MOJ Cyber Security Guidance

Contents

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: 12 August 2020.

This offline version of the guidance is available as a PDF file for convenience. However, it is time-limited: it is not valid after 12 September 2020. For the latest, current version of the guidance, see here.

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 6.12 Cyber security and 6.13 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.

Taxonomy

MoJ has developed their cyber and technical security taxonomy as follows:

Level 1	Level 2
Cyber	Access Control
	Asset Management
	Cryptography
	Operational Security
Technical	Principles
	Data and Information
	Incident Management
	Software Development

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

Document List

Level 1	Level 2	Documents	Target Audience
Cyber	Access Control	Access Control Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
		Accessing MOJ IT Systems From Abroad	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
	Asset Management	General User Video and Messaging Apps Guidance	All users
		Guidance for using Open Internet Tools	All users
		Security Guidance for Using a Personal Device	All users
		Remote Working	All users
	Cryptography	Cryptography	Technical Architect, DevOps, IT Service Manager, Software Developer
	Operational Security	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

Level 1	Level 2	Documents	Target Audience
		Malware Protection Guide: Defensive Layer 3	Technical Architect, DevOps, IT Service Manager, Software Developer
Technical	Principles	Data Security and Privacy	All users
		IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER	All users
		Maintained by Default	Technical Architect, DevOps, IT Service Manager, Software Developer
		Secure by Default	Technical Architect, DevOps, IT Service Manager, Software Developer
		Security Log Collection	Technical Architect, DevOps, IT Service Manager, Software Developer
		Shared Responsibility Models	Technical Architect, DevOps, IT Service Manager, Software Developer

Standards

Authentication, Authorisation & Accounting

- Accounting
- Authentication
- Authorisation

General standards

- Baseline for Amazon Web Services accounts
- Data Destruction
- Data Security & Privacy
- Management access
- Networks are just bearers
- Password Managers
- Secrets management
- Vulnerability scanning

Security Log Collection

- Commercial off-the-shelf applications
- Custom Applications
- Enterprise IT - Infrastructure

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

Guides

General guides

- Automated certificate renewal
- Data Security & Privacy Lifecycle Expectations
- Data Security & Privacy Triage Standards
- Defensive domain registrations
- Online identifiers in security logging & monitoring
- Personnel security clearances
- Standards Assurance Tables
- Cyber Security Consultancy Team: asking for help

Active Cyber Defence

- Mail Check
- Public Sector DNS
- Web Check

Product specific guides

- Using LastPass Enterprise

Suppliers to MOJ

- Assessing Suppliers
- Contracts
- Data Destruction
  - Data Destruction Instruction and Confirmation Letter
  - Data Destruction Contract Clauses - Definitions
  - Data Destruction Contract Clauses - Short Format
  - Data Destruction Contract Clauses - Long Format
  - Data Destruction Contract Clauses - Long Format (Appendix)
- Security Aspect Letters
- Supplier Corporate IT

Mythbusting

- Criminal Justice Secure Mail (CJSM)
- Data Sovereignty
- Internet v. PSN
- IP DNS Diagram Handling
- Multiple Back-to-back Consecutive Firewalls
- `OFFICIAL` and `OFFICIAL-SENSITIVE`

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.

Government Functional Standard - GovS 007: Security

Getting in touch

Contact information

- Email
- Reporting an incident

Vulnerability Disclosure

- Vulnerability Disclosure Policy
- Implementing `security.txt`

Cyber

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

Contact the Cyber Assistance Team for access control advice – CyberConsultancy@digital.justice.gov.uk

Accessing MOJ IT Systems From Abroad

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 abroad, and to do this using their MOJ equipment. But before you travel, consider:

- Do you need to take MOJ IT equipment abroad 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 abroad 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, France, Germany, 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.
    - 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.
    - Reason for maintaining access while abroad.
    - The MOJ data, applications, or services you expect to access during your trip.
    - Who you are travelling with.
2. Contact MOJ Security, and provide them with the information collected in the previous step. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
3. 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 abroad 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 abroad 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.
4. Fill in the overseas travel request form.
5. Send the completed form to MOJ Security, including the answers obtained from the earlier parts of this process.
6. Your request is considered, and an answer provided, as quickly as possible.
7. When you have received all the approvals, send a copy of your request and the approvals to Operational Security.
8. When Operational Security have acknowledged receipt of the request and approvals, the formal process is complete.
9. Check if you need to do anything to prepare for International Roaming .
10. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.
11. 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 abroad.

