



Ministry
of Justice

Cyber Security Guidance

Technical User Edition



Contact details.....	24
Information security policies.....	24
Management direction for information security.....	24
Avoiding too much security.....	24
IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER.....	25
IT Security Policy (Overview).....	26
Line Manager approval.....	34
Shared Responsibility Models.....	35
Technical Controls Policy.....	36
Mobile devices and teleworking.....	47
Mobile device policy.....	47
Mobile Device and Remote Working Policy.....	47
Teleworking.....	54
Accessing MoJ IT systems from overseas.....	54
General advice on taking equipment overseas.....	57
Overseas travel.....	59
Personal devices.....	59
Human resource security.....	61
Prior to employment.....	61
Minimum User Clearance Requirements Guide.....	61
National Security Vetting for External Candidates FAQ.....	62
National Security Vetting contact.....	65
National Security Vetting questions.....	66
Pre-employment screening.....	70
Pre-Employment Screening and Vetting of External Candidates - FAQs.....	70
Security clearance appeals policy.....	74
Security clearance appeals procedures.....	75
Security vetting assessment of need.....	80
During employment.....	80
Ongoing Personnel Security.....	80
Personnel risk assessment.....	82
Reporting personal circumstance changes.....	84
Training and Education.....	85
Voluntary drug testing policy.....	86
Voluntary drug testing policy procedures.....	87
Termination and change of employment.....	90
End or change of employment.....	90
Leavers with NSC and NSVCs.....	90
Asset management.....	91
Responsibility for assets.....	91
Acceptable use of Information Technology at work.....	91
Acceptable Use Policy.....	93
Guidance on IT Accounts and Assets for Long Term Leave.....	99
Protect yourself online.....	100
Information classification.....	101
Data Handling and Information Sharing Guide.....	101
Government Classification Scheme.....	106
Information classification, handling and security guide.....	110

Sending information securely.....	360
Spam and Phishing Guide.....	364
Web Browsing.....	366
Wifi security policy.....	369
System acquisition, development and maintenance.....	372
Security requirements of information systems.....	372
Technical Security Controls Guide.....	372
Security in development and support processes.....	377
Maintained by Default.....	377
Secure by Default.....	377
Source code publishing.....	378
System Test Standard.....	379
Test data.....	384
Using Live Data for Testing purposes.....	384
Supplier relationships.....	386
Information security in supplier relationships.....	386
Assessing suppliers.....	386
Contractual promises.....	386
Security Aspects Letters.....	386
Supplier corporate IT.....	390
Supplier service delivery management.....	391
Azure Account Baseline Templates.....	391
Baseline for Amazon Web Services accounts.....	393
Baseline for Azure Subscriptions.....	397
Information security incident management.....	401
Management of information security incidents and improvements.....	401
Forensic Principles.....	401
Incident Management Plan and Process Guide.....	419
IT Incident Management Policy.....	436
Lost devices or other IT security incidents.....	446
Information security aspects of business continuity management.....	446
Information security continuity.....	446
IT Disaster Recovery Plan and Process Guide.....	446
IT Disaster Recovery Policy.....	456
Compliance.....	460
Compliance with legal and contractual requirements.....	460
Data destruction.....	460
Data security and privacy.....	465
Information security reviews.....	469
Standards Assurance Tables.....	469
Risk Assessment.....	472
Risk Management.....	472
Infrastructure System Accreditation.....	472
What is an IT Health Check, and why is it important?.....	473

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

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

Information security policies

Management direction for information security

Avoiding too much security	All users
IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER	All users
IT Security All Users Policy	All users (Policy)
IT Security Policy (Overview)	All users (Policy)
IT Security Technical Users Policy	Technical Architect, DevOps, IT Service Manager, Software Developer (Policy)
Line Manager approval	All users
Shared Responsibility Models	Technical Architect, DevOps, IT Service Manager, Software Developer
Technical Controls Policy	Technical Architect, DevOps, IT Service Manager, Software Developer

Mobile devices and teleworking

Mobile device policy

Mobile Device and Remote Working Policy	All users (Policy)
Remote Working	All users

Teleworking

Accessing MoJ IT systems from overseas	All users
General advice on taking equipment overseas	All users
Personal Devices	All users

Human resource security

Prior to employment

Minimum User Clearance Levels Guide	All users
National Security Vetting contact	All users
National Security Vetting questions	All users
National Security Vetting for External Candidates FAQ	All users
Pre-employment screening	All users
Pre-Employment Screening and Vetting of External Candidates - FAQs	All users
Security clearance appeals policy	All users
Security clearance appeals procedures	All users
Security vetting assessment of need	All users

During employment

Ongoing Personnel Security	All users
Personnel risk assessment	All users
Reporting personal circumstance changes	All users
Training and Education	All users
Voluntary drug testing policy	All users
Voluntary drug testing policy procedures	All users

Termination and change of employment

End or change of employment	All users
Leavers with NSC and NSVCs	All users

Asset management

Responsibility for assets

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

Information classification

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

Media handling

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

Access control

Business requirements of access control

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

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

User access management

Authentication	Technical Architect, DevOps, IT Service Manager, Software Developer
Management access	Technical Architect, DevOps, IT Service Manager, Software Developer
Managing User Access Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Multi-Factor Authentication	Technical Architect, DevOps, IT Service Manager, Software Developer
Privileged User Backups, Removable Media and Incident Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Privileged User Configuration, Patching and Change Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Privileged User Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Privileged User Logging and Protective Monitoring Guide	Technical Architect, DevOps, IT Service Manager, Software Developer

User responsibilities

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

System and application access control

Account management	Technical Architect, DevOps, IT Service Manager, Software Developer
Authorisation	Technical Architect, DevOps, IT Service Manager, Software Developer
Multi-user accounts and Public-Facing Service Accounts Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Password Creation and Authentication Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Password Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Password Managers	All users
Passwords	All users
Password Storage and Management Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Policies for Google Apps administrators	Technical Architect, DevOps, IT Service Manager, Software Developer

Policies for MacBook Administrators	Technical Architect, DevOps, IT Service Manager, Software Developer
System User and Application Administrators	Technical Architect, DevOps, IT Service Manager, Software Developer
Using LastPass Enterprise	All users

Cryptography

Cryptographic controls

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

Physical and environmental security

Secure areas

CCTV policy	All users
Entry and exit search policy	All users
Personal mail and parcel delivery policy and procedure	All users
Physical security policy	All users
Public protest and demonstrations policy	All users
Security in the office	All users
Security threat level and emergency procedures	All users
Visitor access policy	All users

Equipment

Clear Screen and Desk Policy	All users
Equipment Reassignment Guide	All users
Laptops	All users
Locking and shutdown	All users
Policies for MacBook Users	All users
System Lockdown and Hardening Standard	Technical Architect, DevOps, IT Service Manager, Software Developer

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

Control of operational software

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

Technical vulnerability management

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

Communications security

Network security management

Code of Connection Standard	Technical Architect, DevOps, IT Service Manager, Software Developer
Defensive domain registrations	Technical Architect, DevOps, IT Service Manager, Software Developer
Domain names and Domain Name System (DNS) security policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Internet v. PSN	Technical Architect, DevOps, IT Service Manager, Software Developer
IP DNS Diagram Handling	Technical Architect, DevOps, IT Service Manager, Software Developer
Multiple Back-to-back Consecutive Firewalls	Technical Architect, DevOps, IT Service Manager, Software Developer
Networks are just bearers	Technical Architect, DevOps, IT Service Manager, Software Developer

Information transfer

Bluetooth	All users
Criminal Justice Secure Mail (CJSM)	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Sovereignty	Technical Architect, DevOps, IT Service Manager, Software Developer
Email	All users
Email Authentication Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Email Blocklist Policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Email Blocklist Process	Technical Architect, DevOps, IT Service Manager, Software Developer
Email Security Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
General Apps Guidance	All users
Secure Data Transfer Guide	All users
Secure Email Transfer Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Sending information securely	All users
Spam and Phishing Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Web browsing security policy profiles	All users (Policy)
Wifi security policy	All users (Policy)

System acquisition, development and maintenance

Security requirements of information systems

Technical Security Controls Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Technical Security Controls Guide: Defe	

Test data

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

Supplier relationships

Information security in supplier relationships

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

Supplier service delivery management

Azure Account Baseline Templates	Technical Architect, DevOps, IT Service Manager, Software Developer
Baseline for Amazon Web Services accounts	Technical Architect, DevOps, IT Service Manager, Software Developer
Baseline for Azure Subscriptions	Technical Architect, DevOps, IT Service Manager, Software Developer

Information security incident management

Management of information security incidents and lost devices

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

Information security aspects of business continuity management

Information security continuity

IT Disaster Recovery Plan and Process Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
---	---

Glossary

A glossary of some terms used in this guidance is available [here](#).

Acronyms

A more extensive list of acronyms is available [here](#).

Technical Guidance

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

Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: itpolicycontent@digital.justice.gov.uk.

Change log for Ministry of Justice (MoJ) Security Guidance

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

2021-12-23 13:50 GMT [Update overseas travel guidance](#)

Updates to information on overseas travel and accessing MoJ IT systems from overseas.

2021-12-21 13:18 GMT [Provide seasonal SMS scam advice](#)

Material to help improve awareness and best practices for security.

2021-12-15 15:09 GMT [Use DuckDuckGo search engine](#)

Default to using DDG for content search.

2021-12-13 11:44 GMT [Security threat level guidance](#)

New security threat Level guidance, and associated procedures.

2021-12-13 11:27 GMT [Debrief on return from travel](#)

Added description of a security debrief that is mandatory after some travel or where other security conditions apply.

2021-12-13 11:24 GMT [Accessing MoJ systems from overseas](#)

Added link to supplementary information on the MoJ Intranet.

2021-12-08 09:15 GMT [Email access](#)

Added clarification regarding when access is permitted to a user's business email account.

2021-12-07 15:18 GMT [Email Authentication](#)

Added guidance requiring the use of MTA-SLS and TLS-RPT in MoJ email systems.

2021-12-03 13:39 GMT [Visitor Access Policy](#)

Policy regarding the access and security management controls that are in place for all visitors to MoJ buildings.

2021-12-02 16:54 GMT [National Security Vetting Contact](#)

Updated application form for candidacy to be an NSVC.

2021-11-30 13:54 GMT [Personal Devices](#)

Clarified guidance on connecting personal devices using Bluetooth, and added new section on connected vehicles.

2021-11-22 16:23 GMT MFA

Clarified guidance on sending one-time MFA codes only to individual devices or accounts, not to shared devices or accounts.

2021-11-22 14:14 GMT Government Classification Scheme

Updated and consolidated guidance on classification of Government information.

2021-11-19 15:22 GMT Other guidance and security.txt

Improved structure for other guidance information, and added security.txt file.

2021-11-19 14:29 GMT Security in the office

Key security points for working in a Ministry of Justice location.

2021-11-19 10:09 GMT Sending information securely

Guidance on working securely with paper documents and files.

2021-11-18 17:03 GMT Protests and demonstrations

Policy and guidance on public protests and demonstrations.

2021-11-17 17:07 GMT Personal devices

Updated guidance about using a personal device to connect to a business Teams meeting as a Guest.

2021-11-09 15:37 GMT Acceptable use policy

Provide more detail on monitoring of systems and information, and to clarify the situation regarding Data Protection and the storage or processing of information outside the UK.

2021-11-08 17:30 GMT System backup policy

Corrected broken links within the content, also some structural changes for easier cross-referencing with related topics.

2021-11-04 10:28 GMT CCTV Policy

This policy details the purpose, usage, and management of the CCTV systems within the MoJ.

2021-11-04 09:05 GMT Working securely with paper documents and files

This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office.

2021-11-03 17:12 GMT Email blocking

The policy and processes for blocking emails, and deleting emails through administrative processes, across email services across the MoJ.

2021-11-03 17:00 GMT Domain names

An overview of domain name registration and monitoring principles and responsibilities within the MoJ.

2021-10-29 11:52 BST Logging retention

Information about keeping logging information.

2021-10-20 09:53 BST National Security Vetting contacts

Updates to the process and information for National Security Vetting contacts.

2021-10-19 13:06 BST Remote working

Simplified the guidance regarding remote working.

2021-10-15 16:27 BST Email best practices

Added guidance regarding attachments and the use of 'cc' and 'bcc' fields in emails.

2021-10-15 13:39 BST Security clearance appeals procedures

Added guidance for appealing a security clearance decision.

2021-10-14 13:47 BST Azure subscription baselines

Added guidance on baselines and templates for Azure subscriptions.

2021-10-13 15:50 BST IT Health Checks

Added guidance on requesting and managing IT Health Checks.

2021-10-13 09:26 BST User clearance requirements

Clarification to minimum user clearance requirements.

Role	Responsibility	Which includes...
Contract Owners	<p>Contract Owners are responsible for ensuring contractors adhere to the IT Security Policy set out here and in associated documentation.</p>	<p>Verify that contracts are written to reflect the MoJ's IT Security Policy.</p> <p>Ensure contractors comply with the requirements set out by this policy and associated documentation.</p> <p>Being responsible for escalating the risk of non-compliance by a supplier, and seeking guidance on suspected non-compliance with security requirements in a contract.</p> <p>Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the MoJ, is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.</p>

Incidents

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

Operational Security Team

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

Contact details

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

IT Security Technical Users Policy

Introduction

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

Audience

This policy is aimed at:

Technical users

These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Service Providers

Defined as any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including

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

Incidents

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

Operational Security Team

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

Contact details

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

Line Manager approval

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

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

Examples include:

- General advice on taking equipment overseas.
- Personal DevicesPersonal device use.

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

Steps to follow (Line Managers)

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

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

Steps to follow (Direct Reports)

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

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

Contact details

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

Shared Responsibility Models

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

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

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

Assessments

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

Inherited

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

Shared

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

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

MoJ specific

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

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

Technical Controls Policy

Note: This document might refer to several organisations, information sources, or terms that have

Approach to technical controls

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

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

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

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

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

Overarching objectives

The objectives of this policy are:

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

Technical controls lifecycle

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

POL.TCP.004: The selection of technical security controls **SHALL** be based on a risk assessment.

For systems covered under the accreditation process, this is an assessment conducted following HMG Information Security Selection Criteria.

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

POL.TCP.029: Any access control solution **SHALL** take into consideration the [Information Classification and Handling Policy](#).

POL.TCP.030: All IT systems **SHALL** define and maintain an access control schema which aligns to the [MoJ IT Security Policy](#).

POL.TCP.031: All IT systems **SHALL** follow the [Access Control Policy](#).

User Identity Management

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

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

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

User Registration

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

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

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

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

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

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

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

Privilege Management

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

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

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

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

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

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

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

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

Data Backup

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

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

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

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

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

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

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

POL.TCP.114: All IT systems **SHALL** conform to the [System Backup Policy](#).

Electronic Messaging Policy

Electronic mail (E-Mail)

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

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

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

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

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

Further details on the secure operating procedures applicable to the use of email are provided in the [Acceptable Use Policy](#).

Configuration Management Policy

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

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

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

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

- Has a role such as system support or IT investigation role, such that without further authority or authorisation, an individual might:
 - Act as another user.
 - Obtain credentials for another user.
 - Directly access other users' data.

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

The 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

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

National Security Vetting for External Candidates FAQ

This document provides recruiting managers with answers to frequently-asked questions regarding National Security Vetting for external candidates.

The processes described in this document are under continual review as part of the Ministry of Justice (MoJ) "simpler processes" activities. These FAQs will be updated as required.

Section 1: Directly employed staff

Q1. How does the vacancy manager know what level of clearance a role requires?

Vacancy managers **SHALL** always advertise their roles with the correct level of clearance required. Levels of clearance are defined by the requirements of the role being filled, not by the level of clearance the candidate already possesses. Your National Security Vetting Contact (NSVC) can confirm whether your role requires national security vetting in addition to pre-employment checks. Wrongly classifying roles at advert stage leads to delays in on-boarding.

If you don't know who your NSVC is, refer to the download [here](#).

Q2. What is the pre-employment check process?

This depends on how the candidate is being recruited and their level in the organisation.

Bands A-F (non-SCS) recruited through fair and open recruitment

- All candidates **SHALL** undergo pre-employment checks relevant to the role.
- SSCL will inform applicants to bring their Right To Work (RTW), ID and address documentation to interview.
- Line managers **SHALL** check these documents, make a note of the document reference numbers and input these into Oleo at the Interview Scores Entered stage.
- If the applicant is successful at interview, SSCL will make a provisional offer and ask the candidate to upload copies of the same RTW, ID and address documents into Oleo.
- If NSV is required for the role (as indicated by the vacancy manager in the advert), SSCL will also send a link to the candidate so they can complete an on-line security questionnaire on the NSVS portal.

SCS Grades

- The MoJ SCSBP team work closely with the Government Recruitment Service (GRS), who manage the SCS recruitment campaigns through open and fair competition.
- GRS notify the MoJ SCSBP Team of the successful candidate at interview stage.
- The MoJ SCSBP team contact the candidate to initiate the on-boarding process and send the candidate forms to complete so that SSCL can prepare and issue their contract.
- SCSBP team also arrange a date to meet the candidate and verify their identity documents. These details are used to complete the Clearance Request Form (CRF) and send this to SSCL through the NSVC in the business area.

- Once SSCL process the CRF, a link is sent to the candidate in an email to complete the required security checks on the NSVS portal.

Non-directly employed staff

Refer to [Section 2](#).

Q3. How long do the pre-employment and vetting checks take?

Clearances can involve multiple teams depending on the level of check.

If all information and the correct documents have been provided, the timescales are:

- Baseline Personnel Security Standard (BPSS): average six days.
- Disclosure Barring Service (DBS) standard checks: New checks: average five days.
- Disclosure Barring Service (DBS) enhanced checks: New checks: average six days.
- Counter terrorist check (CTC): new checks: minimum six weeks.
- Security clearance (SC): new checks: minimum six weeks.
- Developed vetting (DV): new checks: minimum 18 weeks.

Although the majority of DBS enhanced checks are completed in six working days, in some parts of the country police authorities quote an estimated response time of six to seven weeks.

Section 2: Staff recruited from external sources (non-directly employed)

As well as any clearance, all staff joining the MoJ from external sources (non-directly employed) are required to complete a BPSS check.

Non-directly employed workers include the following:

- Consultants.
- Contractors.
- Agency staff.
- Fee-Paid workers.

Managers **SHALL** ensure that these applicants undergo the mandatory BPSS checks covering: identity, nationality, immigration, Right To Work (RTW), employment history, and criminal records checks. SSCL will not conduct these checks.

For posts that require NSV:

- The vacancy manager **SHALL** discuss this with their NSVC and obtain a code which needs to be entered on the CRF submitted to SSCL.
- If you don't know who your NSVC is, refer to the download [here](#).
- SSCL only accepts requests with a valid vetting reference code provided on the CRF.
- SSCL sends a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.

To progress NSV applications, SSCL requires evidence of completion of BPSS checks from the contractor or agency before NSV can be initiated. If you need more information, contact SSCL on 0845 241 5359 (option 1).

Section 3: National security vetting

Q1. What is National Security Vetting (NSV)?

There are three levels of national security clearance:

- Counter terrorist check (CTC).
- Security clearance (SC).
- Developed vetting (DV).

These are mandatory for certain job roles and locations throughout the MoJ.

You need the appropriate level of national security clearance if:

- You have a proximity to public figures who have been assessed to be at risk from terrorist attack.

Q7. Why can't candidates use Apple products to submit the security questionnaire?

NSVS is run by UKSV. There are very strict controls in place to make certain that the information you provide is secure. Apple products work in a different way. UKSV can't be assured, by Apple, that their platform is secure.

We do not expect that this will change in the foreseeable future.

Section 5: Changes to roles or personal circumstances

This section contains information for managers and staff who are already in the MoJ, and have changes to their roles or personal circumstances:

Q1. I am a manager and I think a member of my team needs a national security vetting clearance to do a new piece of work. What should I do?

Talk to your National Security Vetting Contact (NSVC). All business areas that have at least one member of staff who holds Security Clearance should have one. If you don't know who your NSVC is, refer to the download [here](#).

Q2. My national security vetting clearance is going to expire soon, what should I do?

Speak to your national security vetting contact (NSVC), they will decide if it needs to be renewed and help you start the process off. If you don't know who your NSVC is, refer to the download [here](#).

Q3. My personal circumstances have changed, who should I advise?

For all changes in personal circumstances, please contact Cluster 2 Personnel Risk Management by emailing: VettingAftercare@cluster2security.gov.uk. Failure to report relevant changes could result in withdrawal of clearance.

Contact details

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

National Security Vetting contact

All business areas in the Ministry of Justice (MoJ) **SHALL** enrol or appoint a National Security Vetting Contact (NSVC) to help business areas progress and monitor applications for security clearance.

Most applications for National Security Vetting (NSV) clearance including Counter Terrorist Clearance (CTC), Security Check (SC), and Developed Vetting (DV) come through recruitment campaigns or are agency staff or contractors.

Some business areas employ large number of NSV-cleared people and those clearances need to be managed and monitored. The MoJ recognises that many personnel are contractors and agency staff, often with clearances held elsewhere. The NSVC **SHALL** facilitate the process and provide the business with a single point of contact and liaison with the National Security Vetting Team and Shared Services Connected Limited (SSCL).

Roles and responsibilities

- NSVCs are a mandatory role and one **SHALL** be appointed if there are National Security Vetted staff in any business area.
- NSVCs **SHALL** undergo the Baseline Personnel Security Standard (BPSS) check as a minimum, and be registered with [MoJ Group Security](#). How many NSVCs a business area needs is for Senior Managers to determine, based on how they are organised. For example, how many NSV clearances need processing and maintenance.
- NSVCs monitor the progress of all applications for an NSV clearance and **SHALL** maintain a register of all active NSV personnel within their business area.
- NSVCs **SHALL** provide the authorisation and complete the SSCL [Clearance Request Form](#) that confirms the level of clearance required for that person. SSCL will not process an application if an NSV matrix code is not supplied by the NSVC.
- NSVCs act as a single point of contact for their business area for SSCL and MoJ security to speed up the NSV process.

For further information regarding roles, responsibilities and necessary security clearances, contact mojgroupsecurity@justice.gov.uk.

Registration

- To register with MoJ Group Security, complete the [Registration Form in the Downloads section](#) at the bottom of this page, and return it to the email address provided in the form.
- On registration, MoJ Group Security provides the NSVC with the documents they need to manage the process and confirm registration with SSCL.

