIRO. There is also a role for Head of Accreditation who lead the accreditation team, and may accept the risk on their team's behalf.

Planning

The planning and generation of an IT Disaster Recovery Plan as described in the IT Disaster Recovery Guide support decisions and subsequent courses of action that reduce the consequences of any disaster event.

It is suggested that a Business Impact Assessment (BIA) is undertaken in order to identify the disaster recovery requirements of all the assets or business processes supported by a particular IT system:

In particular the BIA should contain:

Recovery Time Objective (RTO) – The time in which the business requires IT services to be restored. I.e. The time between a disaster event occurring and full IT system services being restored.

Recovery Point Objective (RPO) – The point in time in which an IT system's data asset/s can be rolled back to where the business can tolerate that period of data loss. I.e. How much historic data in the live IT system can the business tolerate losing in a disaster event.

POL.ITDR.004:

The IT Disaster Recovery Plan for an IT system or IT domain **must be** based on a Business Impact Assessment (BIA), Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

POL.ITDR.005:

Any disaster recovery measure outlined in an IT Disaster Recovery Plan **must ensure** the IT system (or IT domain) can recover from a disaster event within the stated Recovery Time Objective (RTO) as recorded in a BIA.

POL.ITDR.006:

Any disaster recovery measure outlined in an IT Disaster Recovery Plan **must ensure** the IT system (or IT domain) can recover from a disaster event within the stated Recovery Point Objective (RPO) as recorded in a BIA.

Testing and readiness review

An IT system (or IT domain) IT Disaster Recovery Plan needs to be tested regularly to ensure the plan remains fit for purpose and those involved in executing the plan remain familiar with the procedures outlined in it. This increases the MoJ's preparedness in the event of a disaster.

POL.ITDR.007:

Prior to the commencement of live operations, an IT system **must have** its IT Disaster Recovery Plan tested where the outcome is supplied to the system Accreditor to form part of the accreditation decision making process.

POL.ITDR.008:

All IT Disaster Recovery Plans (whether for an IT system or IT domain) **must be** tested annually or when a significant change occurs to that IT system. The testing schedule **must be** outlined in the IT Disaster Recovery Plan.

POL.ITDR.009:

After each test, a review of the IT Disaster Recovery Plan **must be** conducted and updated where appropriate based on the test finding, outcomes or defects identified.

Invocation and escalation

The invocation of an IT Disaster Recovery Plan is closely aligned to corresponding IT Incident Management Plan.

In general, an incident categorised as High impact (see [here](#) for more details) may in turn constitute a disaster event. Each individual IT Disaster Recovery Plan needs to outline the particular circumstances in which the plan is invoked.

POL.ITDR.010:

Each IT Disaster Recovery Plan **must define** the situations and circumstances under which the Plan is to be invoked.

Reporting and alerting

In general, the reporting and alerting structure of an IT Disaster Recovery Plan should align with that of the corresponding IT Security Incident Management Plan. However, depending on the nature of the disaster event, other stakeholders may need to be informed both internally and externally to the MoJ. This is where the MoJ Business Continuity Plan interacts with any individual IT Disaster Recovery Plan for an IT system or IT domain.

POL.ITDR.011:

Each IT Disaster Recovery Plan **must define** a reporting and alerting structure which aligns with the relevant IT Security Incident Management Plan and Business Continuity Plan.

Responsibility for business continuity resides with [MoJ Corporate Security and Business Continuity Branch](#) where further details can be obtained.

Recovery and review

Recovering from a disaster event is generally about the speed of restoring services to normal; however it is important to ensure that security vulnerabilities are not introduced (or re-introduced) during the restoration process and that any lessons learnt are fed back to appropriate stakeholders.

POL.ITDR.012:

Each IT Disaster Recovery Plan **must contain** a pre-defined and tested process and/or set of procedures for restoring the IT systems and services which have been disrupted or disabled during a disaster event.

POL.ITDR.013:

After each disaster incident, the following **must be** reviewed and any recommendations considered:

- The IT Disaster Recovery Plan to consider lessons learnt and any improvements;
- The design of the IT system and controls implements to reduce the impact of a disaster event or aid the restoration process;
- Any changes to the relevant IT Security Incident Management Plan.