By default, MOJ equipment is not enabled for use abroad. Before travelling, contact the MOJ Phone and Mobile Devices team. Ask them to enable International Roaming, 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 abroad

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 Corporate Security Branch as soon as possible.

For any emergency outside normal UK business hours, contact the Duty Security Officer .

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 abroad
- Travelling abroad - business or personal
- 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`

MOJ Duty Security Officer

- Tel: +44 (0)20 3334 5577
- Email: dutysecurityofficer@justice.gov.uk

MOJ Phone and Mobile Devices

- Email: MoJ_Phone_and_Mobi@justice.gov.uk

MOJ Security

- Email: security@Justice.gov.uk

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 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

Contact the Cyber Assistance Team for advice - 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.

Minimum user clearance requirements

Most of the MoJ's IT systems are able to process OFFICIAL information. Therefore all roles in the MoJ require staff to attain Baseline Personnel Security Standard (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.

Contact details

Contact the Cyber Assistance Team for advice - 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 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

Contact the Cyber Assistance Team for advice – 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 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
✓ Ensure that privileged users only use their system administrator account when elevated privileges are required. Their general user account should be used for all other work activities.
✓ Ensure that management or administrative access is limited to users who have been suitably authenticated and have been authorised to perform the specific action. Only those with a genuine business need should have an administrative account, however there should be a sufficient number of administrators that there is not a single point of failure due to absence or administrators leaving the MoJ. This should be enforced through the principle of least privilege.

DO
✓ 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.
✓ Ensure that MFA is mandated for a privileged user to conduct important or privileged actions such as changing fundamental configurations including changing registered email addresses or adding another administrator.
✓ Ensure that MFA is used as a validation step, to confirm actions requested by users, such as a MFA re-prompt when attempting to delete or modify data.
✓ Ensure that default passwords are managed as described in the Password Manager guidance.

DON'T
✖ Allow privileged users to use their privileged accounts for high-risk functions. These include reading emails, web browsing, using an 'administrator' login on an end-user device (such as a mobile device), or logging into a server as 'root'.
✖ Leave default or factory set passwords for any accounts but particularly for privileged system accounts, social media accounts and infrastructure.
✖ Allow a user to have a privileged account, unless they are a service provider and require a privileged account for that specific service.

For more information or help with Privileged Accounts, contact the Cyber Assistance Team.

Contact details

Contact the Cyber Assistance Team for advice – CyberConsultancy@digital.justice.gov.uk

Asset Management

General User Video and Messaging Apps Guidance

Overview

When working from home, you still need to communicate with 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 (information on a whiteboard 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:

- 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 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 lets 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 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 Hangouts	Communication tool: Video and/or voice	MOJ use approved	Digital Service Desk controlled Mac - Self	Internal/External
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
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

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 a tool be approved for use

Refer to the Guidance for using Open Internet Tools for the process to follow when wanting to add a new tool to the list.

Other information
Government policy and guidance

GDS Social Media Playbook

NCSC

Video conferencing services: using them securely

Secure communications principles

Using third-party applications

Last updated: April 22nd, 2020.

Guidance for using Open Internet Tools

This information applies to all staff and contractors who work for the 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:

data.compliance@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.

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

Last updated: April 16th, 2020.

Security Guidance for Using a Personal Device

Summary

Not everyone has access to an MOJ device which can be used remotely. In these extraordinary times, exceptional provision is being developed for you to use your own devices for work purposes.

Until that provision is in place, you must not use a personal device for work purposes.

Guidance

- If you have an MOJ-issued device, you must use that.
- You may not use Office 365 tools (email, calendar, Word, Excel, Powerpoint, etc.) for work purposes on a personal device (desktop, laptop, tablet or phone). This applies to web browser and installed client applications.
- Do not send MOJ information to your personal email account, or use personal accounts for work purposes.
- Do not store work files or information on a personal device (desktop, laptop, tablet or phone).
- Some teams within the MOJ, such as groups within Digital & Technology, and HMCTS, might already have prior permission to use personal devices for aspects of software and service development work. This permission continues, but is being reviewed on an on-going basis.

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

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

Last updated: April 24th, 2020.

Remote Working

Key points

- Be professional, and help keep 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 Ministry of Justice (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 - 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@digital.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

If unsure, contact your Line Manager.

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

Last updated: April 24th, 2020.