Downloads

The following downloads are available from the MoJ Intranet.

- [National Security Vetting contact guide](#).
- [National Security Vetting contact registration form](#)
- [National Security Vetting contacts register](#).

National Security Vetting questions

The processes described in this document are under review as part of Ministry of Justice (MoJ) "simpler processes" activities and these FAQs will be updated as required.

A downloadable version of this document is available [here](#).

National Security Vetting

What is National Security Vetting?

There are three levels of National Security Vetting (NSV) or clearance:

- Counter Terrorist Check (CTC).
- Security Check (SC)
- Developed Vetting (DV)

These are mandatory for certain job roles and locations throughout the MoJ.

You need the appropriate level of national security clearance if:

- You have a proximity to public figures who have been assessed to be at risk from terrorist attack.
- You work in a role which has the potential to cause significant damage to the MoJ or its assets.

Can NSV clearance be transferred from another government department?

Candidates cannot choose to transfer their NSV clearance, which lapses on their last day of employment. The MoJ determines what NSV is required for **the new role** and, if necessary, requests that a candidate's NSV clearance is transferred over before starting a new application for NSV. Not all other government department (OGDs) agree to transfer or share; it is their choice and there are various reasons for transferring or not transferring.

Three scenarios are given here:

Scenario 1: The level of clearance required for the new role is the same level the exporting department held for the individual.

For example, the new role requires SC clearance, and the candidate's exporting department held valid SC clearance for them.

Answer: Transfer can take place provided the exporting department confirms a valid NSV clearance **and** agrees to transfer it to the MoJ. In most cases these transfers can take place. In some exceptional circumstances, departments may refuse to transfer clearance to the MoJ. Where this happens, the candidate is required to complete NSV again.

Scenario 2: The level of clearance required for the new role is higher than the level the individual possesses in their current department.

For example, the role requires SC clearance and the current department holds CTC.

Answer: As the level of clearance is higher, the employee is required to complete an application for the new level on the NSV portal. A link is sent to them by SSCL once they have accepted a provisional offer.

Scenario 3: The level of clearance required for the role is lower than the current department holds.

For example, the employee currently possesses DV clearance with their present department but their new post in MoJ requires SC.

Answer: For security reasons, the MoJ **CAN NOT** transfer the higher level of clearance as the **role** does not require it. However, information is extracted to ensure that the candidate is not required to re-apply for a lower level of transfer. This is subject to the current department agreeing to transfer.

Can a candidate start work before applying for NSV?

If NSV is required for a position, candidates **SHOULD NOT** start until their NSV is confirmed.

In exceptional circumstances, a policy dispensation request can be made to **MoJ Group Security**, who will provide a request form and then give a recommendation on whether to grant or refuse the request. Any risk mitigation measures deemed to be required (such as plans to segregate the candidate from data that they don't have clearance to see) will also be provided for the Senior Security Advisor and the business unit to sign-up to.

As a minimum requirement, a candidate **SHALL** have submitted their Security Questionnaire on the NSVS portal. This does not extend to Contractors and Agency staff, who **SHALL** have their NSV in place before they start. If you don't know who your NSVC is, refer to the download [here](#).

Directly employed staff

How does the vacancy manager know what level of clearance a role requires?

Vacancy managers must always advertise their roles with the correct level of clearance required. Levels of clearance are defined by the requirements of the role being filled, and not by the level of clearance the candidate already possesses. Your NSVC can confirm whether your role requires national security vetting in addition to the usual pre-employment checks. Wrongly classifying roles at advert stage will lead to delays in on-boarding.

If you don't know who your NSVC is, refer to the download [here](#).

What is the pre-employment check process?

The checks required depend on how the candidate is being recruited and their level in the organisation.

Bands A-F (non-SCS) recruited through fair and open recruitment

- All candidates must undergo pre-employment checks relevant to the role, although staff transferring from OGDs have simplified checks.
- SSCL will ask applicants to bring their Right to Work, ID and address documentation to interview.
- Line managers must check these documents, make a note of the document reference numbers and input these into Oleeo at the Interview Scores Entered stage.
- If the applicant is successful at interview, SSCL will make a provisional offer and ask the candidate to upload copies of the same RTW, ID and address documents into Oleeo.
- If National Security Vetting (NSV) is required for the role (as indicated by the vacancy manager in the advert), SSCL will also send a link to the candidate so they can complete an on-line security questionnaire on the National Security Vetting Service (NSVS) portal.
- If the candidate already has any NSV clearances (and has noted this in their pre-appointment form), it may be possible to transfer these to the new role.

Bands A-F (non-SCS) recruited as exception to fair and open recruitment

- These include managed moves and loans and are not advertised in Oleeo.
- The vacancy manager should arrange for the individual to bring their original Right to Work, ID and address documentation to be checked.
- The vacancy manager should then submit a Clearance Request Form (CRF) to SSCL recording the details of these documents.
- SSCL send the successful candidate a provisional offer with links to the "Lumesse" system where they must upload the same documents.
- If NSV is required for the role, the vacancy manager must discuss this with their NSVC and obtain a code which needs to be entered on the CRF. SSCL will only accept requests with a valid vetting reference code provided on the Clearance Request Form.
- SSCL will send a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.
- If the candidate already has any NSV clearances, it may be possible to transfer these to the new role.

SCS Grades

- The MoJ Senior Civil Service Business Partners (SCSBP) team work closely with the Government Recruitment Service (GSR), who manage the SCS recruitment campaigns through open and fair competition.
- GSR notify the MoJ Senior Civil Service Business Partners (SCSBP) Team of the successful candidate.
- The MoJ SCSBP team contact the candidate to initiate the on-boarding process and send the candidate forms to complete so that SSCL can prepare and issue a contract.
- SCSBP team also arrange a date to meet the candidate and verify their identity documents. These details are used to complete the CRF and send this to SSCL via the NSVC in the business area.
- Once SSCL process the CRF, a link is sent to the candidate via an email to complete the required security checks on the NSVS portal. This process is also used to transfer existing clearances for OGD candidates.

How long do the pre-employment and vetting checks take?

Clearances can involve multiple teams depending on the level of check.

If all information and the correct documents have been provided, the timescales are:

- Baseline Personal Security Standard (BPSS): average six days.
- Disclosure Barring Service (DBS) standard checks: New checks: average five days.
- Disclosure Barring Service (DBS) enhanced checks: New checks: average six days.
- Counter terrorist check (CTC): new checks: minimum six weeks.
- Security check (SC): new checks: minimum six weeks.
- Developed vetting (DV): new checks: minimum 18 weeks.

Although the majority of DBS enhanced checks are completed in six working days, in some parts of the country authorities estimate a response time of six to seven weeks.

Non-directly employed

As well as any clearance, all staff joining the MoJ from external sources (non-directly employed) are required to complete a BPSS check. SSCL will not conduct these checks and it is the recruiting manager's responsibility to ensure that they are done.

Further guidance, and a link to the BPSS Verification Form, can be found on the MoJ Intranet [here](#).

Non-directly employed workers include the following:

- Consultants.
- Contractors.
- Agency staff.
- Fee-Paid workers.

For posts that require NSV:

Contact details

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

Pre-employment screening

Pre-employment screening involves a series of checks to help us make informed decisions about the suitability of individuals to work for the Ministry of Justice (MoJ) and its agencies. These checks ensure the following:

- Compliance with current legislation, for example evidence of Right to Work in the UK
- That applicants are who they say they are.
- The integrity of the applicant, our organisation, and the safety of staff and individuals in our care.

Pre-employment screening procedures are required for all people applying for posts or working within the MoJ, including:

- [Directly employed staff](#)
- [Staff transferring from Other Government Departments \(OGD Transfers\)](#).

FAQs

- [Pre-employment screening and Vetting FAQs](#)

Downloads

- [Applying criminal records checks](#)

Contact details

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

Pre-Employment Screening and Vetting of External Candidates - FAQs

This document describes pre-employment screening and National Security Vetting when recruiting External Candidates.

It answers Frequently Asked Questions (FAQs) for recruiting managers.

A downloadable version of this information is available [here](#).

Section 1: Pre-employment screening for directly employed staff

Q1. What is pre-employment screening?

Pre-employment screening involves a series of checks to help us make informed decisions about the suitability of people to work for the Ministry of Justice (MoJ) and its agencies. These checks ensure:

- Compliance with current legislation, for example evidence of right to work in the UK.
- That applicants are who they say they are.
- The integrity of the applicant, the organisation, and the safety of staff and others in our care.

All individuals working with the MoJ **SHALL** be required to complete a Baseline Personnel Security Standard (BPSS) check prior to taking up their role.

In addition, Disclosure and Barring Service (DBS) clearances might be required but only where the role involves interaction with children or vulnerable adults. These clearances are carried out through either a Standard or an Enhanced check.

National Security Vetting (NSV) might be required but only where the role requires Counter Terrorist Check (CTC), Security Clearance (SC) or Developed Vetting (DV) clearance. Refer to [Section 2](#) for more information. NSV is separate and additional to pre-employment screening checks.

Q2. What is BPSS?

Baseline Personnel Security Standard (BPSS) is the minimum level of clearance for all people working across the Civil Service. A BPSS check comprises of the following components or checks:

- Confirmation of right to work in the UK.
- Confirmation of ID and address.
- Eligibility.
- Criminal convictions.
- Employment history.
- Counter-signatory reference (where relevant).
- Health check (where relevant).

Q3. How does the vacancy manager know what level of clearance a role requires?

Vacancy managers **SHALL** always advertise their roles at the correct level of clearance required. Levels of clearance are defined by the requirements of the role being filled, not by the level of clearance the candidate already possesses. Your National Security Vetting Contact (NSVC) can confirm whether the role requires national security vetting in addition to pre-employment checks. Wrongly classifying roles at advert stage leads to delays in on-boarding.

If you don't know who your NSVC is, refer to the download [here](#).

Q4. What is the process for completing pre-employment checks?

This depends on how the candidate is being recruited, and their level in the organisation.

Bands A-F (non-SCS) recruited through fair and open recruitment

- All candidates **SHALL** undergo pre-employment checks relevant to the role.
- SSCL ask applicants to bring their Right to Work (RTW), ID, and address documentation to interview.
- Line managers **SHALL** check these documents, make a note of the document reference numbers, and input these into Oleeo (the recruitment website), at the Interview Scores Entered stage.
- If the applicant is successful at interview, SSCL makes a provisional offer, and asks the candidate to upload copies of the same RTW, ID, and address documents into Oleeo.
- If NSV is required for the role (as indicated by the vacancy manager in the advert), SSCL also sends a link to the candidate so they can complete an on-line security questionnaire on the NSVS portal.

SCS Grades

- The MoJ SCSBP team work closely with Civil Service Resourcing (CSR), now called Government Recruitment Service (GRS), who manage the SCS recruitment campaigns through open and fair competition.
- GSR notify the MoJ SCSBP Team of the successful candidate at interview stage.
- The MoJ SCSBP team contacts the candidate to initiate the on-boarding process, and sends the candidate forms to complete so that SSCL can prepare and issue their contract.
- SCSBP team also arrange a date to meet the candidate and verify their identity documents. These details are used to complete the Clearance Request Form (CRF) and send this to SSCL via the National Security Vetting Contact (NSVC) in the business area.
- Once SSCL processes the CRF Form, a link is sent to the candidate by email to complete the required security checks on the NSVS portal.

Non-directly employed staff

Refer to [Section 2](#).

Q5. How long do the pre-employment and vetting checks take?

Any clearances can involve multiple teams and depend on the level of check.

If all information and the correct documents have been provided, the average time for the checks to be completed is:

- Baseline Personnel Security Standard (BPSS): average 6 days
- Disclosure Barring Service (DBS) standard checks: New checks average 5 days
- Disclosure Barring Service (DBS) enhanced checks: New checks average 6 days

- Counter terrorist check (CTC): New checks minimum six weeks, averaging six weeks
- Security clearance (SC): New checks minimum six weeks, averaging six weeks
- Developed vetting (DV): New checks minimum 18 weeks.

Although the majority of DBS enhanced checks are completed in six working days, in some parts of the country police authorities quote a six to seven week response time.

Section 2: Staff recruited from external sources (non-directly employed)

All staff joining the MoJ from external sources (non-directly employed) are required to complete a BPSS check.

Non-directly employed workers include the following:

- Consultants.
- Contractors.
- Agency staff.
- Fee-Paid workers.

Managers **SHALL** ensure that these applicants undergo the mandatory BPSS checks covering identity, nationality, immigration, right to work, employment history, and criminal records checks. They can check the results on the BPSS Verification Record form, which employers **SHALL** complete to verify that the checks have been made.

Note: SSCL do not conduct these checks.

Further guidance, and a link to the BPSS Verification Form, can be found on the MoJ [Intranet](#).

If you have posts that require NSV

If NSV is required for the role, the vacancy manager **SHALL** discuss this with their National Security Vetting Contact (NSVC), and obtain a code that is entered on the Clearance Request Form (CRF) prior to submission to SSCL.

If you don't know who your NSVC is, refer to the download [here](#).

- SSCL only accepts requests with a valid vetting reference code provided on the CRF.
- SSCL sends a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.

To progress NSV applications, SSCL requires evidence of completion of BPSS checks from the contractor or agency before NSV can be started. If you need more information, contact SSCL on 0845 241 5359 (option 1).

Section 3: National Security Vetting

Q1. What is National Security Vetting (NSV)?

There are 3 levels of national security clearance:

- Counter Terrorist Check (CTC).
- Security Clearance (SC).
- Developed Vetting (DV).

These are mandatory for certain job roles and locations throughout the MoJ.

You need the appropriate level of national security clearance if:

- You have a proximity to public figures who have been assessed to be at risk from terrorist attack.
- You work in a role which has the potential to cause significant damage to the MoJ or its assets.

Q2. How long does national security vetting take?

Typical timings from completion of application are

- Counter Terrorist Check (CTC): New checks minimum six weeks, averaging six weeks.
- Security Clearance (SC): New checks minimum six weeks, averaging six weeks.
- Developed Vetting (DV): New checks minimum 18 weeks.

Q3. NSV takes too long, can the candidate start at BPSS and apply for NSV once they are in post?

If NSV is required for a position, candidates **SHOULD NOT** start until their NSV is confirmed.

In exceptional circumstances, a policy dispensation request **CAN** be made to the Cluster 2 Security Unit (C2SU). Do this by emailing [MoJ Group Security](#). C2SU recommend whether to grant or refuse the request. Any required risk mitigation measures will be provided by C2SU and **SHALL** require the Senior Security Advisor and the business unit to sign-up to these required measures.

Contractors and Agency staff **SHALL** have their NSV in place before they start. For help, contact your NSVC in the first instance. If you don't know who your NSVC is, refer to the download [here](#).

Section 4: Applying for NSV

Q1. I submitted an NSV request several weeks ago, how do I find out where it is?

Contact the SSCL contact centre on 0845 241 5359 (option 1). SSCL are responsible for the registration and sponsoring of all applications for the NSVS portal.

Q2. SSCL have told me that they have completed sponsors' actions, what does that mean?

It means that your security questionnaire has been forwarded to United Kingdom Security Vetting (UKSV), and the vetting process has started. All actions are complete at the MoJ. There are no further actions until UKSV returns the file with a decision.

Q3. Why is the candidate required to fill in forms on the NSVS portal and provide information that may already be held elsewhere in the recruitment process?

NSV is a separate process to anything HR-related. For legal reasons, we often have to ask applicants questions to confirm facts. Even if we have that information elsewhere, we still require the applicant to confirm it. It is usually easier to gather everything we need in one process; the alternative would be to repeatedly return for further information. Experience has shown that this causes significant delay, and we don't ask for information that we would not need.

Q4. What if the candidate doesn't complete specific dates and details for the Security Questionnaire?

All required information on the Security Questionnaire must be completed in full and to the best of the candidate's knowledge. If certain dates or information are not known, an explanation should be added in the information box. Missing or incorrect data will delay the application because the file will be referred to a vetting officer who will have to investigate and find the missing data.

Q5. What happens if the candidate leaves out information?

For security reasons we cannot give too much detail about the vetting process; however, we can confirm that information is checked in a variety of systems and databases. If information is mis-matched, it forces the file to be referred to a vetting officer and this intervention causes significant delay. Thirteen percent of all NSV cases are rejected because the subject doesn't provide their middle name(s) and it is not unusual for people to put the wrong date of birth. It is crucial that accurate information is provided; it really helps vet people quickly.

Q6. My candidate completed the national security vetting application some time ago and hasn't heard anything, who can I check this with?

SC/CTC takes a minimum of six weeks and DV takes at least 18 weeks. If this time frame has been passed, contact the National Security Vetting Contact (NSVC) who requested clearance and they can contact SSCL for an update.

If you don't know who your NSVC is, refer to the download [here](#).

Q7. Why can't candidates use an Apple machine or iPad to submit the NSV security questionnaire?

NSVS is run by UKSV. There are very strict controls in place to make certain that the information you provide is secure. Apple products work in a different way and UKSV can't be assured by Apple that their platform is secure. We do not expect that will change in the foreseeable future.

Section 5: Changes to roles or personal circumstances

This section contains information for managers, and for staff who are already in the MoJ, regarding changes to roles or personal circumstances.

Q1. I am a manager and I think a member of my team needs a national security vetting clearance to do a new piece of work. What should I do?

Talk to your NSVC. All business areas that have at least one member of staff who holds Security Clearance should have one. If you don't know who your NSVC is, refer to the download [here](#).

Q2. My national security vetting clearance is going to expire soon, what should I do?

Speak to your NSVC. They decide if it needs to be renewed and help you start the process off. If you don't know who your NSVC is, refer to the download [here](#).

Q3. My personal circumstances have changed, who should I advise?

For all changes in personal circumstances, contact Cluster 2 Personnel Risk Management by emailing VettingAftercare@cluster2security.gov.uk.

You can find more information [here](#).

Contact details

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

Security clearance appeals policy

The Cluster 2 Security Unit (C2SU) forms part of the Transforming Government Security programme, which aims to standardise and strengthen operational security across Government.

The Ministry of Justice (MoJ) is part of Cluster 2, and so must adhere to this policy.

This policy applies to permanent members of staff and contractors' employees employed on the work of the MoJ, and those organisations for which the Cluster 2 Security Unit holds the responsibility for vetting, including non-departmental public bodies (NDPBs).

It also applies to:

- Existing contractors' employees or other non-permanent staff, who are already engaged in the work of the MoJ.
- Existing permanent members of staff of other government departments and organisations who have applied for a security clearance with the MoJ.
- Existing contractors' employees already engaged on government work in other departments and organisations who have applied for a security clearance with the MoJ.

It does not apply to individuals on initial recruitment to the Civil Service seeking a first security clearance for permanent employment or contractual work with the MoJ.

It does include existing employees of a contractor who are newly deployed to contracted work for the MoJ.

Policy

The MoJ provides a right of internal appeal to the Permanent Secretary where an individual who falls within the scope of this policy has a security clearance refused or withdrawn by the Cluster 2 Security Unit. The appeal **SHOULD** be submitted within 15 working days of notification of the refusal or withdrawal decision.

Where the Permanent Secretary upholds the vetting decision to refuse or withdraw security clearance, there is a further avenue of appeal to the independent Security Vetting Appeals Panel (SVAP). This appeal **SHOULD** be submitted within 28 days of notification that the vetting decision has been upheld.

To achieve this requirement, the Cluster 2 Security Unit must:

- Ensure that the decision to refuse or withdraw national security clearance for an existing permanent or contracted employee (as identified previously) is communicated to the individual promptly and in writing.

- Ensure that the individual is given the full reasons for the decision, and the relevant facts upon which it was based, as far as considerations of security and confidentiality allow.
- Provide the employee with a clear explanation of their right to an internal appeal and the mechanisms by which they can make that appeal, and of their entitlement, should they remain dissatisfied with the outcome, to appeal to the Security Vetting Appeals Panel (SVAP).
- Ensure the appeal process will be carried out independently from the vetting decision makers and anyone involved in the original decision to refuse or withdraw clearance. The process will also - as far as issues of national security and confidentiality allow - be undertaken with transparency, providing a fair opportunity for the appellant to address the reasons for the decision.

Further guidance

Detailed guidance on the processes and timescales for internal and external appeals is given in the Security Clearance Appeals Procedures.

More information about the Security Clearance Appeals Procedures can be obtained from [MoJ Group Security](#).

Contact details

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

Security clearance appeals procedures

These procedures provide an overview of the requirements for appealing a decision by the Cluster 2 Security Unit Head of Personnel Security, or their representatives in the Decision Making or Personnel Risk Management Teams, to refuse or withdraw national security clearance for Civil Service and Government employees and contractors working on Cluster 2 business.

There is an internal appeal to the Ministry of Justice (MoJ) Permanent Secretary, and if the decision to refuse or withdraw clearance is upheld, a subsequent external appeal to the Security Vetting Appeals Panel (SVAP).

More detailed guidance on the processes and timescales for internal and external appeals can be found at [Annex A: Cluster 2 Security Unit Security Clearance Appeals Procedures](#).

In this document the term **SHALL** is used to indicate an absolute requirement.

If you have any queries on the content of this document contact [MoJ Group Security](#).

Scope and aim

These procedures apply to permanent members of staff and contractors' employees employed on the work of MoJ, and those organisations for which the Cluster 2 Security Unit holds the responsibility for vetting, including non-departmental public bodies (NDPBs).

It also applies to:

- Existing contractors' employees or other non-permanent staff, who are already engaged in the work of the MoJ.
- Existing permanent members of staff of other government departments and organisations who have applied for a security clearance with the MoJ.
- Existing contractors' employees already engaged on government work in other departments and organisations who have applied for a security clearance with the MoJ.

It does not apply to individuals on initial recruitment to the Civil Service seeking a first security clearance for permanent employment or contractual work with the MoJ.

These procedures apply to existing employees of a contractor who are newly deployed to contracted work for the MoJ.

The Government functional standard for security

[Government Functional Standard - GovS 007: Security](#) sets the expectations for protecting the government's people, information and assets. In respect of personnel security, it states that government organisations **SHALL** deliver the

appropriate combination of recruitment checks, vetting and on-going personnel security aftercare to reduce the risk from insider threat. Furthermore, GovS 007 states that government organisations **SHALL** have:

A process in place which defines the approach to handling the refusal or withdrawal of clearances for both candidates at the recruitment stage and those already in employment.