Note – The [IT Security – IT Incident Management Policy](#) contains the provision for an incident report to be compiled. Any recovery and review work should be done in conjunction with the production of the overall incident report.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

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 Ministry of Justice (MoJ) 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 MoJ 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 Ministry of Justice (MoJ) 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 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 Ministry of Justice (MoJ) 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) millimeters squared with a maximum strip width of 6 (six) millimeters

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 Ministry of Justice (MoJ) 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) millimeters squared with a maximum strip width of 6 (six) millimeters.

Instruction & Confirmation Letter

The current draft of a templated Ministry of Justice (MoJ) data destruction letter, that may be issued by the MoJ to a supplier. The letter describes required actions and information, followed by a responsive declaration from the supplier.

Letter issued by MoJ

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 Ministry of Justice (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 Ministry of Justice, 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 OFFICIAL under the [UK HMG Government Security Classifications Policy](#) (including sensitive personal data or sensitive commercial data within the same).

Data Lifecycle

The Ministry of Justice 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 Ministry of Justice 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 Ministry of Justice 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 MoJ 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 MoJ 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 Ministry of Justice data is inaccessible by any reasonable commercial and resourced means (such as commercially available data recovery services).

Supplier declaration

Please sign the declaration below and return this letter to the Ministry of Justice, keeping a copy for your own records. Should you have any queries, please contact the Ministry of Justice CISO via security@digital.justice.gov.uk

Return electronically. Electronic signatures or otherwise positive confirmation are accepted.

Chief Information Security Officer Ministry of Justice 102 Petty France Westminster, London SW1H 9AJ
security@digital.justice.gov.uk

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 Ministry of Justice (MoJ)
- 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

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** MoJ technology projects and business activities.

While GDPR applies only to personal information, all MoJ projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow MoJ 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 Security & Privacy Lifecycle Expectations

Below are a series of data security and privacy expectations of Ministry of Justice (MoJ) 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 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

Below are a series of common area guides from Ministry of Justice (MoJ) 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 MoJ 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 MoJ 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 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 Ministry of Justice (MoJ) 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 MoJ.

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 below.

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

Legacy information

Note: This document is Legacy IA Policy material. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact CyberConsultancy@digital.justice.gov.uk.

Note: This document might refer to several organisations, information sources, or terms that have been replaced or updated, as follows:

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).

- CONFIDENTIAL, an older information classification marking, see [Information Classification and Handling Policy](#).
- CPNI ([Centre for the Protection of the National Infrastructure](#)), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the [Government Functional Standard - GovS 007: Security](#).
- IS2 (HMG Infosec Standard 2 Information Risk Management), see the [Government Functional Standard - GovS 007: Security](#).
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the [Government Functional Standard - GovS 007: Security](#).
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the [Government Functional Standard - GovS 007: Security](#).
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- RESTRICTED, an older information classification marking, see [Information Classification and Handling Policy](#).
- SPF ([Security Policy Framework](#)), see the [Government Functional Standard - GovS 007: Security](#), contact security@justice.gov.uk.

Summary

Accreditation is the formal, independent assessment of an IT system or service against its Information Assurance (IA) requirements.

The Ministry of Justice (MoJ) [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 MoJ business or MoJ customers.

Risk Assessment Process

Risk Reviews

Information and the supporting processes, systems and networks are important and valuable Ministry of Justice (MoJ) assets. They are central to enabling the MoJ 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 MoJ's ability to provide efficient and effective services, maintain compliance with legal and regulatory requirements, and maintain its and the Government's reputation.

The MoJ 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 MoJ's dependence on its information systems and services means that there is always a possibility of technology-enabled security threats. Connections between the MoJ'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 MoJ identify its information security requirements. There are three main sources of these requirements.

- The legal, statutory, regulatory and contractual requirements that the MoJ, its partners, contractors and service providers have to satisfy.

- The principles, objectives and requirements for information processing that the MoJ and Government have developed to support their operations, for example the protective marking system and government baseline security standards.
- Assessed risks to the MoJ. 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 MoJ system with other systems. This might limit the usefulness of the MoJ 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 MoJ 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 MoJ standards.
- Assisting with mandatory Government risk assessments.
- Advice on compliance checking.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.