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 again physical interception (such as theft) threats.

Given the autonomous nature of server provisioning and management, it may not always be technically practical to implement such encryption (particularly when a physical server restart would require human intervention with a decryption passphrase).

In general, at-rest encryption **must** always be proportionally considered, even if documented as not reasonable to implement.

Cloud-based

Vendor managed at-rest encryption **must** be enabled by default unless there is a good reason not to (for example, licensing restrictions or severe performance issues).

Vendor managed at-rest encryption (the vendor will typically managed encryption keys, on-the-fly encryption and decryption) is preferred, shifting management to the vendor under the shared responsibility model.

In some circumstances, it *may* be reasonable to self-managed encryption keys but should be relatively rare.

End-User Device based

Native at-rest encryption such as Apple macOS FileVault, Apple APFS or Microsoft Windows BitLocker **must** be used, preferably controlled by central enterprise device management and key management systems.

The NCSC have published end-user device guidance that discusses such technologies.

Portable storage

Portable storage such as CDs, DVDs and USB sticks can be safely used to move data. As usual, data must be adequately protected based on the overall governance and information risk requirements.

While the following certifications are preferred, they may not be required based on the data and data methods being stored or transported.

- FIPS 140-2 Level 3
- NCSC CPA
- NATO Restricted Level Certified

The 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 utilised at-rest encryption to protect on-board data (and subsequent configured accounts) while the device is 'locked' or powered down.

The NCSC End-user Device Security Collection discusses per-platform configuration advice.

Summarily, native at-rest encryption must be enabled with a suitable and proportional decryption code (typically, a password) and hardware-backed cryptography is preferred.

Hashing

Data that should be kept confidential or is worthwhile to otherwise obfuscate should be hashed. This **must** apply where authentication credentials are stored, such as a password.

The published MOJ Password Standard has a section on hashing as part of password storage.

Operational Security

Malware Protection Guide - Overview

Introduction

This guide introduces the information which explains your responsibilities in helping the 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 by email: CyberConsultancy@digital.justice.gov.uk
- Contact the Technology Service Desk to report suspected malware:Telephone: 0800 917 5148.

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 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

Do
✓ 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.

Do
✓ Avoid the need for removable media by using existing approved online collaboration services where possible, for example Office 365. Where removable media has to be used, it must be scanned by approved Anti-virus before and during use.
✓ All web traffic must be routed through a proxy which logs and monitors internet access. This reduces the chance of malicious sites infecting end user devices. The proxy is configured in agreement with the security team. Email must also be routed through email scanning services. Direct Internet access should only be configured for update services, and by exception only.
✓ Allow the installation of applications only from approved stores.
✓ Systems must be able to be updated and must be kept up-to-date with OS and application upgrades and patches. Where possible, software updates should be configured to update automatically. 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.

Don't
✖ 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.
✖ 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 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.

Don't
✖ 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 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 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), which 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.

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 the 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

Technical

Principles

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 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** technology projects.

While GDPR applies only to personal information, all MOJ projects must have excellent data security and privacy properties. 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.

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The 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.

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 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:

- 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. 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 fundementally 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 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

Security Log Collection

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).

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 and are logged, but that you need to provide . 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.

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.

Shared Responsibility Models

The 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.

Standards

Authentication, Authorisation & Accounting

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.

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.

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 integation 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 fundemental 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

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

Examples include those with high privileges on a 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 priviledge 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

General Standards

Anti-malware

This document is retained for Archive purposes. Current guidance regarding Malware is available here.

The base principle

All systems **must** be protected against commodity malware threats through, but not limited to, known malware through signature-based checks.

Any issues found must be proportionally considered for remediation (in general, this is file deletion or escalation for review after quarantine) prior to releasing any files or data for consumption.

File-based malware

Uploaded files (such as an attachment uploaded to a web application) and stored files (any electronic file stored) must always be scanned for malware.

moj-clamav-daemon and moj-clamav-rest may be useful for scanning uploaded files through web applications.

clamAV is a popular open source antivirus engine for detecting trojans, viruses, malware & other malicious threats.

Ransomware

Some malware encrypt or obfuscate data and attempt to extort payment from the victim(s) in order for the decryption to take place. Such malware typically attempts to influence any file available, including remote storage.

Techniques must be in place to isolate and ensure backup regimes are adequately defended against ransomware to avoid backup files being modified by such malware.