Data sharing

As part of the processing of the appeal, there may be circumstances which require the Appeal Team to discuss aspects of the case with third parties. The team always balances the need to limit the disclosure of sensitive information with the need to progress the case with individuals or departments that are crucial to obtaining a fair and balanced appeal process.

In doing so the team always seeks consent from the individual to share data, subject to national security considerations.

As an example, the MoJ employs a Senior Security Advisor (SSA) who liaises with the Security Unit on behalf of the Permanent Secretary.

The SSA provides information to the Security Unit concerning the role in the MoJ for which security clearance is being sought, thereby identifying the level of risk inherent in employing an individual to that post. The SSA is therefore involved in the national security vetting process in an advisory capacity and is made aware of concerns raised by the Security Unit in the course of that process which might result in a clearance being refused or withdrawn.

The SSA also acts as liaison between the Appeals Team and the MoJ throughout the appeal process.

Upon completion of this process, the Head of Vetting Appeals provides a full report and recommendation to the Permanent Secretary. The SSA is invited to view this report before submission.

The final decision to uphold the appeal or the decision to refuse or withdraw is made by the Permanent Secretary and communicated direct to the appellant.

Note: The appellant is defined as the individual who has had their security clearance refused or withdrawn, and wishes to appeal this decision.

Where necessary, data **CAN** also be shared with the appellant's line manager, or the originator of material gathered in the course of national security vetting which has a bearing on the decision to refuse or withdraw clearance. In so doing, consent is always sought from the individual to share data, subject to considerations of national security.

Contacts

For general advice or guidance regarding the National Security Vetting process, contact [MoJ Group Security](#).

To declare relevant changes in your personal circumstances, contact the Cluster 2 Personnel Risk Management Team by emailing VettingAftercare@cluster2security.gov.uk.

Annex A: Cluster 2 Security Unit Security Clearance Appeals Procedures

Internal appeals

Enclosed with the vetting decision letter to refuse or withdraw CTC (Counter Terrorist Check), SC (Security Check) or DV (Developed Vetting) security clearance **SHOULD** be the appeal documents comprising:

- An explanation of the internal vetting appeals policy and process and of the entitlement, should that appeal fail, to appeal to the independent Security Vetting Appeals Panel (SVAP).
- An internal appeal form ([Annex B](#)) to be completed by the individual, and guidance as to what is required of the individual when lodging an appeal, for example provision of any additional information, identification of the reason(s) for the appeal as well as any alleged 'inaccuracy' or 'misunderstanding' in the decision letter.

The vetting decision letter **SHOULD** also provide clear details of where the appeal notice **SHOULD** be sent.

Appeals **SHALL** be made by the appellant and sent to the Permanent Secretary using the "Internal appeal form following refusal or withdrawal of security clearance" ([Annex B](#)) within 15 working days of receiving the vetting decision.

In lodging an appeal, the appellant **SHOULD** provide as full a rationale as they able, based on the reasons provided in the decision letter, with supporting facts where applicable and including any further information or documentation that **MIGHT** assist their appeal. An appeal submission **MIGHT** include information that was not previously available when the original clearance decision was made, where this information is materially relevant to the case.

On receipt of an appeal, the Permanent Secretary **CAN** delegate the handling of it to an appeal officer, usually the Head of Vetting Appeals in the Cluster 2 Security Unit. The appeal officer is independent: they **SHALL NOT** have had any prior involvement or interest in the original decision-making process. The Permanent Secretary reserves the right to hear an appeal internally at their home department in any circumstances if they consider it appropriate.

The Senior Security Advisor (SSA) of the MoJ acts as liaison between the Appeals Team and their department throughout the appeal process. The appeal officer conducts the appeal on behalf of the Permanent Secretary and provides a report and recommendation to the Permanent Secretary. In all cases, the Permanent Secretary makes the final decision.

The appeal officer conducts the internal appeal according to the following guidelines:

1. They contact the appellant within 5 working days of being delegated to handle the appeal. The appeal officer introduces themselves and provide contact details for the appellant, along with an explanation of the next steps in the appeal process.
2. The appeal officer provides the vetting decision maker (usually either the Head of Vetting Decisions or the Head of Personnel Risk Management, or their representative) with the appellant's grounds of appeal and invites them to provide a statement of case and response to the appellant's representations. They are also asked to provide all documents relevant to the decision and the processes involved.
3. On receipt of the decision maker's statement of case and supporting documentation, an appeal bundle is prepared and sent to the appellant, who is allowed a minimum 10 working days to prepare their response based on the contents of the bundle and their own representations.
4. The appeal officer usually invites the appellant to present their case in person at an appeal hearing. Where this is agreed, the appellant is expected to make themselves available for the hearing as directed. If the appellant chooses not to attend the hearing in person, the appeal is considered on papers alone. If the appellant fails to agree a date for the hearing within six weeks of receiving their papers, or fails to attend the agreed hearing without good reason, a further date is set. If the appellant does not attend, the appeal is considered on papers alone.
5. Where appropriate, and with the agreement of the appellant, the appeal hearing **CAN** be conducted via Skype or another secure communications facility. In such circumstances, those attending **SHALL** ensure the appropriate levels of security and privacy are in place for the duration of the hearing.
6. At the appeal hearing, the appellant **MAY** be accompanied by a work colleague from their respective organisation, who may be a trade union representative. Their role is confined to helping the appellant present their representations. They **SHALL NOT** answer questions directly on the appellant's behalf. Formal legal representation is not permitted. If there are any special requirements that the appeal officer needs to be aware of, this **SHOULD** be drawn to their attention in advance of the hearing so that necessary arrangements can be made.
7. The appellant **SHOULD** be provided with a written record of the hearing within 5 working days of the hearing taking place, to allow for their comments and to confirm or dispute the accuracy of the record. In the case of a dispute, both records should be retained.
8. If the appeal officer requires any further information during the appeals process, they **CAN** request this from either party at any time.
9. The appeal officer provides a report and recommendation to the Permanent Secretary within 15 working days of all enquiries being completed.
10. Where, for operational or management reasons, any of the previous timescales cannot be met, the appellant **SHOULD** be notified and, where possible, a revised timescale **SHOULD** be set. Similarly, where the appellant is unable to meet the timescales, the appeal officer **SHOULD** be notified and, where possible, a revised timescale **CAN** be agreed.

On receipt of the report, the Permanent Secretary is responsible for making the final decision. In reaching a final decision, they **SHOULD** consider:

- The statement of HMG personnel security and national security vetting policy, consideration of the interests of national security and the rights and interests of the individual.
- The merits of the original decision and the adequacy of the decision-making process.

- The appellant's grounds of appeal.

The Permanent Secretary informs the appellant of the outcome of their appeal in writing, giving the full reasons for their decision, related to the relevant facts, unless considerations of national security and confidentiality prohibit this. Where an appeal is rejected, the appellant is informed of their further right of external appeal to the Security Vetting Appeals Panel (SVAP). This concludes the internal appeal process.

External appeals

If an individual wishes to appeal against the outcome of the internal appeal, they **CAN** write to the Security Vetting Appeals Panel (SVAP), an independent advisory body which provides a final means of challenging a decision to refuse or withdraw a national security vetting clearance once an internal appeal has been dismissed. In such circumstances, the appellant is advised that if they wish to exercise a further right of appeal to SVAP, they **SHALL** notify the SVAP secretariat within 28 days of the decision of the internal appeal and provide contact details.

The SVAP is available to hear appeals from individuals in government departments and other organisations, or contractors' employees working for those departments and organisations, who have exhausted the internal appeals process and remain dissatisfied with the outcome. It is convened to hear cases as they arise, and consists of a Chairman and two members. The Chairman (and Deputy Chairman) is a senior member of the judiciary.

The SSA **MIGHT** be required to attend the SVAP hearing as well as the appeal officer.

The SVAP makes recommendations to the Head of Organisation in the light of its findings. It can recommend either:

- That the decision to refuse or withdraw security clearance **SHOULD** stand.
- That security clearance should be granted or restored.

The SVAP **CAN** also comment on the vetting procedures and the adequacy of the internal appeals process and make recommendations. The Permanent Secretary takes the final decision on whether to accept any recommendations to grant or restore a security clearance. Depending on the SVAP's findings, which are not binding, the Permanent Secretary **MIGHT** choose to consult with Cluster 2 Security Unit regarding next steps.

Annex B: Internal appeal form following refusal or withdrawal of security clearance

The Internal Appeal Form is available for download [here](#).

Who should complete this form?

This form should be completed by individuals engaged in work for the MoJ who:

1. Have had their security clearance refused or withdrawn; and
2. Have a right to appeal this decision.

If you are not sure that you have a right to appeal, refer to the Vetting Appeals Guidance.

Where should the form be sent?

Send completed forms to the Permanent Secretary, at the address provided to you in the letter which formally notified that your security clearance was refused or withdrawn. Appeals submitted by a third party on your behalf are not accepted.

PART A: Your details

Surname:

Forename(s):

Date of Birth:

Your current home address:

Any temporary address:

Contact telephone number:

Email address (for correspondence):

Department / Organisation:

Job title:

Please confirm you are content to receive correspondence by email at the email address you have provided here:

YES / NO

If no, please let us know where you would like correspondence sent?

Are you appealing against refusal or withdrawal of your security clearance?

YES / NO

If yes, what levels of security clearance were refused or withdrawn?

Do you wish to present your case in person at an appeal hearing?

YES / NO

Do you wish to be accompanied at the hearing by a member of staff or TUS representative?

YES / NO

If yes, please provide details of the individual who will accompany you:

PART B: Details of your appeal

For your appeal, you **SHOULD** provide a full rationale, with supporting facts if necessary, and include any information or documentation that **MIGHT** assist your appeal. Typically, an appeal submission **MIGHT** include information that was not previously available when the original clearance decision was made, where this information is materially relevant to your case. Use a continuation sheet if necessary.

PART C: Declaration

I declare the information given here is true and complete to the best of my knowledge and belief.

Signature of appellant:

Annex C: Framework of staff legal obligations in relation to HMG and Home Office material Official Secrets Act

The Home Office **SHALL** adhere to the Official Secrets Act 1989 which came into force in 1990. It replaced section 2 of the Official Secrets Act 1911, under which it was a criminal offence to disclose any official information without lawful authority. Under the 1989 act, it is an offence to disclose official information. The act applies to:

- Crown servants, including Government ministers.
- Civil servants, including members of the Diplomatic Service.
- Members of the armed forces.
- The police.
- Government contractors, including anyone who is not a Crown servant but who provides or is employed in the provision of goods or services for the purposes of a minister.

Data Protection Act 2018 and UK General Data Protection Regulations

The handling of personal data must comply with UK Data Protection legislation. Departments and agencies should also have regard to UK Data Protection legislation, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

Freedom of Information Act 2000

Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOI) may apply. However, each FOI request **SHALL** be considered on its own merits as the classification is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

Public Records Act 1967

Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

Contact details

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

Security vetting assessment of need

This form should be completed by a line manager or contract manager. Completion of this form allows Ministry of Justice (MoJ) Group Security to determine the correct level of National Security Clearance.

The assessment of need document is available [here](#).

Contact details

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

During employment

Ongoing Personnel Security

Security clearance is a snap-shot of an individual at the time they make their application. Therefore, it is essential that employees are proactively managed using effective ongoing personnel management processes.

When staff are inducted, they are advised of their security responsibilities. Line managers also have a key role in ensuring the security of the department, including personnel security of the people they manage. This is best achieved by following the guidance in this document.

Line Manager Responsibilities

- Brief your staff, including contractors, on local and departmental security arrangements and policies as part of their induction.
- Get to know your staff, including contractors who might only be employed for a temporary basis. This is so you can recognise any changes in their behaviour which might impact on the security of the organisation.
- Do not ignore any concerns you have for fear of not knowing what to do. Refer to the information in this guidance for further details.
- Where appropriate, deal with any concerns by talking to the individual, your manager, or HR.
- Create a positive climate in which security is given priority, and individuals are encouraged to discuss any concerns before they become security problems.
- Be a good role model for all your staff, and display good security behaviours.

vetting, and on-going personnel security management. This allows them to be assured about their people and to mitigate risks from well-placed insiders.

Policy Statement

To achieve this security outcome, the following **SHALL** be followed by the MoJ.

- Determine the need for voluntary drug testing using a threat and risk management approach, based on evidence supplied throughout the National Security Vetting (NSV) process.
- Individuals **SHOULD** co-operate fully with any request to provide a voluntary sample collection for drug testing.
- Confirmation of test results, and any subsequent decision making made, **SHALL** be held on the individual's vetting file, and stored in accordance with the organisation's retention periods.
- Test results **SHALL NOT** be used for any other purpose than deciding suitability to hold NSV. Exceptions to this include legal obligations (for example Court order, or Police warrant), or the transfer of records to another Vetting Authority, as part of clearance confirmation procedures, or where there is an overriding corporate duty of care to the vetting subject.
- Any new information or concerns affecting the reliability of an individual **SHALL** be reported to, and dealt with by, [MoJ Group Security](#), in conjunction with the Senior Security Advisor.

Voluntary drug testing policy procedures

Introduction

The Cluster 2 Security Unit (C2SU) forms part of the Transforming Government Security programme which aims to standardise and strengthen operational security across Government.

Cluster 2 is one of four cross-Government Security Clusters which delivers operational security services to the following Government organisations:

- Home Office
- DEFRA
- Department for Education
- Department for Transport
- Ministry of Justice (MoJ)
- Ministry for Housing, Communities, and Local Government

The MoJ Senior Security Advisor (SSA) is responsible for the overall management of security and for ensuring that the Cluster services and policies provided meet Government and organisational aims for improved security in Government.

If you have any queries about this information, contact [MoJ Group Security](#).

Procedures

These policy procedures support and underpin the [Voluntary Drug Testing Policy](#). Unless otherwise noted, these procedures **SHALL** be complied with fully.

Aftercare arrangements: Use of Voluntary Drug Testing

A security clearance requires ongoing review. A voluntary drugs test is one of a range of vetting aftercare arrangements which provides assurance and confirms that staff are suitable for ongoing access to sensitive government information and assets. Drug testing is a voluntary process which enables security clearances to be assessed and granted in cases where they would ordinarily be refused.

Voluntary drug testing is used when illegal drug use is admitted to during the vetting process.

C2SU decide on a case-by-case basis whether drug testing is necessary. C2SU also identify any potential security risks to Government assets in consultation with the MoJ Senior Security Advisor. In any event, the individual must commit to not using any type of illegal drugs during any period of employment with the MoJ.

Drug testing arrangements

C2SU set a timeframe in which an individual will be periodically tested for a panel of illegal drugs by an accredited and approved drug testing provider.

Disclosure of personal information

Personal information needs to be disclosed to the approved drug testing provider to support the administration of the drug testing process. By agreeing to take part in the voluntary drug test, the individual is subsequently consenting to the following personal information being provided:

- Full name.
- Date of birth.
- Place of work (for example, MoJ).
- Declaration of illegal drug use both historic and current (including type of drug(s), frequency, and quantity).
- Declaration of controlled substances both historic and current (for example, prescription medications).
- Other medical history required to help safely facilitate the drug testing process.

This information is used only for the purposes of facilitating the drug testing process.

Sample collection

The primary method for the sample collection is a hair sample. However, in some circumstances other alternative methods, such as a urine sample, may be used for drug testing analysis. At each drug test an alternative hair or urine sample is taken to allow for independent re-testing, if required (for example if a test result is inconclusive or further evidential testing is required).

The individual is expected to co-operate fully with any request to provide a sample collection. If the initial request cannot be met due to availability issues, such as pre-arranged annual leave commitments, the individual must arrange as soon as possible with the C2SU's drug testing provider, and no later than five working days after the unavailable period, to provide a sample collection for drug testing analysis.

If, due to a change of circumstances beyond the individual's control, they are unable to attend the scheduled appointment, they must give advanced notice (minimum of 24 hours) and reason(s) for non-attendance to C2SU and the drug testing provider. The appointment must be rescheduled within seven days of the original appointment date.

Failure to either provide advanced notice to C2SU and the drug testing provider, or reschedule the original appointment date within the set timeframe, is interpreted as the individual's unilateral withdrawal from the vetting aftercare arrangements, and could lead to withdrawal of the security clearance.

Failure to co-operate with any part of the drug testing process, or if C2SU has reason to believe that deliberate attempts by the individual are being made to delay, frustrate, or circumvent the process, is interpreted as the individual's unilateral withdrawal from the national security vetting aftercare arrangements and could lead to the withdrawal of the security clearance.

Raising concerns

Any concerns about the sample collection process, or about the approved drug testing provider, must be raised with C2SU at once and in any event prior to receiving confirmation of drug testing results. C2SU investigates any concerns raised with the approved drug testing provider.

Confirmation of test results

Confirmation of test results is provided in full to the individual, and shared in their entirety with the Cluster 2 Aftercare Security Unit.

Any positive trace of illegal drugs is grounds for assessing the individual's suitability to hold security clearance. The level of security clearance withdrawn is decided by C2SU on a case-by-case basis.

Confirmation of test results, and any subsequent decision making made by C2SU, is held on the individual's vetting file and stored in accordance with C2SU retention periods.

The test results are not be used for any purpose other than deciding on suitability to hold national security vetting. Exceptions to this include legal obligations (for example court order or police warrant), or the transfer of records to

another Vetting Authority as part of clearance confirmation procedures, or where there is an overriding corporate duty of care to the vetting subject.

Self-reporting

Following the Cluster 2 department's Drugs and Alcohol Substance Policy, or equivalent, individuals misusing substances are encouraged to discuss this with their line manager and urged to seek expert help and advice at the earliest opportunity.

Additionally, holders of national security vetting clearance at all levels are expected to show the highest level of honesty, integrity, transparency, openness, and frankness in sharing personal information (including lifestyle habits, and changes to them) of security relevance, or when engaging with C2SU. Dishonesty and intent to mislead or conceal is viewed seriously and influences whether the clearance is kept.

All information shared with C2SU is treated in confidence. Support is provided where possible.

Self-reporting of any drug misuse is not necessarily considered as automatic grounds for the withdrawal of security clearance. C2SU assess everyone on a case-by-case basis. However, failure to self-report drug misuse which later comes to light via drug testing, or any other means, is likely to lead to security clearance being withdrawn.

The following contributing factors are considered by C2SU. This is not an exhaustive list:

- The type and quantity of illegal drug usage.
- Previous history of the misuse of illegal drugs.
- How long since the previous declaration of illegal drugs use.
- How the illegal substances were acquired.
- The environment in which the illegal drug use took place.

C2SU assess an individual's suitability to continue to hold security clearance by deciding the level of risk they have of being susceptible to pressure or improper influence, or indicate unreliability, because of their actions. The principles around national security vetting focus specifically on the threats posed to UK national security (for example terrorism, espionage, or other actions that would threaten the UK). The threats and any subsequent risks to the business might differ, so they are assessed and managed by locally produced business-related policy and procedures.

Appealing decisions of withdrawing security clearance

If a security clearance is withdrawn following a positive test result, the appeal rights and processes are the same as for withdrawal or refusal of national security vetting clearance for any other reason. Any appeal is dealt with following the terms of the Security Clearance Appeals Procedure. These state that Right of Appeal applies to those falling under these criteria:

- Permanent members of MoJ staff.
- Current contractors or other non-permanent staff, already engaged in MoJ work.
- Current permanent members of staff of other government departments and organisations who have applied for or transferred a security clearance with the MoJ.
- Current contractors already engaged on government work in other departments and organisations who have applied for or transferred a security clearance with the MoJ.

There is no Right of Appeal for individuals on recruitment to the Civil Service seeking employment or contractual work with the MoJ. For further information on the Security Clearance Appeals Procedure, contact Group Security: mojgroupsecurity@justice.gov.uk.

Appealing a positive drug test

Any disputed drug test **SHALL** be appealed to C2SU, in writing, within five days of receiving confirmation of a test result.

An appeal **SHALL** detail the reason or reasons why the positive result is being disputed. This information **SHALL** be shared with the approved drug testing provider and the positive test results **SHALL** be subject to further scientific expert analysis to decide the probability of the positive test result being incorrect. The results of any secondary testing **SHALL** be treated as final.

Review of drug testing arrangements

The requirement for drug testing individual cases **SHALL** be subject to ongoing review, on a case-by-case basis, by C2SU. The individual **SHALL** be formally notified by C2SU if this aftercare arrangement is withdrawn.

Termination and change of employment

End or change of employment

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

If the leaver has security clearance, managers should contact the [Cluster 2 Security Unit](#) to advise that the person has resigned and tell them their leaving date or the date on which they will be moving to a different department.

Leavers should read the HR guidance at [End or change employment](#).

Managers must also [complete a leaver's checklist](#) as a record of actions.

Downloads

[Leavers checklist](#)

A downloadable version of the "End or change of employment" document is available [here](#).

Contact details

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

Leavers with NSC and NSVCs

This information applies to people leaving the Ministry of Justice (MoJ), who have National Security Vetting (NSV), or who are National Security Vetting Contacts (NSVCs).

Staff or contractors that hold clearance of any level **SHALL** attend an exit interview with their manager before they leave the MoJ. Although these interviews are available for all staff, they are compulsory for those with Counter Terrorist Clearance (CTC) or Security Check (SC).

If the leaver holds Developed Vetting (DV) or SC enhanced level, and has been STRAP inducted, they **SHALL** attend a mandatory STRAP debriefing interview with [Cluster 2 STRAP team](#). They **SHALL** also sign a confidentiality agreement and a "Declaration of Cessation of TOP SECRET STRAP Access".

NSVCs who leave

The post of National Security Vetting Contact (NSVC) **SHOULD NOT** be left empty. NSVCs **SHOULD** work with [MoJ Group Security](#) to ensure that a replacement has been selected, and trained, to take over once they have left.

Manager responsibilities

When a member of staff with clearance leaves their department, the manager **SHALL** inform their NSVC, so that the NSVC can update their records and remove the staff member from the list of cleared personnel. The NSVC passes the leaver's details on to [Cluster 2 Security Unit](#). Managers **SHOULD** also use this as an opportunity to take another look at the role, and confirm whether it still needs clearance and, if it does, to what level. The NSVC can advise managers on this analysis.

Downloads

- [National Security Vetting Contact Guide](#).
- [National Security Vetting Contact Register](#).
- [National Security Vetting Assessment of Need](#).