Network propagation

Some malware propagate by scanning the visibile networking space for other hosts to turn into victims. Network-level segregation and defences must be in place to limit lateral infection movement.

Baseline for Amazon Web Services accounts

The 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: cybersecurity@digital.justice.gov.uk

Baseline
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 & Access Management

Enforce Identity & 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 user 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.

SecurityHub

SecurityHub 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
SecurityHub is enabled on all accounts, in all regions, all of the time.	Alerts fire when SecurityHub is not enabled in a MOJ AWS account.	SecurityHub is automatically re-enabled.

Implementation

Various AWS account baseline templates have been developed and published for use.

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 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.

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 diagnositic data collection

It should be exceptional to directly administer a server/node when adequate diagnositic 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 privledges (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 priviledged 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*.

Networks are just bearers

The base principle

IP networks **must** be considered commodity bearers for technical connectivity to faciliate 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

Password Managers

Overview

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?".

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 MOJ's 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.

Vulnerability scanning

The base principle

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.

Application vulnerabilities

Applications **must** be scanned programmatically during development and build pipelines (prior to the final release to production) for vulnerabilities.

Tools such as OWASP ZAP may be useful.

Security Log Collection

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 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 G-Suite (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:

- a: account creation
- b: account lockout
- c: account reinstatement
- d: account authentication failures
- e: account authentication successes after 1 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 (for example, role delegation through AWS IAM)
- k: multi-factor authentication state, such as:
    - 1: enabled
    - 2: disabled
    - 3: reset/rotation
    - 4: 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.

- a: user/group identifier(s)
- b: action/query
- c: response size
- d: 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.

- a: data store identifier(s)
- b: credential identifier(s)
- c: query
- d: query response size
- e: query response time

2. Unauthenticated user activity events

Log Collection Principle(s): 6

Where unauthenticated users interact with applications (for example, a MOJ G-Suite document available on the general Internet through relaxed access controls), associated audit information must be created.

- a: end-client identifier(s)
- b: query metadata
  - 1: destination identifier (such as target hostname, TCP/UDP port and/or full URI)
  - 2: query type (for example, `HTTP GET` or `HTTP POST`)
  - 3: query size
- c: response size
- d: 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 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 G-Suite (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:

- a: account creation
- b: account lockout
- c: account reinstatement

- d: account authentication failures
- e: account authentication successes after 1 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 (for example, role delegation through AWS IAM)
- k: multi-factor authentication state, such as:
  - 1: enabled
  - 2: disabled
  - 3: reset/rotation
  - 4: 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.

- a: user/group identifier(s)
- b: action/query
- c: response size
- d: 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.

- a: end-client identifier(s)
- b: query metadata
  - 1: destination identifier (such as target hostname, TCP/UDP port and/or full URI)
  - 2: query type (for example, `HTTP GET` or `HTTP POST`)
  - 3: query size
- c: response size
- d: 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.

- a: source identifier(s)
  - 1: user(s)
  - 2: repository
- b: activity events
  - 1: resource creation
  - 2: resource destruction
  - 3: 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.

- a: data store identifier(s)
- b: credential identifier(s)
- c: query
- d: query response size
- e: query response time

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:

- a: account creation
- b: account lockout
- c: account reinstatement
- d: account authentication failures
- e, account authentication successes after 1 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

2. Productivity Suite security logs

Log Collection Principle(s): 1, 2, 3, 6

Productivity suites (such as Google G-Suite 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.

- a: client IP address
- b: query
- c: query response content including
  - 1: returned record(s) or NXDOMAIN
  - 2: authoritative nameserver
- d: query response code
- e: 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.

- a: authenticated user name
- b: client IP address
- c: HTTP method (for example, `CONNECT GET`)
- d: full destination/target URL
- e: connection return status code (for example, 200 or 403)
- f: 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:

- a: detect permission changes and the user who changed such
- b: detect all file/folder changes and the user who changed such
- c: 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.

- a:

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:

- a: successful client DHCP requests, including:
  - 1: Requesting client MAC address
  - 2: DHCP scope identifier
  - 3: IP address leased
  - 4: IP address lease duration

- b: unsuccessful client DHCP requests, including:
  - 1: Requesting client MAC address
  - 2: 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.

- a: success or unsuccess status
- b: user/certificate identifier
- c: client IP address
- d: 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.