Related information

- [End or change employment.](#)

Contact details

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

Asset management

Responsibility for assets

Acceptable use of Information Technology at work

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

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

Related information

[Email blocking policy](#) on page 342

Summary

Be sensible when using MoJ IT resources:

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

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

What is meant by IT?

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

Acceptable use of MoJ IT

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

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

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

Unacceptable use of MoJ IT

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

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

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

Why unacceptable use is a problem

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

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

Unacceptable use might also affect you, too:

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

Keeping control

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

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

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

While you might be careful about acceptable use of MoJ IT, there are still risks from [malware](#), [ransomware](#), or [phishing](#) attacks.

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

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

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

Personal use of MoJ IT

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

Personal use of MoJ mobile phones

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

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

This usage must always be for work purposes.

Examples of unacceptable MoJ mobile phone use include:

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

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

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

Using MoJ IT outside your usual workplace

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

You should also [ask](#) before taking MoJ IT equipment outside the UK.

Avoid using removable media

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

Personalisation of equipment

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

Contact details

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

Acceptable Use Policy

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

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

Related information

[Technical Controls Policy](#) on page 36

Introduction

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

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

Scope

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

Failure to adhere to this policy **MIGHT** result in:

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

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

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

Protection of assets

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

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

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

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

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

POL.ITAUP.005: All Users **SHALL** be made aware that non-conformance to the system SyOPs constitutes a breach of the MoJ [IT Security Policy](#), and **MIGHT** result in disciplinary action.

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

POL.ITAUP.007: Any request to perform an action on an IT system which contravenes its SyOPs **SHALL** be approved by the [Cyber Assistance Team](#) and the [Operational Security Team](#), or the MoJ Chief Information Security Officer (CISO), before the action is taken.

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

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

Reviewing access to data and information systems

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

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

When to remove access and return assets

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

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

How to remove access and return assets

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

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

Contact details

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

Protect yourself online

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

1. Use a strong password to protect your laptop, computer and mobile devices. To choose a good password, follow [NCSC guidance](#).
2. Think before clicking on links or attachments within emails. By hovering your cursor over the link you can find the actual URL. If you are unsure if an email is genuine, [contact your IT or security team](#).
3. Do not use your work email address to register for accounts on websites for personal use. For example, a shopping website does not need your work email address. Using the wrong address could open up your work email account to spam and fraudulent emails. This in turn could harm your department's IT system.

Note: This document provides guidance for handling and sharing of information and data up to and including OFFICIAL and OFFICIAL-SENSITIVE, or the older Impact Level (IL) 3. Where information attracts a high protective marking or IL, advice **SHALL** be sought from the MoJ [Operational Security Team](#) and the MoJ Chief Information Security Officer (CISO).

Demonstration of Compliance

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

Handling data on MoJ IT systems

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

- Data in transit.
- Data at rest.

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

Ownership of information

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

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

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

Electronic data transfer and storage

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

Data in transit

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

Secure network (system-to-system electronic transfer)

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

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

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

- the most urgent cases, seek approval from your manager or the Information Asset Owner before adopting lesser controls. Decisions must be risk based, and the assessment must be recorded at the earliest convenient opportunity.
- Existing material with former protective markings including UNCLASSIFIED, PROTECT, and RESTRICTED does not need to be retrospectively reclassified. See the [transition note](#) in this guidance.
 - Descriptors, such as PERSONAL or COMMERCIAL are no longer used. In exceptional circumstances or where the recipient might not recognise the sensitivity of the information being sent, authors may include 'handling instructions' in a document or email to draw attention to particular requirements.
 - The security officer for your part of the MoJ should be consulted to agree controls if you receive, handle or otherwise process any information at SECRET or TOP SECRET.

Controls

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

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

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

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

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

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

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

Marking of information

Marking is only needed for information which is OFFICIAL-SENSITIVE, SECRET or TOP SECRET.

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

This could mean:

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

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

Transition to the classification system

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

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

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

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

Classification	Description
SECRET	Very sensitive information that requires protection against highly sophisticated, well-resourced, and determined threat actors. For example, where compromise could seriously damage military capabilities, international relations, or the investigation of a serious crime. For regular, unsupervised access to SECRET information, someone would be expected to have passed National Security Vetting Security Check (SC) clearance. In exceptional circumstances, someone with BPSS might be granted occasional supervised access to UK SECRET assets, or be required to work in areas where SECRET or TOP SECRET information might be overheard.
TOP SECRET	Exceptionally sensitive information that directly supports, or threatens, the national security of the UK or its allies, and requires extremely high assurance of protection from all threats.

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

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

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

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

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

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

Classification	Definition	Marking
OFFICIAL	All information related to routine public sector business, operations and services. Almost all personal information falls within the OFFICIAL classification.	

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

Additional information on how to manage information is described in the [Information Asset Management Policy](#).

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

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

- Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.
- Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.
- Incorrect disposal can lead to unauthorised access to information. Disposal of information should be done using approved processes, equipment or service providers. Refer to the [MoJ Data Destruction guide](#) to understand when the disposal should be witnessed and recorded.

OFFICIAL and OFFICIAL-SENSITIVE

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

Examples include:

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

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

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

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

SECRET

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

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

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

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

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

TOP SECRET

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

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

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

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

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

Reclassifying information

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

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

Reclassification examples

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

Example 1

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

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

Example 2

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

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

The original report retains its **OFFICIAL** classification and **SENSITIVE** handling caveat.

Example 3

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

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

Handling and securing information

The [HMG Government Security Classifications Policy](#) is the most comprehensive guide on the security measures necessary for each of the three security classifications, including measures related to the following:

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

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

Handling and securing OFFICIAL and OFFICIAL-SENSITIVE information

Type	Measure	Example
PERSONNEL	Make sure all MoJ staff including contractors undergo baseline security clearance checks.	A contractor working with the MoJ Security Team must undergo a baseline background check (i.e. BPSS check) at minimum. Refer to Security Vetting Guidance .
PHYSICAL	<p>Make sure that you lock your screen before you leave your desk.</p> <p>When working in an unsecured area, for example when working remotely, think about whether unauthorised people might be able to eavesdrop on your conversations, or look over your shoulder at your screen.</p> <p>The MoJ has additional requirements when moving assets which can be found in the HMG Government Security Classifications Policy.</p> <p>Transferring information from one location to another requires planning and preparation, including a risk assessment. More information on this is available in the HMG Government Security Classifications Policy, and from your manager.</p>	<p>A software developer working from a flatshare should take calls in private, and use headphones and a privacy screen.</p> <p>A technical architect working on the requirements for a new MoJ platform should lock their laptop before leaving their desk.</p>

Type	Measure	Example
TECHNICAL	<p>Protect information "at rest" by using appropriate encryption.</p> <p>Appropriate encryption is also necessary when protecting information in transit.</p> <p>Digital Marketplace (GCloud) services can be used for OFFICIAL information.</p> <p>You must not use removable media such as an USB memory stick unless it is unavoidable. When you have to use one, it must be MoJ issued, encrypted so that the effects of losing it are minimised, and the data erased securely after use.</p>	<p>In the development of a new cloud-hosted solution, the following criteria should be considered: remote access connections and sessions are encrypted using an appropriate VPN; information stored "at rest" on end user devices and the cloud is encrypted; information in transit between the end user and the cloud service, such as payment services, is encrypted; and the cloud service used is a Digital Marketplace (GCloud) service.</p> <p>When using any services over the PSN, make sure you fully read the agreements that you make with the service provider for details and definitions about the data you use or transfer using the service, to ensure you understand the risks to compliance, confidentiality, integrity, and availability.</p>

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](#) for further guidance.

Handling and securing **SECRET** information

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

Sending documents

Options for sending documents are covered in the Sending Information guidance note.

Disposing of paper information

MoJ offices have bins or bags that are specifically intended for secure waste disposal of documents or files, including:

- Personal information that relates to an identifiable individual or individuals.
- Sensitive information that **SHOULD NOT** be disclosed.
- Any material bearing a visible classification marking.

POLPPR015: You **SHOULD** read and follow the [secure waste disposal](#) guidance on the MoJ Intranet before disposing of any document or files.

POLPPR016: Before disposing of information, you **SHOULD** check whether it should be retained on a file, and whether it is covered by a 'retention schedule'. The [Records and Retention team](#) can advise on this.

Long-term storage

The MoJ has arrangements for the secure long-term storage of paper documents and files. If you want to keep paper-based information, but no longer need to regular access to it, refer to the information on the MoJ Intranet regarding [keeping, deleting, and disclosing information](#). The [Records and Retention team](#) can provide additional guidance.

What to do if you think there has been a security breach

POLPPR017: If you suspect that the security of the information you work with has been compromised in any way, you **SHALL** [report it immediately](#).

Note: A security breach does not have to involve the actual loss of information. The potential loss of information also counts. For example, if a security cabinet has been left unsecured, there may be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

POLPPR018: The level of risk and potential impact to MoJ assets, and, most importantly, physical harm to our people and the public, determines the controls to be applied and the degree of assurance required. The MoJ **SHALL** ensure a baseline of physical security measures are in place at each site, and receive annual assurance that measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, such as in response to a security incident or change in the Government Response Level.

POLPPR019: The implementation of all security measures **SHALL** be able to provide evidence that the selection was made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI), and [Government Functional Standard - GovS 007: Security](#).

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards is subject to annual review or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting [MoJ Group Security](#).

Contact details

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

Contact the Privacy Team for information on Data Protection Impact Assessments: privacy@justice.gov.uk

If you are not sure who to contact, ask the Operational Security Team:

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

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

Access Control Policy

This policy gives an overview of access control security principles and responsibilities within the Ministry of Justice (MoJ). It provides a summary of the policies and guides that apply to MoJ access management.

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

Related information

[Technical Controls Policy](#) on page 36

Audience

This policy is aimed at:

Technical users

These are in-house MoJ Digital and Technology staff responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.

Service Providers

Defined as any other MoJ business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data), for or on behalf of the MoJ.

General users

All other staff working for the MoJ.

"All MoJ users" refers to General users, Technical users, and Service Providers, as defined previously.

Policy Sections

This policy aligns to industry standards and frameworks, and is divided into four security categories (and subsections describing the controls) addressing:

1. Business Requirements of Access Controls.
2. System and Application Access Controls.
3. User Access Management.
4. User Responsibilities.

Best Practice Framework - IAAA

Identification, Authentication, Authorisation, and Accounting (IAAA) are the core principles of an Access Control Policy. The principles apply to all security categories described in this policy, as follows:

Identification

POLACP001 : The MoJ **SHALL** provide a unique ID that is assigned, named, and linked to a private account, for each user.

Authentication	POLACP002 : To access MoJ systems, users SHALL authenticate themselves.
Authorisation	POLACP003 : Specifying access rights, privileges, and resources to users SHALL be granted in line with the principle of least privilege.
Accounting	POLACP004 : Successful and unsuccessful attempts to access systems and user activities conducted while using systems SHALL be recorded in logs.

Note: If any of the controls within this policy cannot be applied, they are considered an exception to be assessed for inclusion within a risk register.

Business Requirements of Access Control

The MoJ's business or strategic requirements limit access to MoJ information and information processing facilities, as described in the following subsections.

Access Control Policy

POLACP005 : This access control policy **SHALL** be established and maintained, based on business and information security requirements, to inform associated standards and guidance, for all users.

POLACP006 : The policy **SHALL** also follow the additional principles of:

- "Need-to-know".
- Non-repudiation of user actions.
- Least privilege.
- User access management.

Access to Networks and network services

This subsection aligns to the principle of least access, to protect a network and network services which are covered in other areas of this policy, specifically:

- Authorisation procedures for showing who (role-based) is allowed to access what, and when. Refer to subsections [Information Access Restrictions](#) and [Management of Privileged Access Rights](#).
- Management controls and procedures to prevent access and real-time monitoring. Refer to the categories called [System and Application Access Control](#) and [User Access Management](#), with monitoring covered in the subsections called [Password Management System](#) and [Management of Privileged Access Rights](#).

System and Application Access Control

POLACP007 : The MoJ **SHALL** strive to prevent unauthorised access to systems and applications, as described in the following subsections.

Information Access Restrictions

POLACP008 : Access to information and application system functions **SHALL** be restricted by following access control policies and procedures.

POLACP009 : In particular, System Designers and Administrators **SHALL** use adequate authentication techniques to identify with confidence user access to their system or data, using the principle of "least privilege". Refer to the guidance on [Authorisation](#) for more detail.

Secure Log-on Procedures

POLACP010 : Where required by the access control policy, access to systems and applications **SHALL** be controlled by a secure log-on procedure, including the following points:

- POLACP011 : Multi-user (MU) accounts **SHALL** be managed carefully using PAM or a Bastion server, to avoid accountability type security risks. Refer to the [Multi-user Accounts and Public-Facing Service Accounts](#) guidance.

- POLACP012 : Front-end users accessing the MoJ's public services **SHALL** authenticate via the GOV.UK Verify Service. Refer to the [User Facing Services](#) guidance.
- POLACP013 : System Designers for internal systems **SHALL** use the MoJ's single sign-on (SSO) solution to authenticate via an Identity and Access system.
- POLACP014 : Passwords **SHALL NOT** be stored or transmitted over the network in clear text, nor be protected with encryption that has known security weaknesses. Refer to the [Password Management Guide](#).

Password Management System

POLACP015 : The MoJ's password management systems **SHALL** be interactive, ensure quality passwords are used, and **SHALL** store and transmit passwords in a protected form, specifically:

- POLACP016 : Systems **SHALL** support MoJ password requirements that are provisioned and maintained by System Administrators.
- POLACP017 : System Administrators **SHALL** always have time-bound administrative sessions, which **SHALL** be protected using [Multi-Factor Authentication \(MFA\)](#).
- POLACP018 : The system **SHALL** regularly monitor, review, and revoke these sessions when no longer required.
- POLACP019 : Strong passwords, separate and unique for each account or service, **SHALL** be created and maintained by all users. Refer to the [Password Management Guide, Roles and Responsibilities section](#), [Passwords](#) and [CyberAware advice](#).
- POLACP020 : Users **SHALL** change a password initially received by a system or support team before carrying out MoJ tasks. Refer to [Passwords](#).
- POLACP021 : Password history and blocking of commonly guessed passwords **SHALL** be enabled in a system. Refer to the [Password Creation and Authentication Guide](#).
- Regular password change is not required, as it is an [outdated and ineffective practice](#).
- POLACP022 : Password managers or vaults used at the MoJ **SHALL** align to industry standards to securely store and transmit passwords in a protected form. Refer to [Password Managers](#) and [Password Vaults and Managers](#).

Note: Contact the [Cyber Assistance Team](#) if you have specialised needs when selecting or using a storage tool.

Access Control to Program Source Code

- POLACP023 : When coding in the open, MoJ Technical users and Service Providers **SHALL** follow coding best practices and keep code separate from configuration and data.

User Access Management

User access management ensures authorised user access, and prevents unauthorised access to systems and services. These are described in the following subsections.

User Registration and de-registration

POLACP024 : A formal user registration and de-registration process **SHALL** be implemented to enable the assignment of access rights, specifically:

- POLACP025 : Multi-User (MU) or shared ID accounts **SHALL** only be used directly if there is no alternative. Refer to [Multi-user Accounts and Public-Facing Service Accounts](#).
- POLACP026 : The identity of the new user **SHALL** be confirmed. For all MoJ staff members, this is established as part of pre-employment screening and vetting using the Baseline Personnel Security Standard (BPSS), which is the joint responsibility of HR (performed on their behalf by Shared Services Connected Ltd), and a line manager. Refer to [Security Vetting](#) and the [BPSS](#) information.
- POLACP027 : The hiring line manager **SHALL** submit a ServiceNow [Order IT](#) role-based access request on behalf of the new user. For example, a list of Role-based access control (RBAC) groups or applications.
- POLACP028 : The hiring manager's line manager (or the budget holder) **SHALL** authorise the application for user registration within ServiceNow [My Approvals](#). This confirms the user's identity, and hence access rights, are correct.
- POLACP029 : Confirmation of the Clearance Level **SHALL** be initiated by a line manager, and carried out by [United Kingdom Security Vetting](#) (UKSV) to recruit new staff (civil servants, armed forces and temporary staff), or staff changing their MoJ roles. Refer to [Clearance Levels](#).

- POLACP048 : MFA **SHALL** be used with privileged accounts, including access to enterprise-level social media accounts.
- POLACP049 : Default passwords **SHALL** be managed securely and safely by privileged account users, described in the [Password Manager](#) guidance. Refer to the [Privileged Account Management](#) guidance for more information.
- POLACP050 : All users with ownership and use of privileged accounts **SHALL** have these secured, controlled, monitored, and audited by System Administrators every month using an industry-standard Privileged Access Management (PAM) tool. Refer to the [Privileged Account Management](#) guidance for more information.

Note: Privileged access rights provide a Technical user or a Service Provider with an enhanced level of access to the MoJ's information systems, compared to a General user. This can include the authorisation to configure networks or systems, provision and configure accounts and cloud instances, and so on.

Management of Secret Authentication Information of Users

POLACP051 : The allocation of secret authentication information, such as passwords or encryption keys, **SHALL** be controlled through formal management:

- POLACP052 : User password management **SHALL** be configured, so a password is changed after the initial log-on and invalid if not used in a specified time. Refer to the [Passwords](#) guidance.
- POLACP053 : System Administrators and systems **SHALL** never send passwords by email, as it is an unsecured channel.

POLACP054 : Instead, users **SHALL** receive a time-limited password-reset link or code to their registered email address or phone number. Refer to the Government guidance "[Send a link to trigger password resets](#)".

Review of User Access Rights

POLACP055 : System Administrators **SHALL** review users' access rights at regular intervals:

- The review of user access rights is covered in this policy under [User Access Provisioning](#).

Removal or Adjustment of Access Rights

POLACP056 : All employees and external party user's access rights to information and information processing facilities **SHALL** be removed upon termination of their employment, contract or agreement, or adjusted when changing their role:

- The removal or adjustment of user access rights is covered in this policy under [User Access Provisioning](#).

User Responsibilities

Users are required to follow the MoJ's practices in the use of secret authentication. This is described in the following subsection.

Use of secret authentication information

- POLACP057 : All users **SHALL** follow the MoJ's password policy, as referenced in the [Password Management System](#), and the associated tools referenced in the [Secure Log-on Procedures](#).

Enforcement

- This policy is enforced by lower-level policies, standards, procedures, and guidance.
- Non-conformance with this policy could result in disciplinary action per the department's disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they may also be prosecuted. In such cases, the department will always cooperate with the relevant authorities and provide appropriate evidence.

Incidents

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

Operational Security Team

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

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 b

Specific responsibilities of individual privileged users are likely to vary depending on the systems they manage. The system's Information Risk Assessment Report documents the security controls ([MoJ Information Assurance Framework Process](#)). The [IRAR](#) should be completed as part of this process. For a comprehensive list of individual responsibilities, privileged users should refer to the system specific documentation.

This page is the first in a series of guides for privileged users within the MoJ; refer also to the related guides.

Who is this for?

This guide is aimed at two audiences, both technical.

- 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.
- Any other MoJ business groups, Agencies, contractors, IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of, the MoJ.

Related guides

For further details about privileged user responsibilities, refer to the following guides.

- The [Privileged Account Management Guide](#) provides the guidelines to ensure that privileged accounts are securely managed. It is part of the [Access Control Guide](#).
- The [Logging and Protective Monitoring Guide](#) provides information about security procedures privileged users should implement to conduct logging activities.
- The [Backups, Removable Media and Incident Management Guide](#) provides information that privileged users should follow to reduce the impact of a security incident, and understand how they should respond.
- The [Configuration, Patching and Change Management Guide](#) provides privileged users with guidance to ensure that systems are configured securely, that change is managed correctly, and that systems are patched regularly.

Management of privileged user accounts

Privileged user accounts have a high degree of risk associated with them due to the control that they give the privileged user, hence they must be treated with great care. To reduce the risk of a data breach on the MoJ systems, access rights must be managed in the following ways.

- Privileged user accounts should only be created for users with a genuine business need, and only for the duration that the business need exists.
- Privileged access must be limited and granted in line with the principle of least privilege necessary to fulfil the required function.
- The privileged accounts should be strictly controlled, and their number kept to the absolute minimum per system or app.
- Privileged user passwords must be created in line with the MoJ's [Password Guide](#).
- The password for a privileged user account must not be re-used for another privileged user account or a normal user account.
- Privileged user passwords must be deleted along with the account when a privileged user leaves the MoJ or changes role.
- Multi Factor Authentication (MFA) must be used for privileged user accounts where possible. Refer to the [Password Guide](#) for further details.
- Privileged user accounts must only be used when carrying out administrative tasks such as creating new user accounts or implementing software updates. At all other times a normal user account must be used, e.g. for tasks such as searching the internet and reading emails.
- Privileged user accounts on depreciated systems must be reviewed quarterly by system owners for breach as aging systems frequently cannot be, or are not, patched leaving them vulnerable to take over.
- Privileged users must not abuse the privileges they are given, such as circumventing controls put in place to protect the MoJ.

For further information on managing privileged user accounts refer to the

Guidance for system specific privileged users:

- Where responsible for DOM1 systems, ensure backups are made to offsite locations such as to Dell EMC SANs in the MoJ off-site Ark and Ark-F data centres.
- Where responsible for Quantum systems, ensure backups are made to the redundant data centre.
- Where responsible for end user data, ensure data is not stored on or backed up to users' end devices but rather stored on OneDrive or Google Drive.

Incident management and response

Privileged users play a front-line role in detecting and responding to incidents. To ensure that they are prepared to respond to any incidents, privileged users should:

- Know and be able to implement the incident management plans and processes required for their systems. For instance, within HMPPS, privileged users should know that the HMPPS Incident Management function operates within the HMPPS Infosec and Service Team, and when they are to be contacted.
- Ensure that any system-specific incident management controls align with the [MoJ's IT Disaster Recovery Policy](#) and the [Incident Management Policy and Guide](#).

General enquiries, including theft and loss

Technology Service Desk - including DOM1/Quantum, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

Note: The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses, and the Digital & Technology Digital Service Desk Slack channel (#digitalservicedesk), are no longer being monitored.

HMPPS Information & security:

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

Incidents and contact details

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

For help with incidents, including theft and loss, contact:

Technology Service Desk - including DOM1, Quantum, and the Digital & Technology Service Desk

Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses are no longer being monitored.

HMPPS Information and security

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

For non-technology incidents, contact the MoJ Group Security Team: mojgroupsecurity@justice.gov.uk

Contact the Privacy Team for information on Data Protection Impact Assessments: privacy@justice.gov.uk

If you are not sure who to contact, ask the Operational Security Team:

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

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

For example, in WhatsApp, to prevent someone adding you to a group without your knowledge, change your settings: **Settings > Account > Privacy > Groups > My Contacts**. This change means that only people you know (your contacts) can add you to a group.

Limit access to your accounts

You might be tempted to share access to your social media account, for example if you want to have postings regularly, even while you are away.

Avoid sharing access to your social media account. It's easy to forget who the details are shared with. It's also possible that postings might be made on your behalf that you don't agree with, or are not acceptable.

Any MoJ social media accounts that do need to be shared will have proper access controls in place. You should never need to share your account details for work purposes.

If you need more help on this, contact your Line Manager or [Cyber Security](#).

Don't click on suspicious links

Unfortunately, social media postings are a common way of sending you links to malware or other problem material. Postings might also be used to send you 'phishing' attacks.

In the same way that you should be careful with any links or attachments sent to you using email, you should also be suspicious of links or attachments sent to you through social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

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

What to do if your account is bombarded

Remember that these attacks are short lived

Due to the amount of organisation and effort required to coordinate such an attack, they do not last long, and like an intense inferno, will soon burn themselves out.

Do not respond to the attack

These attacks are designed to attack the person controlling the account as well as the agency itself. By only responding to messages not involved in the attack - especially those trying to share positive messages, the attackers will run out of interest far sooner than if you engage them. If they are posting harmful or threatening messages, report the accounts.

In a single sentence - "don't feed the trolls".

Feel free to walk away

Dealing with these attacks can be emotionally draining; even just reading the messages can have a far greater impact on you than you realise. Take breaks in the event of an attack, even if it's hard to - consider going for a walk to force yourself away.

Cyber Security Advice

Cyber Consultants and Risk Advisors

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

System and application access control

Account management

Introduction

This guide provides help on account management, for example when passwords should be changed or when user accounts should be locked. For more information, refer to the [Password Management Guide](#).

The information is aimed at two audiences:

- The in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the [Event, Problem, Incident, CSI and Knowledge \(EPIC\) team](#).
- Any other Ministry of Justice (MoJ) business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the MoJ.

Account lockouts

Account lockouts must be implemented within MoJ systems for the following reasons:

Failure to change passwords within the allocated time.

Systems must have a "change password" function to recover the account or contact information for the IT Service Desk.

Unsuccessful connection attempts.

Allow no more than 10 consecutive login attempts before lockout.

Forgotten passwords.

All MoJ systems must have a forgotten password link on the login page, enabling the user to change the password on their own. Ensure this uses multi-factor authentication for user verification.

Removed or revoked access.

Users may experience account lockouts due to inactivity, need to know permissions or change of employment status such as contract termination. Access to these accounts must only be re-enabled with line manager approval.

Systems should have a way to forcibly revoke an account, and disconnect any active session instantly. This is to deal with scenarios such as suspicion that an account or access has been compromised. The session disconnect is required because revoking an account on some systems does not necessarily invalidate an existing session immediately.

Password changes

When designing and developing systems for use within the MoJ, password changes must be enforced for these events:

- A user has forgotten their password or is experiencing login issues.
- There has been a security incident involving the account or password.
- An authorised person, such as line manager or IT support, requests the change.
- The system prompts you to change a password.
- You suspect an account might have been compromised.

Password changes must be made within the following time frames:

Type of system	Maximum time allowed for a change
Single-user systems, such as laptops	1 week
All other systems	1 day

Revoking accounts

All MoJ user accounts are access controlled according to the user's 'need to know' requirements and their employment status. Accounts should be revoked at contract termination and during long-term absences, such as maternity or long-term sickness leave. The MoJ revokes user accounts in alignment with the [Access Control Guide](#).

Multi-user accounts

In this context, a multi-user account is where a single set of credentials is used by more than one person. This can be found on legacy systems where there is a dedicated administrator account. Multi-user accounts allow multiple users with individual logins and varying permissions to use the same account. Multi-user accounts need to be managed carefully using [Privileged Account Management](#) (PAM) or a Bastion server to avoid security risks associated with accountability. Multi-user accounts should only be used directly if there is no alternative.

Note: A [Bastion server](#) is a specially strengthened system that provides access to parts of the Ministry of Justice (MoJ) private network from an external network, such as the Internet. It provide specific access to to a well-defined set of servers or services, rather than permitting general access across the network.

The multi-user account checklist requires that you:

- Undertake a Business Impact Assessment (BIA) before implementation of a multi-user account to understand risks posed to the MoJ.

Note: The BIA provides details on how the business views the impact to their information assets and services following a loss of Confidentiality, Integrity or Availability. This is useful because it provides a steer on what types of incidents result in the highest impact to the business and how tolerant the business is to a loss of service provision. For help on creating a BIA, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

- Create a pre-defined and authorised list of users.
- Implement using the 'need to know' access principle on the PAM. Alternatively, if using a bastion host, find out what options there are to enforce this principle.
- Regularly check for redundant user IDs and accounts on either the PAM or bastion hosts. These should then be blocked or removed.

Public-facing services

Developers and administrators should ensure that front-end users who access the MoJ public-facing services or applications are authenticated through the GOV.UK Verify Service. When this is not possible, for example when an individual does not have a UK address, passwords must:

- Be easy to use, for example, pasting passwords into web forms should be enabled.
- Not be forcibly changed simply as a result of a period of time passing. However, passwords and other account access mechanisms must be revoked for an individual when they are no longer authorised to work with the account.
- Use Two Factor Authentication (the [Password Creation and Authentication Guide](#) provides further advice).
- Be changed when required, for example after a system compromise is identified, or if the limit of unsuccessful password attempts is reached and the account is locked.
- Be reset using a one-time password.

The [Password Creation and Authentication Guide](#) provides further guidance creating a strong and complex password.

Service accounts

Service accounts must be used for system and application authentication at a privileged level. Service accounts must use certificates for authentication, however if these cannot be used, then passwords are an acceptable alternative. The [Password Creation and Authentication Guide](#) provides further guidance on how you must create a strong and complex password.

Contact details

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

Single-Sign On

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

- Have a pre-defined identity source for users, such as Active Directory, Google Directory or LDAP. This means a developer or service provider must use an established MoJ SSO solution rather than creating a new one.
- Normally be based on applications rather than groups of people. This means that SSO is to a specific application or service, rather than saying something like 'all administrators of the Widget application have SSO-managed access'. Instead, SSO must be enabled for the 'Widget' application. It can be based on groups of people or roles if these have been defined.

Contact details

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

Password Management Guide

Introduction

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

The information is aimed at two audiences:

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

Roles and responsibilities

All MoJ Digital and Technology users

Everyone must ensure that password creation, distribution and maintenance is done securely.

Passwords must not ordinarily be shared. Refer to the [Password Storage and Management Guide](#) for exceptions and alternative solutions for sharing passwords.

Passwords must be strong and complex. Refer to the [Password Creation and Authentication Guide](#) for more details.

Passwords must be changed upon indication of compromise.

Passwords must be distributed securely. Refer to the [Password Storage and Management Guide](#).

Multi-factor authentication (MFA) must be enabled for existing systems, wherever possible. MFA must be enabled for new systems. Further guidance can be found in the [Password Creation and Authentication Guide](#) and the [Multi-User Accounts and Public-Facing Service Accounts Guide](#).

Where a default password is applicable, it must never be guessable.

Software Developers, Technical Architects and Development Operations

Make every effort to avoid creating yet another new or modified password-based authentication system. If it is unavoidable, then ensure that the following security requirements are adhered to:

- Multi-user accounts should be avoided, but if required refer to the [Multi-User Accounts and Public-Facing Service Accounts Guide](#) for further guidance.
- Technical controls must be implemented to support requirements in the [Password Creation and Authentication Guide](#).
- Applications or software must support MFA, and where possible single sign-on (SSO) solutions used by the MoJ.

- Passwords must not be stored in clear text or using encryption algorithms with known security weaknesses.
- Passwords must not be transmitted in clear text over networks.
- All applications or software must use HTTPS to require authentication.
- Applications or software must provide some form of role management, whereby an authorised user can take over the functions of another without having to know the other users' password.
- Passwords and other secrets (SSH Keys, DevOps secrets, etc.) must never be embedded into applications. The use of key vaults, such AWS Secrets Manager, is strongly recommended.
- Where a default password is applicable, it must never be guessable.

Suppliers and vendors

Suppliers and vendors must ensure that their systems support the password requirements set by the MoJ.

Supplier or vendor systems must be able to change, reset and revoke passwords. This must be possible using well-defined processes.

Suppliers and vendors must implement the technical controls in the MoJ guidance, such as locking accounts after repeated access attempts and blocking common password choices, to improve the effectiveness of password-enforcement and compliance.

Senior Business Owners for Contracts should ensure that when contracts are signed, the supplier receives explicit guidance on password management and it is included in the associated contractual Security Management Plan (SMP).

System Administrators

System Administrators (SAs) must ensure that systems support the password requirements set by the MoJ. When provisioning and maintaining user accounts, SAs must:

- Require a change of initial or first-time passwords.
- Verify a user's identity before resetting a password.
- Implement automated notification of a password change or reset.

SAs must also ensure privileged accounts:

- Are authorised only for a specified time.
- Are managed and regularly reviewed for user access, so that access is revoked when a user no longer needs it. This is to prevent unauthorised access.
- Use MFA for user authentication.
- Have activity logs for the purposes of review and monitoring.

Related guides

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

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

Contact details

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

Password Managers

[Ministry of Justice \(MoJ\) guidance](#) makes clear that you should have different passwords for different services. These passwords must be complex.

But how do you remember all these different passwords?

The simplest way is to use a [Password Manager](#). If you have lots of different, and complex, passwords for all your accounts, using a password manager makes life much easier.

This article provides guidance on using password managers within the MoJ.

Password managers and vaults

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 to use a password manager or a password vault

The following table shows when you might use a password manager or vault:

Scenario	Tool	Notes
Single user, personal accounts	Password manager	For accounts that only you use, or have access to, then you would probably store the details in a password manager. An example would be storing the username and password for your work email account; only you should have access.
Multiple users, shared accounts	Password manager or password vault	Some accounts might be shared between a group of users. For example, a team might need to know the password for an encrypted document. If the access required is for a sensitive or operational system, then a more heavily protected tool such as a password vault might be appropriate.
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.

Good password managers

A password manager should never store passwords in an unencrypted form. This means that keeping a list of passwords in a simple text file using Notepad would be A Bad Thing.

Good password managers encrypt the passwords in a file using strong encryption. It shouldn't matter where you store the encrypted file. Storing the list "in the cloud" lets your password manager access the data from any device. This is useful if you are logging in from a laptop, or a mobile device. Storing the passwords locally means the password manager works even when offline.

A good password manager will have:

- Strong encryption for the list of passwords.
- Network access for encrypted lists stored in the cloud.
- A dedicated app but also a pure web browser method for working with your password list.
- A tool to generate passwords of varying complexity.

For these reasons, MoJ advice is that you **SHOULD NOT** use password tools within an app to protect data files that are processed by the app. For example, you **SHOULD NOT** use the password tools with Microsoft Word, Excel, or Powerpoint, to protect MoJ information within files. Instead, either:

1. Store the data files in a shared but secure area, such as the MoJ SharePoint storage facility.
2. Use separate encryption tools to protect data files, separate from the app that works with the data files.

Of these two options, storing data files in a shared but secure area is strongly preferred. The reason is that you can add, modify, or revoke access permissions to the storage area easily.

If you have no choice, and have to use app-based password protection, ensure that the same password is not used indefinitely for a data file. You **SHOULD** use a different password for:

- Each major version of a data file, for example version 2.x is different to version 3.x.
- Any data file where the password is more than three months old.

Note: This advice is a specific exception to the [general guidance](#), that you do not normally need to change passwords.

Password expiry

You don't have to change a password because it is old. The reason is that time-expiry of passwords is an [...outdated and ineffective practice](#).

Some current or legacy systems don't allow passwords that follow MoJ guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to MoJ guidance.

Password managers

Use a password manager to help you keep track of your passwords.

These are tools that help you create, use, and manage your passwords. A useful overview is available [here](#).

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager. For example, development teams in MoJ Digital & Technology use [LastPass](#).

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services. Some managers have extra features, such as password generators. Some managers can even automatically fill-in username and password fields for you when during log in.

The password manager database is often stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for your MoJ account and service details is recommended.

You can find additional useful information about password manager tools [here](#).

Extra guidance for system administrators or developers is available [here](#).

System administrators or developers

Follow the [Government Service Manual for Passwords](#) when you administer or develop MOJ systems or services.

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

The [NCSC guidance](#) for simplifying passwords says that forcing complex passwords has:

- Marginal security benefit.
- A high user burden.

Technical controls are more effective at protecting password-based authentication. Examples include:

- [Locking accounts](#) after repeated access attempts.
- [Blocking](#) common password choices.

Related guides

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

- The [Account management](#) guide explains why you might need to change your password. It also addresses when and how you should change your password.
- The [Multi-User Accounts and Public-Facing Service Accounts Guide](#) explains when you should use a multi-user account and how you should authenticate a service account.
- The [Password Creation and Authentication Guide](#)

Multi-factor Authentication

[Multi-factor Authentication \(MFA\)](#) provides extra security for login and access controls. MFA is also referred to as Two-Factor Authentication or 2FA.

MFA **SHALL** be implemented and enabled on MoJ systems and services, including user accounts, wherever possible.

When performing a privileged action, such as installing or reconfiguring a system, or changing critical or sensitive details, it is important that the user is correctly and reliably authenticated. This is best done by using MFA. For example, before deleting a database configuration, MFA **SHOULD** have been completed successfully during the authentication process, to confirm that the user is indeed who they claim to be, and that they are indeed authorised to perform that privileged task.

In general, follow the [NCSC guidance](#) for enabling MFA.

Use [Time-based One-Time Password Algorithm \(TOTP\)](#), or hardware and software tokens, as the preferred MFA mechanisms. If possible, avoid using SMS or email messages containing one-time login codes. If TOTP applications, or hardware- or software-based tokens, are not available to you, then SMS MFA or email MFA is still better than no MFA.

Systems **SHALL** offer MFA alternatives to users where they are available. For example, MFA codes sent by SMS are not suitable if mobile devices are not allowed in the room or building where the privileged task is being performed.

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

Extra measures

Check that a system, service, or information protected by a password is not [classified](#) as SECRET or TOP SECRET. Make sure that it doesn't contain delicate material. Examples include contracts, or personal data or information. If it does contain such material, you might need extra access control.

Check which other systems have access to the system or service. Make sure that the access control suits the material at both ends of the connection.

Appropriate extra measures might include tokens or other multi-factor authentication devices. Think about using an existing authentication system other than passwords. Avoid creating new authentication systems. Try to reduce what a user needs to remember. For more information about authentication, refer to the [Authentication guide](#).

A technical risk assessment helps identifies extra controls for systems. This is mandatory for systems that need formal assurance. Multi-user systems are also subject to a Business Impact Assessment (BIA). For example, an assessment might find that you need extra checks for logging in to an account or service. The checks might depend on various factors such as:

- Time of login.
- Location of login.
- Number of previous connections from the connecting IP address.
- Whether to allow more than one login at a time.

Examples of these extra mechanisms include:

- Biometrics.
- Tokens.
- Certificate-based authentication.

Password storage

Never store, display or print passwords [in the clear](#). If you need to store them, do so by using [salted hashes](#).

Ensure the password storage security matches the [classification](#) of the system or data. For help with the appropriate strength of hashing, contact the Cyber consulting team: CyberConsultancy@digital.justice.gov.uk, or the security team: security@justice.gov.uk

Extra information on handling and protecting passwords is in the [Password Storage and Management](#) guide.

Password access attempts

If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is locked. A successful use of the password resets the count to zero again.

Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator or the MoJ IT Service Desk. The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work. Checks ensure that an attacker cannot use the password reset process.

Blocking bad passwords

You should not try and use [obvious passwords](#). Attempts to do so will be blocked.

Developers and administrators should configure systems to check for and block obvious passwords embedded within a password. For example, `MySecretPassword` is not a good password! Use password and hash lists from [SecLists](#) or [Have I Been Pwned](#), to help prevent bad passwords.

Distributing passwords to users

There are times when a system needs to send a password to a user. An example is when granting access to a service for the first time. To send a password to a user, the mechanism used **SHALL** be secure. The protection should match the sensitivity of the information protected by password.

Passwords created for a user should always be [single-use](#). Use an out-of-band channel to send the password to the user. For example, send the password to the user's line manager who will give it to the user.

For more information, refer to the [Password Storage and Management Guide](#).

Single-use passwords

Some passwords are 'one time' or single-use. Administrators and developers use these to grant access to a service for the first time. After using the password once, the user **SHALL** immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they **SHALL** become invalid.

The following table shows the valid lifetime of a single-use password:

Type of system	Lifetime of a single-use password
Single-user systems, such as laptops	1 week
All other systems	1 day

Multi-user systems and services

All multi-user systems and services **SHALL** check for redundant User IDs and accounts. If necessary, remove the redundant IDs or accounts.

The [Access Control Guide](#) discusses the management and removal of accounts.

If someone is no longer allowed to access a system, check for and change any shared account or common password they might still have.

For more information, refer to the [Multi-user accounts and Public-Facing Service Accounts Guide](#).

Identity Providers and Single Sign-On

When you need an authentication solution, try to use existing MoJ services. Examples include Identity Provider (IdP) or Single Sign-On (SSO) services, such as Office 365 or Digital and Technology G-Suite.

This helps reduce the need to design, create, deploy and manage yet another solution.

SSO integration in existing IdP solutions improves the user experience. This is because you can authenticate to systems using existing MoJ credentials.

For more information, refer to the [Multi-user accounts and Public-Facing Service Accounts Guide](#).

Account management

This guidance on passwords is separate from the guidance on account management. You should still follow the rules and processes for managing accounts. In particular, while you don't need to [change passwords after a period of time](#), you should still expire accounts promptly. Examples would be when accounts are no longer required, or have fallen out of use.

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

Contact details

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

Password Storage and Management Guide

Introduction

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

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

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

Password storage

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

- [LastPass](#)

Do not store sensitive information, such as passwords or credit card details, in unapproved tools. In particular, do not use "Autofill" tools to help fill in forms, unless the tools are provided and approved by the MoJ.

Contact the Cyber Assistance Team (CyberConsultancy@digital.justice.gov.uk) if you have a specialist need to use a different storage tool.

Sharing passwords

Passwords should not normally be shared. Sharing of passwords should be avoided by delegating privileges to other accounts, for example to provide access to a document or inbox.

Passwords can be shared for the following exceptions:

- For an encrypted document that has to be shared to make sense.
- For generic administration accounts on third-party services or applications, which support only a single account for administration purposes. If multiple individuals will perform the role, then the account password would have to be shared. [Privileged Access Management \(PAM\)](#) should be used where possible for systems that are administration only.

Some applications, for example, some social media tools, do not have 'role awareness'. This means you can't have access associated with a role; it must be through an individual account. This is sometimes 'solved' by having a PAM tool, where the PAM tool provides a more comprehensive managed 'gateway' to the underlying tool.

If there is a strong business need for shared access to a resource, account or system, then access to the password should be monitored and continually reviewed. This would be performed by:

- Regular auditing of who should have the password.
- Access revocation by changing the password if someone should no longer have access.
- Using proactive monitoring where it is enabled, for example by cross-referencing instances where the password is used with the dates and times that an authorised person could be using the password.

A shared password must be:

- Governed by PAM, and only be used by known and trusted users.
- Changed if any user in the group is no longer allowed access.
- Shared using a password manager.

Password vaults and managers

A password vault is a tool that stores passwords and other high-value secrets or credentials in an encrypted form. A password manager provides extra user-friendly tools for working with a password vault, for example helping you log in to applications or websites using the credentials stored within the vault. Password managers allow you to keep track of multiple passwords and avoid weak passwords.

The MoJ prefers [LastPass](#) for Team use, or business use by an individual.

Some teams, particularly service development and administration, have specialised needs that make other password vault tools more suitable. These project-specific tools include:

- AWS Key Management
- Azure Key Vault
- Hashicorp Vault
- Kubernetes Secrets

For further guidance on password strength, refer to the [Password Creation and Authentication Guide](#). Contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk if you have a specialised need to use a different password manager or vault.

Contact details

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

Policies for Google Apps administrators

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

These policies must be adhered to by all Google Administrators, including Super Administrators. All Administrator activity is recorded, auditable and notified to all other Administrators.

Why?

These policies ensure two things:

1. That administrators have a clear understanding of what is considered acceptable, so that they do not inadvertently perform an administrative action which is later considered unacceptable.
2. In the event that a security incident does occur in relation to Google Apps, that there is a clear policy which can be referred to, to support any action that is taken.

Actions requiring authorisation

The following actions require formal authorisation (e.g. an email confirming that the action can proceed) from at least 2 of the following 3:

- The Chief Digital Officer.
- The Chief Information Security Officer (CISO) for the Ministry of Justice (MoJ).
- The MoJ Digital Information Assurance Lead.

Actions:

1. Elevate any single user access to administrator from non-administrator.
2. Access any other users' emails or data (active or suspended).
3. Changing any 'global' configuration within Google Apps which affects all users.
4. Transfer any user's data (active or suspended) to another user. This also requires a request from the business area Service Manager.

Things you must do

1. Maintain the active list of all users (active and suspended) and maintain their access control to applications.
2. If anyone who has a Google Apps account leaves the organisation for any reason.
3. Suspend the account.
4. Transfer user's data to a user decided on by their line manager. This also requires a request from the business area Service Manager.
5. On a minimum quarterly basis (rota'd with other Admins) conduct an audit to check:
 - Any escalation of privileges from non-administrator to administrator.
 - Any forwarding of email accounts.
 - Any taking ownership of User accounts.

Policies for MacBook Administrators

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

All User accounts are created as 'Admin' to allow for software installation as part of normal business requirements.

Each laptop has a separate Admin account (created on build) to allow for User deletion and password resets

These policies must be adhered to by all MacBook Fleet Administrators.

Why?