- a: client IP address
- b: firewall/router identifier
- 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. Internal DNS namespace zone content

Log Collection Principle(s): 4

Internal domain name spaces must ultimate forward, in an RFC5936 (DNS Zone Transfer Protocol (AXFR) compatible format including all information described in the RFC.

3. DHCP scopes (and the functional segmentation of each)

Log Collection Principle(s): 5

Machine-readable DHCP scope exports (and surrounding metadata/description of the purpose of each scope) must be created and forwarded.

4. Endpoint protection security logs

Log Collection Principle(s): 6

Security log data (as defined by the vendor) must be created and forwarded.

5. Mobile device enrollment activity

Log Collection Principle(s): 1, 2, 3, 6

Where a mobile device management solution is used and end-user devices register/enrol and de-register/de-enrol with it, enrollment data should be created in and forwarded.

- a: enrolment or un-enrolment event type
- b: end-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
- c: 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 defenisve cyber security, such as detecting breaches.

Baseline Maturity Tier

1. Device power events

Log Collection Principle(s): 1

Devices must create and forward local power events.

- a: power on (including good or bad state)
- b: power off (including if restart)
- c: disk encryption state

2. User identification activity

Log Collection Principle(s): 1, 2

Devices must create and forward local Authentication and Authorisation events.

These event types must be logged and forward:

- a: account creation
- b: account lockout
- c: account unlock
- d: account authentication failures
- e: account authentication successes after 3 or more failures
- f: account password changes
- g, group membership addition / deletion (in particular, any group that gives admin access)
- h: group creation
- i: privilege modification for users (changes to ACL's, granting of new roles in RBAC models)
- j: privilege escalation events (use of sudo, UAC)
- k: multi-factor authentication state, such as:
  - 1: enabled
  - 2: disabled
  - 3: reset/rotation
  - 4: recovery method used

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded, even where they are captively routed through central enterprise IT DNS services that forward comparable log data.

- a: device IP addresses (local and public, if known/applicable)
- b: VLAN tag for associated network interface (if known)
- d: query
- e: query response content including
  - 1: returned record(s) or NXDOMAIN
  - 2: authoritative nameserver
- e: query response code

4. Security-related operating system event data

Log Collection Principle(s): 6

Any additional security-related logs, as defined by NCSC's Logging Made Easy template, from all end-user devices operating a Microsoft Windows operating system must be created and forwarded.

Comparable events from other operating systems (for example, Apple macOS or QubesOS) to that described by NCSC's Logging Made Easy template must also be created and forwarded.

5. Security-related software event logs

Log Collection Principle(s): 6

Security-related logs from any local endpoint protection software (for example, anti-virus) should be forwarded.

- a: detection information
  - 1: process/binaries
  - 2: detection criteria (for example, malware type)
- b: reaction information (for example, quarantine)
- c: 'last scan' information
- d: signature information

6. Network information

Log Collection Principle(s): 5

Devices must create and forward sufficient data to record the network posture around the device.

- a: IP address of DHCP server
- b: IP address leased
- c: IP address subnet leased
- d: IP address lease duration
- e: Network interface identifier
- f: DHCP response instructions, for example:
  - 1: DNS servers
  - 2: Proxy servers

7. VPN dial-up activity

Log Collection Principle(s): 5

Where dial-up VPN is in use, connection-related log data must be created and forwarded.

- a: success or unsuccess status
- b: VPN concentrator domain name and IP address
- c: user/certificate identifier(s) used
- d: network interface identifier

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded.

- a: client IP address
- b: network interface identifier(s)
- c: request response code
- d: request content, including:
  - 1: IP protocol (for example, ICMP)
  - 2: destination/target port
  - 3: destination/target IP address
  - 4: destination/target hostname address (if reverse lookup performed)

2. Command/executable runtime information

Log Collection Principle(s): 6

Log data to reflect the launching and subsequent processing activity stemming from user, or user profile, triggered commands/executables.

- a: user identifier(s)
- b: device identifier(s)
- c: command executed
- d: executable launched

3. Configuration information

Log Collection Principle(s): 6

Devices must create and forward sufficient data to record the changing state of device configurations.

- a: profile or GPO changes
- b: conflict detection

Hosting Platforms

We have developed a series of logging requirements for hosting platforms, such as virtualised and/or containered compute with associated supporting services such as database and queuing services at different maturity tiers in order to support defenisve 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 G-Suite (acting as an identity provider)
- Local user stores within operating systems

These event types must be logged and forward:

- a: account creation
- b: account lockout
- c: account reinstatement
- d: account authentication failures
- e: account authentication successes after 1 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 (for example, role delegation through AWS IAM)

- k: multi-factor authentication state, such as:
  - 1: enabled
  - 2: disabled
  - 3: reset/rotation
  - 4: 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.