These policies ensure two things:

1. That administrators have a clear understanding of what is considered acceptable, so that they do not inadvertently perform an administrative action which is later considered unacceptable.
2. In the event that a security incident does occur in relation to the MacBook Fleet, that there is a clear policy which can be referred to, to support any action that is taken.

Actions requiring authorisation

The following actions require formal authorisation (e.g. an email confirming that the action can proceed) from at least 2 of the following 3:

- The Chief Digital Officer.
- The Chief Information Security Officer (CISO) for the Ministry of Justice (MoJ).
- The MoJ Digital Information Assurance Lead.

Actions:

1. Creating a Mac account for a non MoJ member of Staff.
2. Access any other users' locally held data (active or suspended).
3. Transfer any user's locally held data (active or suspended) to another user. This also requires a request from the business area Service Manager.

Things you must do

1. Maintain the active list of all active users.

2. Raise an incident with the Operational Security Team (OperationalSecurityTeam@justice.gov.uk) and inform MoJ security (security@justice.gov.uk) and the MoJ CISO when leaving Staff have not returned all MoJ assets in their possession.
3. If anyone who has a MacBook account leaves the organisation for any reason.
4. Retrieve the Users equipment and suspend the account.
5. If requested by a Head of Profession, transfer user's data to a user decided on by their line manager. This also requires a request from the business area Service Manager.
6. On a minimum quarterly basis conduct a random percentage audit to check the encryption status of Mac Books and/or Airs.

System Users and Application Administrators

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

How to use this document

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

Who does it apply to?

All Users of the "[ORGANISATION]" Information and Communications Technology (IT) systems.

This document is designed to help Users utilise and access "[ORGANISATION]" IT systems in a safe and secure manner. Everyone using "[ORGANISATION]" IT systems must follow these procedures.

When and how should these procedures be used?

Users' Security Awareness training will cover these procedures.

Users must read this document prior to using any "[ORGANISATION]" IT Systems for the first time, and revisit it every six (6) months to remind themselves of the procedures. Regular audits will be performed to check that these procedures are being followed.

Users must understand that they are responsible for maintaining the security of "[ORGANISATION]" systems, and that failure to comply with these SyOPs could lead to compromise of the "[ORGANISATION]"s infrastructure or even the entire GSI. Users must note further that either failure to comply with this SyOPs or failure to return the security sign off form would be considered a breach of the "[ORGANISATION]" [IT Security Policy](#).

For further all the security related information required, please refer to:

- The "[ORGANISATION]" staff [intranet Security homepage](#)
- Remote User Security Operating Procedures (SyOPs) (if applicable)
- Blackberry User SyOPs (if applicable)

Area of control	All Users	Application Administrators Only
Shut-down and start-up	<p>Start-up:</p> <ul style="list-style-type: none"> • A physical inspection of the workstation must be carried out for any signs of tampering prior to switching the machine on. • The sharing of credentials, and attempting to logon as someone else (or with credentials which you are not authorised to use), are strictly forbidden. <p>Shut-down:</p> <ul style="list-style-type: none"> • Users must log-off the workstation and ensure it is switched off whenever left unattended for more than 4 hours or overnight. 	

Physical access controls	<ul style="list-style-type: none">• Only authorised members of staff with registered user accounts are permitted access to the system.• The equipment used to access the system must be checked on a daily basis for evidence of tampering or suspicious devices attached to it, for example unknown Universal Serial Bus (USB) devices attached to the rear of the main workstation.• Protectively marked and sensitive hardcopy material must be securely stored away under lock and key following the [ORGANISATION] Clear Desk Policy, published on the [ORGANISATION] intranet.• When accessing the system from portable computing devices, access is only to be made in approved area (refer to the SyOPs for Remote Access use).• Visitors must be supervised during working hours, and any sensitive documentation being worked on is to be hidden from line of sight as much as possible.
Awareness	<ul style="list-style-type: none">• When visitors are present, ensure that they are only able to access information for which they have a need-to-know.• Users must be aware of anyone 'shoulder surfing' and viewing information for which they do not have a need-to-know.• Users must not hold conversations over any telephone or send communications via fax or email if the information being discussed is protectively marked RESTRICTED.

Identification and authentication	<ul style="list-style-type: none">• Users must not attempt to log on as another user, or share their system access credentials with others.• Users must not allow unauthorised users to observe their screen.• Users must not allow any person to observe them entering their system access credentials (e.g. password).• Passwords used on the system must be created in line with the [ORGANISATION] Password Standard.• Users must invoke the screensaver before leaving their workstation unattended (by pressing 'windows' key + L).• A User account must only be created with permissions commensurate to that User's business role, and are only to be enabled once a signed copy of these SyOPs have been received from the user.• A User account must be disabled when that staff member leave the [ORGANISATION] or where their business role does not require them to have access.
Resetting user passwords	<ul style="list-style-type: none">• To change a password, Users must hold down Ctrl + Alt + Delete on their keyboard and select 'Change Password'.• If the password requires resetting, contact the IT Service Desk.
System Use	<ul style="list-style-type: none">• Users must not exceed (or attempt to exceed) their given access privileges, amend the system configuration or plug in any unauthorised devices.• Any unauthorised attempt at changing the configuration of the system, escalating privileges or installing devices/software may be subject to investigation and formal disciplinary action.• Unauthorised software must not be installed or used on the system.• Administrator level accounts should only be used when carrying out administrative tasks; at all other times a Normal User account should be used.

Acceptable use	<ul style="list-style-type: none"> The system must only be used in accordance with the [ORGANISATION] Acceptable Use Policy. The system must only be used for the business purposes for which it is intended. Any attempt to use it for other reasons may constitute a disciplinary offence.
Import/Export	<ul style="list-style-type: none"> A log must be maintained of all file imports/exports, this can either be a paper based or held electronically. All imports/export of electronic data/files to the System must be scanned for malicious code. Users must check and file exports to ensure that only files that they intended to export from one environment to another are exported. Where a network printer are used, Users must ensure print outs are collected promptly to minimise the risk of inadvertent disclosure.
Anti virus	<p>In the event of a User suspecting a virus attack on the network, they must carry out the following steps:</p> <ul style="list-style-type: none"> If operationally possible, leave the system switched on in its infected condition; Disconnect the affected workstation from the network (where possible); Mark the system and any associate storage media with a label stating that the machine has a suspected virus; Inform the IT Service Desk who will provide assistance.
Removable media	<ul style="list-style-type: none"> No System media or document is to be removed from the building without prior authorisation from the Information Asset Owner. All media and documents exported from the system must be registered in the media/document register and clearly marked with their protective marking in accordance with the Information Classification and Handling Policy. When a media/document is sent outside the [ORGANISATION] to an external body the following procedures must be adhered to: <ul style="list-style-type: none"> The export must be covered by an Information Sharing Agreement between the Authority and the external body which has been approved by the Information Asset Owner. Each export must be authorised by the Local/System Manager. Each export must have a data export receipt filled out and returned by the receiver to account for the transactions successful delivery
Secure Disposal of Protectively Marked material	<ul style="list-style-type: none"> Protectively Marked material must be disposed separately from general waste. Such waste should not be accessible to those without the proper authority. PROTECT and RESTRICTED classified information can be disposed via standard office provided shred bins allocated to hold material up to and including RESTRICTED. For CONFIDENTIAL, SECRET OR TOP SECRET information, Corporate Security Team must be contacted when securely disposing of paper documents, and [ORGANISATION] OST must be contacted for the secure disposal of IT devices. Further instructions can be found on the [ORGANISATION] Intranet, Confidential Waste Disposal page.

Security Incident and General Reporting Procedures

- All requests for IT support and all reports of IT failures must be logged with the IT Service Desk.
- Any incident involving a suspected or known security breach involving personnel, hardware, software, communications, document or physical security must be reported immediately to the IT System Manager and the [ORGANISATION] Operational Security Team (OST).
- Any loss of IT equipment, [ORGANISATION] or personal data should be **reported**. Report also to the Users' line manager, the OST (OperationalSecurityTeam@justice.gov.uk) and to the Data Access & Compliance Unit (DACU).

To ensure a quick response all emails must be marked Urgent and have 'Data Incident' in the title/subject heading.

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

Name:

Date:

Signature:

Incidents

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

Operational Security Team

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

General enquiries, including theft and loss

Technology Service Desk - including DOM1/Quantum, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

Note: The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses, and the Digital & Technology Digital Service Desk Slack channel (#digitalservicedesk), are no longer being monitored.

HMPPS Information & security:

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

Using LastPass Enterprise

What is LastPass?

LastPass is an online password management tool that we make available to you to help you create, store and share passwords. Using it means you no longer need to remember dozens of passwords, just a single primary password. It keeps all your website logins protected, helps with creating new 'strong' passwords and password sharing when required.

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

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

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

Who should use it?

MoJ LastPass accounts can be requested by anyone in MoJ Digital and Techn

The MoJ has an 'order of preference' for [which types of MFA to use](#):

- Hardware-based (for example, Yubikeys)
- Software-based (for example, Google Prompt on a mobile device)
- TOTP-based (the code is held by a dedicated app such as Google or LastPass Authenticator on a mobile device)
- SMS-based (a one-time code sent via SMS)

If you don't have an MoJ-issued work smartphone you may use a personal device for MFA.

Sharing passwords

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

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

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

Using it overseas

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

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

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

Keeping LastPass update to date

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

Need help?

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

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

Cryptography

Cryptographic controls

Automated certificate renewal

Note: If you want client certificates, contact SoftwareAssetManagement@justice.gov.uk.

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

Note: If you want client certificates, contact SoftwareAssetManagement@justice.gov.uk.

Cryptography

The base principles

- All data **must** employ adequate and proportionate cryptography to preserve confidentiality and integrity whether data is at-rest or in-transit.
- Existing cryptographic algorithms (and implementations thereof) should be used - at the highest possible abstraction level.

In-transit

In-transit encryption techniques can both protect data during transit through cryptography but also help facilitate the establishing of identity of devices on one or more sides of the connection.

Transport Layer Security (TLS)

The [National Cyber Security Centre \(NCSC\)](#) have published information on good TLS configurations <https://www.ncsc.gov.uk/guidance/tls-external-facing-services>.

In general, subject to document exceptions (such as end-user needs and required legacy backwards compatibility).

Testing

Tools such as [Qualys SSL Server Test](#) and Check TLS services from checktls.com **must** be used where applicable to help identify most common issues and configuration problems.

While these tools are not a replacement for skilled testing, the outputs of these tools can help you identify inefficient or insecure configurations which should be considered for remediation.

Configurations should be periodically re-validated.

Internet protocol security (IPsec)

NCSC have published information on good IPsec configurations <https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data>.

At-rest

At-rest encryption techniques can protect data while being stored and even during some processing. At-rest techniques usually protect against physical theft or attack methods.

Server-based

Local storage (such as operating system locations) and filestores (such as storage area networks) should be considered for at-rest encryption to help mitigate again physical interception (such as theft) threats.

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

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

Segregation and supersession

Key variables that are issued from CESG are typically issued with two editions. The first is for immediate deployment and the second is for emergency supersession. In the case of hard disc encryption the supplier holds the live edition and the MoJ Crypto Custodian holds any others. All supplier crypto deployment environments are not at the same site as the MoJ Crypto Custodian and this provides natural segregation of the editions.

Ecrypt uses a lifetime key variable and does not have more than one edition. In the event of compromise, the usual CINRAS report and request to CESG for emergency replacement of the key variable will be required.

PKI Services	The services provided in the delivery of Public Key Infrastructure. PKI Services includes those provided either as a root or subordinate Certificate Authority, Registration Authority, and Validation Authority.
	The usage of digital certificates for cryptography or digital signatures within applications and other IT systems is not considered a PKI Service, but those systems would consume PKI Services.
PKI Customer	An entity (a user or organisation) that is authorised to access the PKI Services for the purposes of signing or revoking digital certificates. Some PKI customers may also provide delegated PKI Services.

General PKI Policy

Overview

This section describes the common PKI policy that applies regardless of the type of PKI service in question. It covers the following subsections:

- Governance Structure
- Technical Architecture
- Operational Policy
- Process Requirements

Governance Structure

Roles and Responsibilities

- Senior Information Risk Owner (SIRO) – Responsible for all risks to do with the PKI Services. Final point of escalation for incidents.
- Departmental Security Officer (DSO) – Responsible for the operational governance of the PKI Services and the report line for the ComSO.
- Communication Security Officer (ComSO) – Responsible for day to day management of the PKI Services, relationship management with CESG and UKKPA (GCHQ's UK key production authority), mustering and other formal processes. First point of escalation for incidents and managing initial incident response.
- Crypto Custodians – Responsible for day to day operation of the PKI services, including the distribution of keys from the UKKPA. Where keymat is provided from the UKKPA they shall be formally trained and authorised Crypto Custodians. For other services they should be formally trained. Note that the Authority's Crypto Custodian may delegate key management responsibilities to Supplier Crypto Custodians.
- IT Security Officer (ITSO) – Responsible for operational IT security management.
- Administrators – Responsible for configuration, maintenance and support of the PKI services
- Auditors – Internal and external auditors including UKKPA and MoJ Information Assurance who ensure that the PKI Services are running within specification and comply with legal and regulatory requirements, HMG Policy and MoJ Policy.

Incident Response

1. There shall be an Incident Response and Escalation process in place.
2. The incident response process shall cover procedures for:
 - Impact minimisation
 - Escalation
 - CRL issue
 - Digital Forensics
 - BC / DR
1. The escalation shall be from the person discovering the incident to the local Crypto Custodian, then the MoJ Crypto Custodian, then ComSO, then DSO then SIRO. Escalation to CINRAS and other external bodies shall only be performed by the ComSO, DSO or SIRO.

User Registration

1. Any individual who requires access to the IT Systems providing PKI Services shall be subject to stringent background checks shall be vetted to at least Security Check (SC) before any access to the system is permitted.
2. **Important:** Interim access pending security clearance must not be allowed under any circumstances. The impact of allowing such access in the event that the individual is not subsequently cleared would be to revoke and reissue all certificates signed by the PKI Services.
3. When clearance is confirmed and identity is validated by MoJ, the user shall be enrolled in the services required and shall be issued with the relevant credentials for access.
4. Users shall be removed from the systems and their credentials revoked as soon as they leave the role related to the PKI Services. The relevant HR Processes must be reviewed, and updated if necessary, to account for this policy.

Authentication

1. All Users of the PKI Services shall be authenticated beyond reasonable doubt for the purposes of legal admissibility of evidence in accordance with BS 10008. Password strength, complexity and expiry rules must comply with [MoJ Password requirements](#).
2. Access to Root CA Services must be subject to multi-factor authentication and subject to two-man rule.
3. Access to specific signing functions shall be subject to specific authentication and access control policies including two man rule.

Accounting

1. Auditing and accounting of all PKI functions must be carried out in accordance with HMG Good Practice Guide 13. The integrity and confidentiality of accounting logs must maintained to British Standard BS 10008 as appropriate for legal admissibility of evidence, in the event that disputes need to be heard in a court of law.
2. Internal audit by authorised auditors shall take place at least every quarter
3. Where PKI Services are subordinate to external services, e.g. UKKPA or PSNA, then the audit and accounting regime must comply with the policies of the relevant authority.
4. Audit reports shall be provided to the DSO and SIRO quarterly.

Compliance

1. The PKI Services shall at all times comply with Legal and Regulatory requirements including (but not limited to):
 - Data Protection Act (1998 and 2003)
 - Official Secrets Act (1989)
 - Cryptography Export Regulations
 - Regulation of Investigatory Powers Act (2002) (RIPA) Part 3
 - Export Controls Act (2002)
 - Electronic Communications Act 2000
 - SI 2002/318 The Electronic Signatures Regulations 2002
1. The PKI Services shall at all times comply with HMG Policy including:
 - Security Policy Framework
 - HMG IA Standard 4
 - HMG IA Standard 5
1. The PKI Services shall at all times comply with any Code of Connection, Memorandum of Understanding or other connection criteria that applies to the environment in which the services are deployed. These shall include as a minimum:
 - PSN Code of Connection
 - GSI Code of Connection (while GSI connections remain)

Technical Architecture

Technical Design Considerations

The design of PKI systems must ensure:

2. There shall be a CPS for each signing certificate.

References

The following are FITS PKI Policy specific references used within this document.

Ref:	Title & Location
1	HMG Security Policy Framework (SPF) v11.0 Nov 2013 https://www.gov.uk/government/publications/security-policy-framework
2	CESG Cryptographic Standards – Cryptographic Mechanisms, Algorithms & Protocols v1.0 July 2010
3	CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT Systems v1.7 – Oct 2012
4	HMG IA Standard No.4 - Management of Cryptographic Systems v5.3 – Oct 2013
5	HMG IA Standard No.4 - Supplement 1 - Roles and Responsibilities v3.0 - Apr 2013
6	HMG IA Standard No.4 - Supplement 2 - Concepts and Terminology of Cryptography v1.0 - Apr 2011
7	HMG IA Standard No.4 - Supplement 4 - Labelling of Cryptographic Items v2.0 – Nov 2012
8	HMG IA Standard No.4 - Supplement 5 - Account Management v1.0 - Apr 2011
9	HMG IA Standard No.4 - Supplement 6 - Personnel & Physical Security of Crypto Items v3.0 - Nov 2012
10	HMG IA Standard No.4 - Supplement 7 - Accounting of Cryptographic Items v1.0 - Apr 2011
11	HMG IA Standard No.4 - Supplement 8 - Movement of Cryptographic Items v1.0 - Apr 2011
12	HMG IA Standard No.4 - Supplement 9 - Destruction & Disposal of Cryptographic Items v2.0 - Apr 2012
13	HMG IA Standard No.4 - Supplement 10 – Compliance v2.0 – Oct 2013
14	HMG IA Standard No.4 - Supplement 11 - Incident Reporting for Cryptographic Items v2.0 - Apr 2012
15	HMG IA Standard No.4 - Supplement 13 - Assurance Standards v4.0 – Oct 2013
16	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://datatracker.ietf.org/doc/rfc3647/
17	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://datatracker.ietf.org/doc/rfc5280/
18	RFC 6960 - Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP http://datatracker.ietf.org/doc/rfc6960/
19	https://shop.bsigroup.com/SearchResults/?q=BIP%200008 <ul style="list-style-type: none"> • BIP 0008-1:2008 Evidential weight and legal admissibility of information stored electronically. Code of Practice for the implementation of BS 10008 • BIP 0008-2:2008 Evidential weight and legal admissibility of information transferred electronically. Code of practice for the implementation of BS 10008 • BIP 0008-3:2008 Evidential weight and legal admissibility of linking electronic identity to documents. Code of practice for the implementation of BS 10008
20	CESG Good Practice Guide 45 - Identity Proofing and Verification of an Individual v2.3 – July 2014

21	CESG Good Practice Guide 46 – Organisational Identity v1.0 – Oct 2013
22	HMG IA Standard No. 5 – Secure Sanitisation – v4.0 – April 2011
23	ITU-T Recommendation X.509 – Public-key and Attribute certificate frameworks [10/2012] http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11735
24	RFC 2986 - Certification Request Syntax Specification – November 2000

Use of HMG Cryptography Policy

Related information

[Technical Controls Policy](#) on page 36

Legacy information

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

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

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

About this document

This document is the Ministry of Justice (MoJ) IT Security – Use of HMG Cryptography Policy. It provides the core set of principles, expectations, roles and responsibilities for using HMG cryptographic material.

How to use this document

Each policy statement outlines a security requirement and where applicable, a reference is provided to further material. A unique identifier is associated with each statement for easy reference. The format of each statement is illustrated as follows:

POL.CRYPTO.XXX

Policy statement text.

The policies outlined in this document form the baseline standard. However this policy is not a replacement for HMG Information Assurance Standard No. 4 - Management of Cryptographic Systems [Ref, 2]. HMG IAS4 remains the primary reference source where this policy provides a supplement to it.

Use of HMG Cryptography Policy

Introduction

POL.CRYPTO.001

It is the policy of the MoJ to follow the policy of HMG Information Assurance Standard 4. This document endorses and augments that policy. Where the local policy contained herein, if different to HMG Policy, the local policy overrides HMG policy and must be adhered to.

Scope

This policy is concerned with the use of HMG cryptographic material used on any MoJ IT system and/or where HMG cryptographic material is obtained through the MoJ.

Purpose

MoJ uses a wide range of cryptography products or various classifications and is serviced by several suppliers. This policy is intended to supplement the HMG IAS4 [Ref, 2] and assist suppliers to procure encryption from CESG and manage its life cycle.

Audience

Anyone who wants to obtain encryption from CESG and everyone who is, or needs to be, CRYPTO or ACCSEC authorised (refer to the glossary) to handle Key Variables (KV) or hardware.

In accordance with HMG IAS4 [Ref, 2] encryption is only provided for fully accredited systems. There are long lead times to obtain encryption products from CESG (which fluctuate between 8-12 weeks and are always subject to change). It is recognised that there needs to be some flexibility in the process to order encryption and this guide helps meet that requirement.

Definitions

Trusted Hand

An individual who is at least BPSS cleared and recognised as a member of staff of a supplier.

Communication

POL.CRYPTO.002

The use of secure email **must be** used a primary method of communication for all and any communications from suppliers in respect of cryptography to the MoJ Crypto Custodian, Communications Security Officer (COMSO) and IT Security Officer (ITSO) regardless of whether the protective marking is UNCLASSIFIED or NOT PROTECTIVELY MARKED and up to RESTRICTED.

Acceptable secure email methods are GSi, xGSi and CJSMS accounts. All queries towards CESG must be forwarded to the MoJ Crypto Custodian and/or COMSO. CESG must not be contacted direct.

New requirements for encryption and/or hardware

As soon as the need for encryption is identified the system Accreditor, the COMSO must be informed by the Project Manager and agreement sought for the need for the hardware, software and encryption from CESG.

The process requires that an applicant is appointed and that applicant is responsible for ensuring that the product is suitable for the requirement and it is their responsibility to familiarise themselves with the CESG Security Operating

Procedures (SyOPs) for that product. The applicant can delegate this element to someone else but that person must be identified to the other parties of this approval process.

POL.CRYPTO.003

The Project Manager **must appoint** an applicant. Exceptionally, the applicant can be the Project Manager. The applicant **must contact** the vendor of the encryption product and obtain the latest version of the CESG macro enabled word application form to complete.

This form must be completed by the applicant with a full explanation of the requirement and attached with, if appropriate, a diagram (e.g. MS Visio diagram) which explains the solution and this must be sent to the COMSO, Accreditor and MoJ Crypto Custodian for approval with the application form.

Note: The applicant is responsible for ensuring that the product is suitable and meets the desired business requirement.

If the solution requiring encryption has not yet been Accredited (at the time the application is being drafted), or if the current RMADS need to be updated to accommodate this requirement, a timetable must be set out for the delivery of draft RMADS and SyOPs, this **must be** attached to the application form.

The COMSO and Accreditor must both approve and notify the MoJ Crypto Custodian in order for the form to be sent to CESG for processing.

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

Further processing is required by the MoJ Crypto Custodian and upon dispatch to CESG the MoJ Crypto Custodian will give the applicant a reference number (hereafter referred to as the IAB account number) which must be referred to in any future communications regarding the requirement.

Increase in a community (usage of Crypto)

When it is necessary to increase the number of licences, changes to hardware or otherwise change how Crypto used, the applicant must obtain the latest form from the vendor and send the form to the Accreditor and COMSO for approval. The applicant must refer to the CESG X reference which can be found in the documentation that the supplier holds.

POL.CRYPTO.004

The applicant **must determine** whether or not a change to the RMADS or SyOPs are necessary and confirm this on application. If changes are required it must be declared how and when this will happen.

POL.CRYPTO.005

The Accreditor and COMSO **must** both agree and approve the change and advise the MoJ Crypto Custodian.

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

Authority to Operate Certificate

The MoJ Crypto Custodian and the Vendor will be advised by CESG of the Authority to operate and this will be forwarded to the applicant by the MoJ Crypto Custodian, with this certificate the applicant can purchase the relevant hardware or licences from the vendor.

It is the responsibility of the applicant to raise any relevant purchase orders though the MoJ purchase order system or progress the financial procurement for the product through other channels.

CRYPTO and ACCSEC authorisation

If there is a requirement to store Key Variables locally, the supplier must appoint a Local Crypto Custodian (LCC) and Local Alternate Crypto Custodian (LACC). Both must attend the CESG training course for Crypto Custodians and be sponsored by the MoJ Crypto Custodian.

Any subject who handles Key Variables for the MoJ must be SC cleared and CRYPTO or ACCSEC authorised initially by the MoJ Crypto Custodian. The subject must provide the details on the Crypto Authorisation form through secure channels and provide the contact details of the vetting office which approved their clearance.

POL.CRYPTO.006

Every 12 months the LCC and LACC **must re-authorise** each other and check that their clearances are still valid and this must be evidenced and recorded with the authorisation form for audit purposes.

If the LCC or LACC CRYPTO or ACCSEC authorises anyone else locally, there are responsible for checking the security clearances and maintaining and renewing the authorisation or de-authorisation process and keeping records available for inspection and audit by the MoJ Crypto Custodian or Authority.

Delivery of Key Variables

When Key Variables arrives and has been checked and recorded by the MoJ Crypto Custodian an email will be sent to the applicant to inform them that their Key Variables has arrived.

Key Variables distribution

All Key Variables is stored and managed centrally by the MoJ with some exceptions such as hard disk encryption which suppliers need to store locally.

There are special arrangements for the local storage of Key Variables which must be agreed with the COMSO.

POL.CRYPTO.007

Key Variables **must not** be deployed unless the encryption solution is accredited or the timetable has been set out and agreed on its delivery, draft RMADS and final SyOPs must be made available to the MoJ Crypto Custodian.

POL.CRYPTO.008

The applicant **must agree** with the MoJ Crypto Custodian how the Key Variables is to be deployed, or provide the details of the person who will manage this if it is not the applicant. Generally speaking the Key Variables is retained at MoJ HQ and issued out for a short period of time in order to encrypt the system and then returned to MoJ HQ for storage.

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

1. Collected from and returned to MoJ HQ by a CRYPTO or ACCSEC authorised person and transported in a secure lockable container (such as a lockable briefcase or a CPNI approved transportation container).
2. Collected and returned by trusted hand for transportation in a secure lockable container to a CRYPTO or ACCSEC authorised person in tamper evident packaging using the usual Government Protective Marking Scheme (GPMS).
3. Dispatched from and returned by a reputable courier who guarantees delivery within 24 hours and provides a tracking service (not Royal Mail). The Key Variables must be sealed within tamper evident packaging and appropriately protected. Suppliers must take full responsibility for this process and arrange for courier to collect and return.

Key Variables Management

POL.CRYPTO.009

The management of Key Variables **must be** in accordance with HMG IAS4 Supplement 7 [Ref, 3].

Key Variables Destruction

POL.CRYPTO.010

Suppliers **must not** under any circumstances destroy Key Variables. All Key Variables must be returned to the MoJ Crypto Custodian for destruction.

Business continuity

POL.CRYPTO.011

The MoJ Crypto Custodian, the Alternate Crypto Custodian and any authorised signatories and or people who have access to the safes where cryptographic material that is managed by the MoJ Crypto Custodian is stored must conform to the IT Security Policy - HMG Cryptography Business Continuity Management Standard [Ref, 4].

Annual Audit of Crypto

Every 12 months the COMSO will inspect the arrangements for sites locally storing Key Variables. A date will be agreed with the COMSO to inspect the premises, audit the paperwork and check the crypto stock.

References

ID	Title	Version / Issue
1	IT Security Policy	V1-00
2	HMG IS4 - Management of Cryptographic Systems	Issue 5.1, Apr 2011
3	HMG IS4 - Supplement No.7 - Accounting of Cryptographic Items	Issue 1.0, Apr 2011
4	IT Security Policy - HMG Cryptography Business Continuity Management Standard	V0-01

Physical and environmental security

Secure areas

CCTV policy

The policy complements the Ministry of Justice (MoJ)'s overall security policy.

The CCTV Policy applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ occupied premises.

Agencies and arm's length bodies (ALBs) are expected to comply with the corporate framework, but **MAY** establish their own arrangements tailored to operational needs and **SHOULD** supplement the framework with local policy or guidance for any business-specific risk.

Related information

[Logging and monitoring](#) on page 261

Objective

The MoJ has in place several CCTV surveillance systems installed within its core buildings. This policy details the purpose, usage, and management of the CCTV systems, and the procedures to be followed to ensure the MoJ complies with relevant legislation and the current Information Commissioner's Office (ICO) Code of Practice.

The MoJ has due regard to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act 2000, the Protection of Freedoms Act 2012, and the Human Rights Act 1998. The

MoJ also has due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012, and the 12 guiding principles contained therein.

This policy is based upon guidance issued by the ICO.

This policy and the procedures it details apply to the MoJ CCTV systems, including security guards' body worn cameras. CCTV images are monitored and recorded in strict accordance with this policy.

The policy is applicable to all buildings owned or occupied by the MoJ, where MoJ monitored CCTV is installed.

The policy is available for download [here](#).

Contact details

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

Entry and exit search policy

The Ministry of Justice (MoJ) "Entry and Exit Search Policy" applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ occupied premises.

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

The policy defines the access controls that are in place when entering and exiting MoJ buildings.

The policy is available for download [here](#).

Physical security advice

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

Contact details

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

Personal mail and parcel delivery policy and procedure

This personal mail and parcel delivery policy applies to all Ministry of Justice (MoJ) employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ occupied premises.

Agencies and Arms Length Bodies (ALBs) are expected to comply with this corporate framework but **MAY** establish their own arrangements tailored to operational needs and **SHOULD** supplement it with local policy or guidance for any business-specific risk.

Objective

Following a review by Government Security Centre People and Physical (GSCPP), it is recommended that the MoJ implements a policy on personal and business deliveries, including prohibiting personal parcel deliveries, to MoJ buildings. This policy prohibits deliveries of personal items to MoJ buildings, to comply with HMG minimum physical standard No.10 on mail or delivery management. For further information regarding this standard, contact mojgroupsecurity@justice.gov.uk.

This provides MoJ employees, contractors, partners and other interested parties with a clear policy on mail deliveries, to prevent attack, damage, or interference (malicious or otherwise) to MoJ assets, and - most importantly - physical harm to MoJ people and the public.

Responsibilities

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

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

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

- Perimeter control.
- Guarding.
- Site access.

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

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

Policy statements

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

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

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

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

Compliance

The level of risk and potential impact to MoJ information, assets and people determines the controls to be applied, and the degree of assurance required. The MoJ **SHALL** ensure a baseline of physical security measures are in place at each site, and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, for example in response to a security incident or change in the Government Response Level.

The implementation of all security measures **SHALL** be able to provide evidence that the selection was made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure, and [Government Functional Standard - GovS 007: Security](#).

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards are subject to annual review, or more frequently, as warranted.

Physical security advice

Physical security advice, including specific advice on this guidance, can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Public protest and demonstrations policy

This policy provides Ministry of Justice (MoJ) employees, contractors, partners, and other interested parties with enough guidance to take proportionate measures in case of public protest or demonstration.

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

Audience

This policy complements the MoJ overall security policy.

This Public Protest Policy applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This includes employees of other organisations who are based in, or work at, MoJ occupied premises.

POL.PPD.001

Buildings located in Central London, within the Government Security Zone (GSZ), receive information from the GSZ control room about proposed protests – either from information provided by the organisers or through monitoring social media.

Following any public protest or demonstration, the most senior grade based at the site, or in Moderate Risk and larger sites, the Senior Responsible Officer (SRO), has responsibility for ensuring that detailed records are kept of any incidents, including:

- The identity of those involved.
- The date, time and location.
- The behaviour involved.
- The impact, such as damage, injury, or disruption.
- Any warnings issued or other steps taken to defuse the situation.

Policy Statements

POL.PPD.003: The buildings' incident control plan **SHOULD** be reviewed regularly to ensure that it is up-to-date with good communication systems for the Incident Control Officer or Deputy Incident Control Officer to direct matters.

Managing the site, including security detail

POL.PPD.004: The following aspects of site management **SHOULD** be addressed:

- Minimise the number of entry points to the building.
- Ensure the outside areas are clear of debris, dustbins, ladders, tools, or equipment.
- Check that emergency equipment, grab bags, first aid supplies, and personal radios are in place, easily accessible and working properly. It is advisable to test them beforehand.
- Check and test building security and emergency systems.
- Ensure [CCTV coverage](#) is fully operational and can provide the highest recording resolution possible.
- If your building has scaffolding erected or is near scaffolding, let your security staff know.
- Report any suspicious activity to police by dialling 999 in an emergency, or call 101 if not an emergency.

People management and communication

POL.PPD.005: In the days leading up to a planned event, all employees **SHOULD** be fully briefed.

POL.PPD.006: The building **SHOULD** have a strong, visible management presence who **SHOULD** identify themselves to the police in the event of any trespassing or damage.

POL.PPD.007: Security officers, where possible, **SHOULD** be highly visible.

POL.PPD.008: All staff **SHOULD** remain vigilant and report any suspicious activity to security or the police.

POL.PPD.009: All members of staff **SHOULD** be fully aware of any emergency and evacuation procedures.

Compliance

POL.PPD.010: The level of risk and potential impact to MoJ assets and most importantly physical harm to our people and the public determines the controls to be applied and the degree of assurance required. The MoJ **SHALL** ensure a baseline of physical security measures are in place at each site and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, such as in response to a security incident or change in the Government Response Level.

POL.PPD.011: The implementation of all security measures **SHALL** be able to provide evidence that the selection has been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI), and [Government Functional Standard - GovS 007: Security](#).

POL.PPD.012: The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards **SHALL** be subject to annual review, or more frequently if warranted.

REQUIREMENT 9 and REQUIREMENT 10*Project Scoping & Supplier Selection*

Supplier:

- Ensure that the proposal includes provision for through-development testing, including security testing. Demonstrable compliance with the OWASP Testing Guide ([downloadable from the OWASP web-site](#)) is encouraged. The level of security testing required must be agreed with the Accreditor, and will need to be directly commensurate with the risk involved.

MoJ Project Team:

- Ensure that suppliers are aware of the requirement for testing, including not only functional testing but also security testing. Reject any proposals that do not make provision for this.
- Ensure that supplier proposals are realistic about the benefits of any offshoring elements of the proposals, and have accommodated realistic project costs and timescales for testing to address offshoring risks. Conduct an internal sanity check of supplier estimates for security and other testing. Reject any proposals where cost or time estimates are unrealistic.

MoJ Accreditor/IA:

- Support assessment of functional and security testing proposals.

Contract Award

MoJ Project Team:

- Ensure that the contract requires the supplier to test the solution against internationally recognised standards at all stages of the development (unit testing, integration testing, acceptance testing, etc). Suppliers must be contractually required to agree test scopes, including security test scopes, with the MoJ before the start of testing. The MoJ must be contractually entitled to visibility of all test results and progress on remedial activities to the MoJ. Ensure that the scope of testing in the contract includes security testing of the solution, at a level agreed with the Accreditor and the IA Team.
- Ensure that the contract retains executive control over the test process by the MoJ, with the ability to reject substandard delivery, require remediation and enforce contractual penalty clauses.

MoJ Accreditor/IA:

- Review offshoring elements of supplier contracts, including test arrangements. Provide input to the Project Team as required to support contractual terms for test, particularly security elements of testing.

Development

Supplier:

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

MoJ Project Team:

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

MoJ Accreditor/IA:

- Support test review and remedial activities.

In-Service & Beyond

Supplier:

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

MoJ Service Management:

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

MoJ Accreditor/IA:

- Support test review and remedial activities.

REQUIREMENT 11

Project Scoping & Supplier Selection

Supplier:

- Ensure that any proposal to use landed resources is clearly stated. Ensure that any associated costs and risks are identified.
- Where landed resources are to be used, ensure that the proposal clearly sets out what information assets and collateral assets would be made available to those resources, how many landed resources are proposed, from where, what level of clearance would be required, and how clearance information requirements would be satisfied.
- Where clearance is not possible to an equivalent level for a landed resource as for a UK resource, identify what the additional residual risks of this will be, how it is proposed to mitigate these risks. The proposal should identify any practical difficulties with these arrangements and how they will be overcome, as well as setting out the additional costs involved.

MoJ Project Team:

- In liaison with the MoJ Accreditor and MoJ IT IA, ensure that proposals for using Landed Resources are realistic.
- Ensure that the costs associated with the use of landed resources have been fully considered in the proposal.
- Reject any unrealistic or un-costed proposals for use of Landed Resources.

MoJ Accreditor/IA

- Support assessment of security risk and residual risk with supplier proposals to use landed resources.
- Advise on the feasibility of using landed resources from high-threat countries if relevant.

Contract Award

Supplier:

- Ensure that use of landed resources is in line with contractual requirements.

MoJ Project Team:

- Ensure that the supplier contract includes provision to enforce suitable security controls surrounding landed resources, as agreed during supplier selection.
- Ensure that the project budget includes a suitable level of contingency to accommodate any changes in offshoring costs due to change in Threat Assessment for landed resources.

MoJ Accreditor/IA:

- Review offshoring elements of supplier contracts.

Development

Supplier:

- Ensure that all landed resources are vetted to a level commensurate with the value of the information to be handled by that landed resource. Where it is not possible to effectively vet a landed resource to the required level, landed resources must not be used.
- Inform the MoJ immediately if resource requirements change.

MoJ Project Team:

- Ensure that the MoJ Accreditor and MoJ IT IA are kept fully informed of any change in supplier requirements, and that no change in Landed Resource requirements is agreed without the explicit approval of the IA Team.
- Ensure that the supplier is kept fully informed of any change in Threat Assessment relating to landed resources and of the impact on project delivery.

MoJ Accreditor/IA

- Ensure that the MoJ Project Team are made aware of any change in Threat Assessment relating to Landed Resources, and of how this will impact the project.

In-Service & Beyond

Supplier:

- Ensure that all landed resources are vetted to a level commensurate with the value of the information to be handled by that landed resource. Where it is not possible to effectively vet a landed resource to the required level, landed resources must not be used.
- Inform the MoJ immediately if resource requirements change.

MoJ Service Management:

- Ensure that the MoJ Accreditor and MoJ IT IA are kept fully informed of any change in supplier requirements, and that no change in landed resource requirements is agreed without the explicit approval of the IA Team.
- Ensure that the supplier is kept fully informed of any change in Threat Assessment relating to landed resources and of the impact on project delivery.

Further Reading

Title	Version / Issue
CPNI Personnel Security in Offshore Centres	04/2009
CPNI Good Practice Guide: Outsourcing: Security Governance Framework for IT Managed Service Provision	02/08/2006
CESG Good Practice Guide 16: Taking and Using Cryptographic Items Overseas	Issue 1.0, 08/2009
CESG Good Practice Guide 23: Assessing the Threat of Technical Attack Against IT Systems	Issue 1.0, 04/2010

Notes

<http://www.owasp.org>

Wherever it is considered that there may be a requirement to use real or anonymised data, rather than synthetic data, the MoJ "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, refer to [this guidance](#).

A particular consideration for offshoring is DPA Principle 8: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

For example, an offshore organisation based in Country A, which provides second-line support for an MoJ application from Country A, might rely on teams from its offices in Country B to conduct development and third-line support activities. This would have an impact on the Threat Assessment and hence the risks to the capability.

The Baseline Standard requires at least three years' worth of previous employment history. From experience, it is considered that a commensurate length of time is also required to build up a suitably rich credit history and social footprint to enable reliable checks to be conducted.

<http://www.cpni.gov.uk/advice/personnel-security1/overseas-criminal-record-checks/>

For example, for personal data transferred outside of the EEA the European Commission approved model clauses as per Directive 95/46/EC of the European Parliament and of the Council, provides a useful template. This can be found at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF>. The legal framework for managing the export of Protectively Marked information must be no less restrictive than this.

Cyber Security Advice

Cyber Consultants and Risk Advisors

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

Protection from malware

Malware Protection Guide - Overview

This guide introduces the information which explains your responsibilities in helping the Ministry of Justice (MoJ) to prevent, detect and recover from malware. The MoJ has a three layer defence approach aligning with the National Cyber Security Centre (NCSC) guidance to mitigate the risks posed by malware. If one layer of defence is compromised then malware should be blocked or detected by the next layer.

Related information

[Email blocking policy](#) on page 342

[Technical Controls Policy](#) on page 36

Detailed information

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

- [Malware Protection Guidance - Defensive Layer 1](#): Preventing malicious code from being delivered to devices - This section explains the preventative measures which should be taken to prevent malware from entering the 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

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

Malware Protection Guide: Defensive Layer 1

Introduction

This guide explains the types of controls that need to be implemented to form the first of three layers of defence. Layer 1 reduces the likelihood that malicious content will reach the Ministry of Justice (MoJ) network through implementing the controls outlined in this guide. This guide is a sub-page to the [Malware Protection Guide](#).

Who is this for?

This Malware Protection information is mainly intended for in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other MoJ bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the MoJ, will also find this information helpful.

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

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, refer to the NCSC guidance on Cloud Security or ISO27017 . These provide guidelines for information security controls applicable to the provision and use of cloud services.
Ensure that if you are managing an email system, all inbound emails to the MoJ are scanned for malware. For Microsoft systems this is provided by Office 365 which quarantines any suspected malware.
Avoid the need for removable media by using existing approved online collaboration services where possible, for example Office 365. Where removable media has to be used, it must be scanned by approved Anti-virus before and during use.
All web traffic must be routed through a proxy which logs and monitors internet access. This reduces the chance of malicious sites infecting end user devices. The proxy is configured in agreement with the security team. Email must also be routed through email scanning services. Direct Internet access should only be configured for update services, and by exception only.
Allow the installation of applications only from approved stores.
Systems must be able to be updated and must be kept up-to-date with OS and application upgrades and patches. Where possible, software updates should be configured to update automatically. Refer to the Vulnerability Scanning and Patch Management Guide for further information.
A formal process must be developed and documented to ensure all firewall configuration changes are approved before being implemented.
Be aware of the risks of ' watering hole attacks ' that use GitHub or other open source code repositories. These attacks place malware into popular sites. Avoid trusting code, components, or other resources from popular sites. Refer to the Access Control Guide for further information.

Do

- # 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

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

Malware Protection Guide: Defensive Layer 2**Introduction**

This guide explains the types of controls that need to be implemented to form the second of three layers of defence. This guide is a sub-page to the [Malware Protection Guide](#).

Who is this for?

This Malware Protection information is mainly intended for in-house Ministry of Justice (MoJ) Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other MoJ bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the MoJ, will also find this information helpful.

Defensive Layer 2: Preventing malicious code from being executed

Layer 1 might not always prevent malware from reaching the network. Assume that malware can and will reach MoJ devices at some point. The next layer of protection prevents malicious code from taking effect. The following tables outline ways in which you can help prevent malicious code from executing.

Do

- # Ensure that all systems and endpoints are scanned by anti-malware software. Refer to [Note 1](#) for more details.
- # Ensure that if you are developing a new Microsoft Windows based system, that the 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.

- Don't make statements that defame, slander or lower the reputation of the MoJ, any person or organisation.
- Don't forward email [chain letters](#) to your contacts. Instead, report them to security@justice.gov.uk.
- Be aware of unsuitable attachments, for example video clips, images, or executable files. MoJ email automatically filters many unapproved attachment types, particularly those that can contain executable files. Emails containing those attachments are likely to be quarantined and not delivered.
- Avoid excessive use of email, and sending email to large numbers of recipients. Ask yourself if it really makes sense to "Reply All"?
- Any recipients in the "To" or "Cc" fields can retrieve the addresses of all other recipients in those fields. If you are sending an email to a list of people outside MoJ, where privacy of individuals might be relevant, place your list of recipients in the "Bcc" field and set the "To" field to your own address. This ensures that none of the recipients can retrieve the identities of the other recipients.
- Keep your operating systems up to date to prevent susceptibility to viruses.
- Scan email attachments to detect viruses and other malware.

Be aware that the MoJ monitors the use of electronic communications and web-browsing. Your manager can request reports detailing your activity if they suspect inappropriate use of email or web-browsing facilities.

[Ask](#) if you want further information.

Monitoring

The MoJ monitors all email for security purposes.

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

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

Email threats

Although email is a powerful business tool, it has problems. In this guidance, we describe some of the problems, and how you can avoid them.

Email threats often use familiar email addresses to disguise attacks, or to pose as valid emails. Email threats are becoming more frequent and pose one of the biggest problems for MoJ systems and services.