- a: SSH keypair generation/revocation, including:
  - 1: public key
  - 2: keypair ‘friendly name’ / identifier
- b: account login attempts
  - 1: public key
  - 2: username

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded.

- a: client IP address
- b: query
- c: query response content including
  - 1: returned record(s) or NXDOMAIN
  - 2: authoritative nameserver
- d: query response code
- e: 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.

- a: authenticated user name (if applicable)
- b: client identifiers:
  - 1: IP address
  - 2: reverse lookup client name (if applicable)
- c: HTTP method (for example, CONNECT GET)
- d: Where available, full destination/target URL or SNI value
- e: connection return status code (for example, 200 or 403)
- f: 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.

- a: virtual machine creation (including templates)
  - 1: identifier(s)
  - 2: operating system image information
- b: virtual machine ‘power’ events
  - 1: identifier(s)
  - 2: ‘power’ on
  - 3: ‘power’ off (including restart flag)
- c: virtual machine deletion
  - 1: identifier(s)
- d: virtual machine resource modification events:
  - 1: CPU addition/removal
  - 2: RAM addition/removal
  - 3: Networking additional/removal
  - 4: 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.

- a: resource creation (including templates)
  - 1: identifier(s)
  - 2: resource type
  - 3: operating system image information (if applicable)
- b: container ‘power’ events
  - 1: identifier(s)
  - 2: ‘power’ on
  - 3: ‘power’ off (including restart flag)
- c: resource deletion
  - 1: identifier(s)
- e: resource modification events:
  - 1: 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:

- a: successful client DHCP requests, including:
  - 1: Requesting client MAC address
  - 2: DHCP scope identifier
  - 3: IP address leased
  - 4: IP address lease duration
- b: unsuccessful client DHCP requests, including:
  - 1: Requesting client MAC address
  - 2: 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.

- a: client IP address
- b: firewall/router identifier
- 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. Internal DNS namespace zone content

Log Collection Principle(s): 4

Internal domain name spaces must ultimate forward, in an RFC5936 (DNS Zone Transfer Protocol (AXFR) compatible format including all information described in the RFC.

3. DHCP scopes (and the functional segmentation of each)

Log Collection Principle(s): 5

Machine-readable DHCP scope exports (and surrounding metadata/description of the purpose of each scope) must be created and forwarded.

4. Endpoint protection security logs

Log Collection Principle(s): 6

Security log data (as defined by the vendor) must be created and forwarded.

5. Security-related logs for all Windows-based end-user devices

Log Collection Principle(s): 6

Security-related logs, as defined by NCSC's Logging Made Easy template, from all end-user devices operating a Microsoft Windows operating system must be created and forwarded.

6. Mobile device enrollment activity

Log Collection Principle(s): 1, 2, 3, 6

Where a mobile device management solution is used and end-user devices register/enrol and de-register/de-enrol with it, enrollment data should be created in and forwarded.

- a: enrolment or un-enrolment event type
- b: end-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
- c: 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.

- a: success or unsuccess status
- b: user/certificate identifier
- c: client IP address
- d: concentrator identifier

8. Pipeline events

Log Collection Principle(s): 1, 2, 3, 6

Continuous integration and continuous deployment pipelines obey instructions to manage hosting environments and are a privileged position to oversee all tenant resources, they must be highly auditable to clarify activity and attribute the same.

- a: source identifier(s)
  - 1: user(s)
  - 2: repository
- b: activity events
  - 1: resource creation
  - 2: 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

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).

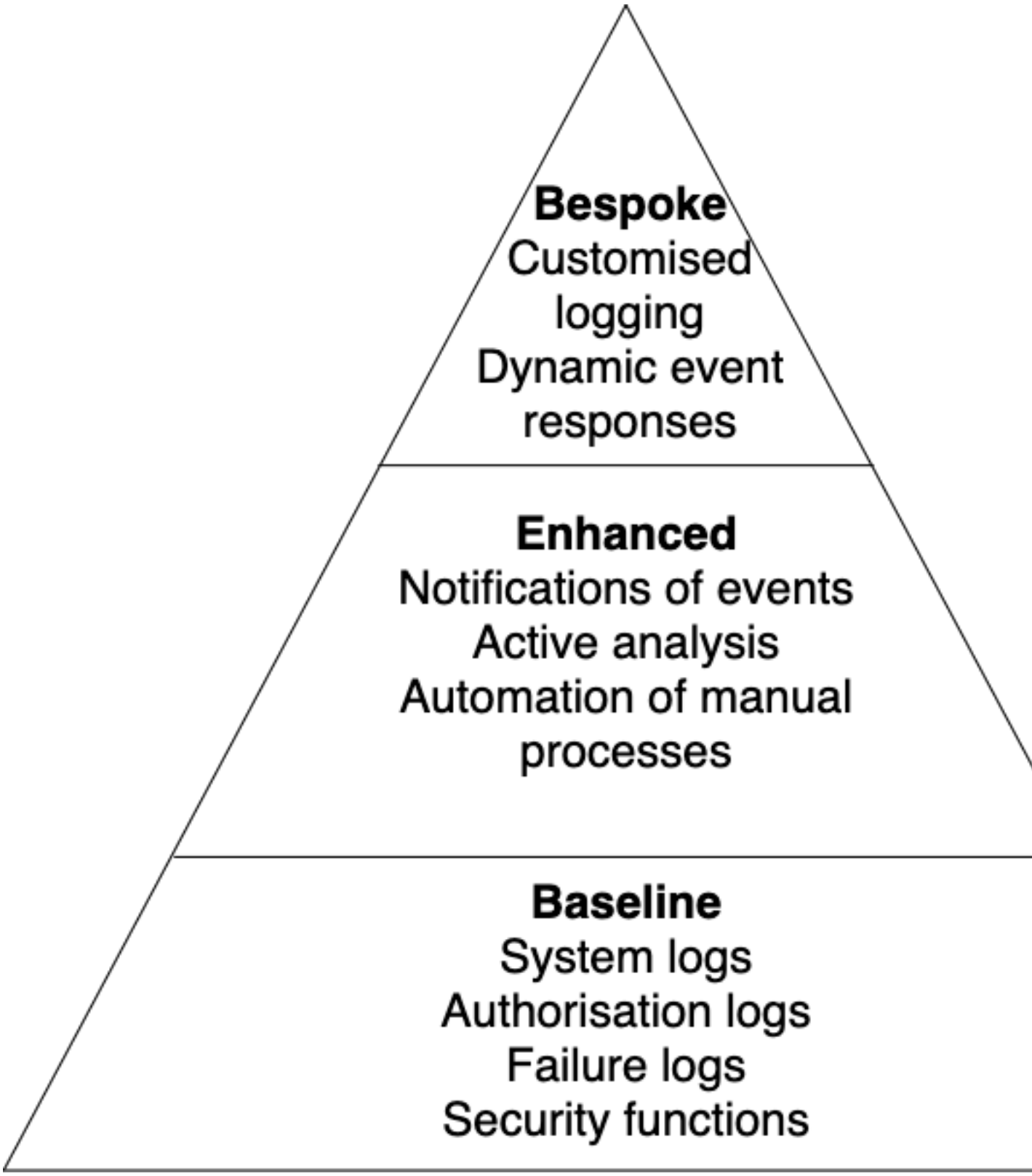
Three tiers have been developed to reflect the breadth and complexity of collecting and forwarding log data.

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.

Last updated: April 20th, 2020.

Guides

General Guides

Automated certificate renewal

Where technically suitable, all new 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.

Data Security & Privacy Lifecycle Expectations

Below are a series of data security and privacy expectations of 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 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 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 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.

Defensive domain registrations

The 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 doman registrations and operations.

Online identifiers in security logging & monitoring

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 that we do so when we design, implement, and operate our online services. Put simply, it is easiest for us to assume that any information we capture and process from our public-facing services might contain personal information and protect this information accordingly.

What are online identifiers?

Online identifiers are anything that could be used to track someone as they interact with our online services. This can include their IP address(es), any cookies that we (or 3rd parties we use) set on their devices, information placed into local storage on their device, username(s) associated with our services, and things like third-party authentication tokens etc. It could also include metadata captured about a device interacting with our 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 us as part of using a service (thus providing a link between all of the activities that their IP or session cookie has done with their identity), or if there is a legal route available to us to unmask the identity behind an identifier - such as by 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 ICO key definitions and 'Recital 30' from the Article 29 Working Group. There is also an informative article here).

What does this mean for our services?

We need to think carefully about what metadata about a user's interaction with our service we are capturing, how long we are retaining that information, and who will have access to it. We need to be clear in our privacy notices on our services about the information we capture as part of a user's interaction with them - including 'anonymous' interactions, such as just browsing information about the services. Metadata like this must be included in the scope of privacy impact assessments for our services.

This only applies to our externally-facing services; it does not apply to our internal services, although it is undoubtedly good practice to apply the same approach.

What does this mean for security logging and monitoring?

Under the updated data protection legislation we are still able to log and monitor the use of our services to help defend them against cyber security attacks, and misuse (such as fraud).

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. Thus we are still able to log and monitor external interactions with our services to look for evidence of cyber security attacks, and to enable us to act to protect those services - such as by blocking an IP address associated with known malware, or which is trying to perform a denial of service against us.

However we must be careful that we do not over-retain such log information, or share it with those who do not need to see it, without lawful justification. We must also ensure we act in a proportionate way with this data.

The MoJ CISO is ultimately responsible for all logging and monitoring systems which have been implemented for cyber security purposes, and as such is the Information Asset Owner for all logging and monitoring data.

By default we will retain raw logs in direct relation to security logging and monitoring purposes for at least 90 days and 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.

Aggregate data from logging systems (such as number of particular types of events, total numbers of visits to sites, etc) 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 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 as sensitive logs should be analysed programmatically in-situ. Bulk exporting should be prevented by default technical/access controls where possible. If

a bulk extract from a logging system is required (for example, into a more complex analytical system or in a wider migration) then this requires the approval of the MOJ CISO.

Personnel security clearances

Baseline Personnel Security Standard (BPSS)

Unless otherwise agreed formally by 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.

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

Standards Assurance Tables

The 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 seperately.

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 authorsed 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?

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 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@digital.justice.gov.uk. For help with data protection, contact data.compliance@justice.gov.uk.

The consultant 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.

Active Cyber Defence

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, 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.

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.

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.

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, 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).

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.

Product specific guides

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 master 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 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 G-Suite 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 screts.

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 master password

You need to create a master 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 master 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 master password with anyone, even your line manager or MOJ security.)

Using it abroad

Taking a device (such as personal smartphone) that has MOJ LastPass installed counts as travelling abroad 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 master password as you have forgotten it, contact lastpass-admins@digital.justice.gov.uk

Suppliers to MOJ

Assessing suppliers

The 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 G-Suite, Microsoft Office 365, Trello and AtlassianCloud based on the Cloud Security Principles, information risk assessment techniques and shared data within HMG.

Contractual promises

The 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.

Data Destruction

Instruction & Confirmation Letter

The current draft of a templated 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: _____

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

Short format clause

The current draft of the 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.

Long format clause

The current draft of the 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 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 MOJ commodity long format data destruction appendix. The appendix is a dependancy 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).

Security Aspects Letters

Purpose

The 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)

……(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 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 abroad

Supplier staff are **not** prohibited from working abroad while processing MOJ data on the basis that adequate information controls and governance are maintained.

When working abroad, 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 acknowleges these cases.

Local end-user device data

The MOJ acknowleges 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.

Mythbusting

Criminal Justice Secure Mail

The MOJ operates the CJSM service to enable those people working in the Justice system who do not have access to a suitable email service to exchange information in a safer way.

The MOJ does **not** require the use of CJSM where other suitably secure and efficient means can be used. It is considered a safe option to enable communication but it is only an option.

Government secure email policy

Email services that are materially aligned to the UK government secure email policy are suitable for the movement of `OFFICIAL` data, including where the `SENSITIVE` handling caveat has been applied.

Data sovereignty

The 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 Cybersecurity team - cybersecurity@digital.justice.gov.uk
- The MOJ's Data Protection Officer - data.compliance@justice.gov.uk

Internet -v- PSN

The internet is 'ok'

The 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 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 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.

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.

Getting in touch

Contact information

Email

The MOJ D&T Cybersecurity team can be reached via cybersecurity@digital.justice.gov.uk.

Suppliers to the MOJ should primarily contact your usual MOJ points of contact.

Reporting an incident

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

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

Vulnerability Disclosure

Vulnerability Disclosure Policy

The 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/

Implementing security.txt

Domains where the 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/master/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/master/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.