There are many possible threats, including:

- Viruses: These can be spread between computers in emails or their attachments. They can make PCs, software or documents unusable.
- Spam: This is unsolicited mail sent in bulk. Clicking on links in spam email may send users to phishing websites or sites hosting malware. Often email spam mimics the addresses of people you know.
- Phishing: These are emails disguised to look like a legitimate company or bank to illegitimately obtain personal information. They usually ask you to verify your personal information or account details. Often links will direct you to a fake website, made to look like the real thing.
- Social engineering: In the context of security, social engineering refers to manipulating people to do something or divulge confidential information. For example, you might get a call from someone pretending to be from a software supplier, claiming that a virus has been found on your PC; they demand personal details before they can remove the virus.
- Spoofing: A spoofed email is where the sender (in this case, a criminal) purposely alters part of the email to make it look as though it was from someone else. Commonly, the sender's name/address and the body of the message are made to look as though it was from a legitimate source. It is commonly used to trick the recipient into providing confidential information such as passwords, or to market an online service dishonestly, or to sell a bogus product. Check the real sender of any email you receive if you ever have any doubt or uncertainty. If the sending address is one you don't recognise, do not click on any link contained within the email.

The MoJ scans approximately 14 million messages a month for threats (figures from November 2020). Of these, we might expect to find 1.4 million "spam" messages, 150,000 "phishing" messages, and about 1,000 malware messages (including viruses). Unfortunately, not every virus or spam email will be identified and blocked. The good news is that there are some simple steps you can take to reduce the threat:

- If you are not expecting the email, do not reply to it.
- If you are at all suspicious, do not divulge your details or any sensitive information.
- Avoid opening potential scam emails.
- Don't open unexpected attachments or click on strange links in emails, even if the email appears to be from someone you know. Check the style and content; if it isn't consistent with previous emails, it could be a scam.
- Do not reveal personal or other sensitive information in response to automatic email requests.
- Avoid sharing your business email address on the internet. These might be collected and used by automatic 'harvesting' software programs.
- Never use your MoJ email address to register for non-work related sites.

If you think you've received a scam email, or a virus, [report it immediately](#). Do not click on any link or forward it to anyone. Only delete it from your inbox when you have been told to do so.

Further reading from the NCSC

[Email security and anti-spoofing](#)

Other email problems

Auto-forward

Auto-forwarding is where you get your email system to send emails automatically to another account. This might seem very useful, especially if for some reason you can't access your normal business email account, for example while you are away on holiday.

But auto-forwarding is very risky.

You can't be certain that the forwarded emails are safe to send to the new account. For example, the new account might have weaker technical security, making it easier for a hacker to break in and read your email.

You might also be auto-forwarding emails sent to you from outside the MoJ; perhaps from another government department or commercial organisation.

When an email is sent to you, you are responsible for ensuring that everything in the email is handled correctly. This means looking after it to the standard required for that information. You mustn't send that information to another email address, where the required security standards might not be met.

Never use auto-forwarding to forward emails from your MoJ business email address to another non-MoJ email address. In particular, never forward email from your MoJ business email address to a personal email address.

Note: An external email service is any service that is outside the .gov.uk domain.

There might be occasions when you have a genuine business need to auto-forward email to another email account, where the new address has the same or higher security standards. An example is forwarding from an MoJ business email address to another MoJ business email address. If you have business need for this, [ask for help](#).

Chain letters

These are letters sent to several people who are asked to send copies to several others. They sometimes threaten that bad things will happen if the letter is not forwarded. Chain letters are a hoax.

Chain letters usually do not have the name and contact information of the original sender so it is impossible to check on their authenticity.

Legitimate warnings and solicitations will always have complete contact information from the person sending the message.

Newer chain letters may have a name and contact information but that person either does not exist or is not responsible for the hoax message.

Warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist, are probably hoaxes.

Don't circulate warnings yourself; real warnings about viruses and other network problems are issued for everyone by MoJ technical services.

Note: When in doubt, don't send it out.

Scams

Scams are "get rich quick" schemes. They make claims such as promising your bank account will soon be stuffed full of cash if follow the detailed instructions in the letter or email. In reality, it is an illegal plan for making money.

A typical scam includes the names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then remove that name and add yours to the bottom.

You are then supposed to mail copies of the letter or email to a few more individuals who will hopefully repeat the entire process. The letter promises that if they follow the same procedure, your name will gradually move to the top of the list and you'll receive money.

Other high-tech scams using IT also exist. They might be sent over the internet, or may require the copying and mailing of computer disks rather than paper. Regardless of the technology used to advance the scheme, the end result is still the same.

Scams are a bad investment. You certainly won't get rich. You will receive little or no money. The few pounds you may get will probably not be as much as you spend making and mailing copies of the letter if hard copy.

By their very nature, scams are harassing. Sending such mails using MoJ facilities is prohibited. The misuse of computer resources to harass other individuals or groups is unacceptable. Any person tempted to forward an email scam should familiarise themselves with the HR intranet pages, particularly the section regarding disciplinary action and electronic communications.

Note: Scams also clog up the system and reduce the efficiency of our servers.

How to recognise a scam

From the older printed letters, to the newer electronic kind, scams follow a similar pattern, with three recognisable parts:

- A hook: this to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl is dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
- A threat: when you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. Others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.
- A request: some older chain letters ask you to send money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to "Distribute this letter to as many people as possible." They never mention clogging the internet or the fact that the message is a fake; they only want you to pass it on to others.

If it sounds too good to be true, then it is!

Bogus calls

There are a range of scams that can target you at home or at work. Callers usually say they are from IT Support, and tell you that they have detected a virus on your machine that needs to be removed. The bogus caller will then either:

- Direct you to a website, in the hope you will download malicious software.
- Try and obtain details from you about your computer, or the MoJ network.

In all genuine situations, the MoJ IT Service Desk will provide you with an incident reference number if there is a real problem with your machine.

If you receive a call from someone claiming to be from the IT Service Desk, always ensure you ask them for the incident reference number. Then disconnect the call, and call the IT Service Desk yourself, directly. If the original call was genuine, when you provide the incident reference number, they will be able to help you.

In general:

- Treat all unsolicited calls as suspicious.
- If possible, note the details and incoming telephone number of the caller.
- Do not go to any external site if directed from an unsolicited call.
- Never give any information about your computer to the caller.
- Check if the call is genuine with your IT Service Desk. [Report the call](#) as a security incident if it is not. Use a different phone from that used to take the original call.

Hoaxes

Hoax letters are designed to trick you into believing, or accepting as genuine, something false and often preposterous: the messages they contain are usually untrue.

Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people. Who wouldn't want to warn their friends about some terrible virus that is destroying people's systems? Or help this poor little girl who is about to die from cancer?.

Chain letters and hoax messages have the same purpose but use a slightly different method of coercing you into passing them on. Chain letters, like their printed ancestors, generally offer luck or money if you send them on (scams). They play on your fear of bad luck and the knowledge that it is easy for you to send them on. Scams play on people's greed and are illegal no matter what they say in the letter.

The risk and cost of hoaxes

The cost and risk associated with hoaxes may not seem to be that high. If, however, you consider the cost of everyone within the MoJ receiving one hoax message, spending two minutes reading it and another two minutes forwarding it on or discarding it, the cost can be significant.

Handling these messages may also make our mail servers slow down to a crawl or crash.

Spammers (bulk mailers of unsolicited mail) may harvest email addresses from hoaxes and chain letters. Many of these letters contain hundreds of legitimate addresses, which is what the spammers want. There are also rumours that spammers are deliberately starting hoaxes and chain letters to gather email addresses.

How to recognise a hoax

A request to "send this to everyone you know" (or some variant) should raise a red flag. The warning is probably a hoax. It's unlikely a real warning message from a credible source will tell you to send it to everyone you know.

If the warning uses technical language, most people, including technologically savvy individuals, tend to believe the warning is real.

There may be credibility by association. If the janitor at a large technological organisation sends a warning to someone outside of that organisation, people on the outside tend to believe the warning because the company should know about those things. Even though the person sending the warning may not have a clue what he is talking about, the prestige of the company backs the warning, making it appear real.

These make it very difficult to be certain a warning is a hoax. Check if the claims are real, and if the person sending out the warning is a real person. Ask yourself if they are someone who would know what they are talking about.

Type of hoaxes

Scam chains

Mail messages that appear to be from a legitimate company but that are scams and cons, for example [Advance fee scams](#).

Giveaways

Stories about giveaways by large companies. If you only send this on, some big company will send you a lot of money, clothes, a free vacation, etc., etc. You would have to wait forever for any of these to pay off.

Malicious warnings (virus hoaxes)

These are warnings about Trojans, viruses, and other malicious code, that have no basis in fact.

Virus hoaxes have flooded the internet with thousands of viruses worldwide. Paranoia in the internet community fuels such hoaxes. An example of this is the "["Good Times" virus hoax](#)", which s□Don, soS

This means that the MoJ implements a number of controls for email systems:

- [Sender Policy Framework](#)
- [Domain Keys Identified Mail](#)
- [Domain-based Message Authentication, Reporting and Conformance](#)
- [Mail Transfer Agent Strict Transport Security](#)
- [TLS Reporting](#)

Related information

[Email Security Guide on page 348](#)

Sender Policy Framework

Sender Policy Framework (SPF) **SHOULD** be implemented for email domains. SPF enables organisations to publish a Domain Name System (DNS) record of all the domains and IP addresses which are trusted for sending and receiving email.

SPF is verified by checking a specific TXT DNS entry in emails. Emails are flagged if they are not sent from the domains and IP addresses published in the DNS record.

The MoJ enforces SPF controls to help users spot spoofed or unknown email addresses. Suspicious emails are sent directly to the "spam" folder, instead of to the user's inbox.

When creating an SPF record in the public DNS, use all the IP addresses or address ranges from which an email might be sent. You can use both IPv4 and IPv6 addresses. An SPF record might look like the following:

- An example of a basic SPF record to be added to an organisation's public DNS, where it uses Google, might be:

```
v=spf1 include:spf.google.com ~all
```
- An SPF record including Google's IP ranges and a sending service with an IP address range, might be:

```
v=spf1 include:spf.google.com ip4:80.88.21.0/20 ~all
```
- An example of a more complex record, with additional services and some dedicated IP addresses, might be:

```
v=spf1 include:spf.protection.outlook.com include:mail.zendesk.com
ip6:2001:db8::/32 ip4:203.0.113.6 ~all
```

In the previous examples, v=spf1 is an SPF record, include: means email can only come from these sources, ~all considers any other email as a soft fail, and -all considers any other email as a hard fail.

Note: A hard fail **SHOULD** be used when a domain is being forged by spam.

To correct SPF failures, add the sending systems you use to your SPF record. Do this using either the IP address or by reference to another SPF record. These previous examples are unique, so check the actual domain or IP range of the email sending service. Also check with the supplier on setting up SPF records.

Domain Keys Identified Mail

Domain Keys Identified Mail (DKIM) **SHALL** be enabled for all MoJ email domains. DKIM enables automatic filtering or rejection of emails that fail DKIM verification.

- DKIM can verify a sender domain by looking up the sender's public key published in the DNS. You can then determine if an email has been tampered with during transit, for example during a "Man-In-The-Middle" attack.
- A valid digital signature provides assurance that the hashed content has not been modified since the signature was affixed to the email message.
- The MoJ enforces DKIM controls to help users identify communication tampering attacks by sending the messages directly to the spam folder, instead of to the user Inbox.
- DKIM **SHALL** be used across the MoJ, including by executive agencies and ALBs.

Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication standard that **SHALL** be used with SPF and DKIM to:

TLS Reporting

TLS Reporting (TLS-RPT) is a protocol that allows a domain to advertise a destination for sending email services to report the success or failure of encryption in transit.

The MoJ **SHALL** implement and use TLS-RPT for MoJ email systems.

To 'enable' TLS-RPT, publish a DNS record telling mail sender tools where to send TLS-RPT reports. A sending email service checks for the record, and if one exists it is used to send a report to the address provided.

For more information on UK Government configuration and use of TLS-RPT, refer to the [published guidance](#).

Making changes to the domain name system

Changes **SHALL** be made to DNS records when implementing SPF, DKIM, DMARC, MTA-STS, and TLS-RPT controls. When requesting changes, specific information **SHALL** be included for each record. If given the option, set a short time to live (TTL) in DNS records to monitor changes quickly, and fix any issues.

DKIM example

Record type: TXT

Host or record name: selector.domainkey

Put your selector, or the selector provided by your service provider, in place of selector in the host or record name.

Record value: v=DKIM1; k=rsa; p=<your DKIM key>

Paste your DKIM key from your key generator in place of <your DKIM key>.

Some providers might use a CNAME record instead of a TXT record. Follow the guidance from your provider.

GSI is no longer used, but the following addresses still route through to @justice.gov.uk. The following table shows the authorised users you can contact to request DNS changes:

Record Type	Contact
*.gsi.gov.uk, *.gsx.gov.uk, *.gse.gov.uk, *.gcsx.gov.uk, *.*.gsi.gov.uk	Vodafone Contact GDS
*.gov.uk or any other domains	Your registrar, DNS provider or Internal System Admin
*.cjsm.net	Egress

DMARC example

Record type: TXT

Host or record name: dmarc

Record value: v=DMARC1;p=none;fo=1;rua=mailto:dmarc-rua@dmarc.service.gov.uk,mailto:dmarc@<yourdomain.gov.uk>

Create the email address and put your domain in place of <yourdomain.gov.uk>.

SPF example

Record type: TXT or CNAME (check guidance for your service on which to use).

Host or record name: @ (if required)

Record value: v=spf1 include:<your email server domain> ip4:<your email service IP>
~all

Put your email server domains or email sending IP ranges in place of the < > sections. You do not need to include both. In many cases you might only need include:.

DNS contact details

For DNS changes and associated advice, contact the Platforms and Architecture team: domains@digital.justice.gov.uk

Contact details

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

Email blocking policy

POLEBL004 : When establishing the criteria for adding an item to the blocklist, the MoJ **SHOULD** go through an impact assessment to establish the impact of adding the specific item to the internal blocklist. If the impact might be substantial, for example causing widespread disruption, or where legitimate emails might be blocked, then the blocking object **SHOULD** be reconsidered or rescoped.

POLEBL005 : As part the review process, or as a result of a user reported issue such as an incident reported through a user's local IT Team, a legitimate email might become blocked because it is now on a blocklist. This might be where the email address was added to the blocklist manually, or incorrectly flagged by automated tools in the email system. In this scenario, the MoJ **SHOULD** promptly unblock affected emails, and re-evaluate the blocking rule responsible, in line with this policy. This unblock **SHOULD** happen through the incident management process. All users are encouraged to speak with their Local IT team about concerns with email delivery, or email blocking.

POLEBL006 : In the event that a legitimate email is blocked by an automatic vendor driven process, or included as an "indicator of compromise" through a threat intelligence product, the MoJ **MIGHT** request that the object be reviewed or reclassified.

POLEBL007 : Before adding any object to the blocklist, or automatically removing it from an MoJ mailbox, impact analysis **SHALL** be carried out and documented through the MoJ change/incident management process.

Deletion of existing emails in scope for blocking

POLEBL008 : As part of the blocking procedure, the [Operational Security Team](#) **SHOULD** have the ability to delete or purge emails across the estate which match the blocking criteria listed in the blocklist. This is an optional step, done at the discretion of the [Operational Security Team](#).

POLEBL009 : Purging of existing emails which have been added to the blocklist **SHALL** be done under peer review. Peer review **SHOULD** be completed by an independent member of the team who is not involved directly in the analysis or investigation of the email. Peer review takes place only if there is a further threat of users interacting with the newly classified email.

POLEBL010 : If deletion of emails takes place, then details of the criteria **SHOULD** be included as part of the documentation process recorded as part of change or incident management.

POLEBL011 : Where appropriate, users are encouraged to delete for themselves any emails confirmed to be in scope for blocking or deletion. Deletion of emails by the [Operational Security Team](#) **SHOULD** take place only where there is a significant number of users who received the newly classified email.

POLEBL012 : Removing emails from recipient mailboxes is a viable alternative to adding emails to an email blocklist. This **SHOULD** be the preferred option to prevent users from interacting with emails considered for blocking or removal.

POLEBL013 : Deletion of emails **SHOULD** be done in such a way that the email could be recovered if required. If this is not possible, the email **SHOULD** be moved to the users 'junk' folder rather than simply being deleted.

POLEBL014 : Users **SHOULD** be made aware of the deletion of emails. However, this is not mandatory.

POLEBL015 : The MoJ has no responsibility to delete emails from unmanaged MoJ mailboxes.

POLEBL016 : Automatic deletion of emails for users **SHOULD** be done through automated processes. The [Operational Security Team](#) **SHALL** minimise access to the mailbox from which unwanted emails are purged.

Automated blocking tools

POLEBL017 : MoJ email services **SHOULD** come with inbuilt vendor managed blocking facilities based on known Indicators of Compromise (IOC's) to prevent emails entering or leaving the MoJ email environments. This vendor managed list **CAN** either be done through general lists of IOCs, or heuristic scanning.

POLEBL018 : The email service vendor **SHOULD** provide the MoJ with the ability to reclassify incorrectly classified emails. This reclassification process **SHOULD** be accessible to the MoJ Cyber Security team, as well as email administrators.

The Cyber Security Team encourages the integration with 3rd party threat intelligence feeds from trusted providers as part of the in-depth defence strategy.

Blocking or deleting received emails

POLEBL019 : Any MoJ user who receives an email suspected to be one of the [types described previously](#) CAN request that the email be blocked, preventing future similar emails from being received. On receipt of this, the MoJ reviews the evidence and determines if addition to a blocklist is appropriate. Further actions taken follow the policy statements in this guidance.

POLEBL020 : Addition of emails to the blocklist is completed by either the local email service management team, or by the [Operational Security Team](#). If the former, then approval **SHALL** be obtained from the [Operational Security Team](#).

POLEBL021 : In the event that an email is causing widespread disruptions or impacting business, then the individual email administration team responsible for the email platforms CAN delete emails or place blocks on emails without prior approval. This **SHOULD** be done under change and incident management, with notifications sent to the [Operational Security Team](#).

POLEBL022 : The MoJ **SHALL** provide a way for users to request emails for review by the relevant teams.

Preemptive blocking

POLEBL023 : If MoJ security receives intelligence about a credible threat to the confidentiality, integrity, or availability of an MoJ managed email service, then those emails **SHOULD** be added to the blocklist. Before blocking according to this policy statement, the intelligence **SHOULD** go through an impact analysis.

POLEBL024 : All blocks **SHOULD** remain in place until the threat is no longer a credible threat to the MoJ.

POLEBL025 : Email from previously known or blocked items **MAY** be re-added to the list if there is credible information or grounds to do so.

Automatic blocking of emails based on attachments

POLEBL026 : The MoJ **SHOULD** be able to restrict the delivery or sending of emails with certain malicious file attachment types.

POLEBL027 : A complete list of email attachments blocked **SHOULD** be kept and managed by the individual email administrators, and **SHOULD** be consistent across different email services in use across the MoJ estate.

Contact details

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

Email blocking process

The Ministry of Justice (MoJ) manages a number of different mail platforms, including infrastructure in Google Workspace, as well as Microsoft Exchange (on-premise) and Microsoft Cloud platforms.

There are numerous reasons that email might be blocked. An email matching the criteria on a blocklist is only one reason.

If you have any concerns about email delivery, contact your email service provider or Infrastructure exchange team.

Related information

[Email blocking policy](#) on page 342

[Email Security Guide](#) on page 348

Definitions

Within this guidance, 'email' might refer to individual user mailboxes, shared or group mailboxes, or distribution lists and mailing lists.

More specifically, a recipient or mailbox is any functional MoJ email account, for example security@justice.gov.uk.

Throughout this guidance, references to malicious emails include the following specific threats:

- Emails which contain malware.
- Phishing emails.
- Spoofed or impersonal emails.
- Harmful emails.
- General spam emails.

There are a number of different email threats that exist in information technology. Each threat varies in complexity, and the impact it might have on the MoJ and its employees.

Spam

Spam emails, also called junk emails, involve the sending of nearly identical messages to numerous recipients. They are high volume, unsolicited messages.

Malicious or malware

These emails are specifically designed to damage operational systems or disrupt business operations. While the email itself may not be malicious, it might contain URLs or file attachments which are malicious.

Phishing

This is an email-based attempt to acquire sensitive information such as credentials including IDs and passwords for malicious purposes. Phishing emails typically masquerade as a trustworthy person supposedly taking part in electronic communications.

Spoofed or impersonation emails

These emails are from a forged sender address. At first glance, the email seems to be from a respected or reputable email sender, or an individual you know or trust.

Harmful emails

These are emails that are not necessarily classified as malicious, but might cause distress or harm to users. Examples include threatening emails, or Denial of Service (DoS) attacks.

Email blocklist

The purpose of any email blocklist is to prevent malicious emails entering or leaving the MoJ email infrastructure.

A blocklist consists of some or all of the following elements:

- IP address.
- Network range.
- Domain name.
- Email address.
- URL.
- Other email characteristics.

Each element helps identify more precisely where the sender is suspected of delivering malicious emails.

Throughout this document, any item on the email blocklist is referred to as a 'blocklist object'.

Each individual mail platform has its own set of objects that can be added to the blocklist. These objects vary from product to product.

Note: Users **SHOULD NOT** interact with any unsolicited or unwanted emails. Instead, follow email spam handling processes. For more information on this, contact your local IT Service Desk.

All email platforms in use by the MoJ **SHALL** have the ability to add items to the blocklist. The MoJ security team **SHALL** have appropriate permissions to update and review items on this list.

Internal blocklist

There are two specific types of blocklists:

Impact assessment

Any blocklist object **SHOULD** be defined so as to not result in widespread email failures. For example, it would not be helpful to block the whole of @gmail.com. Each blocklist object **SHOULD** be examined, taking into account the characteristics of the specific blocklist, and relevant intelligence sources.

Senders that have an established history of clean or legitimate emails, but have recently been sending emails of concern, **SHOULD NOT** be added automatically or instantly to the blocklist. Instead, the sender **SHOULD** be 'quarantined' by the affected email system.

Avoiding the use of blocklists

Requests are sometimes made to block individual senders based on repeat, vexatious, or otherwise undesirable content. Take care when determining whether the sender truly has malicious intent, or whether they are a simply a member of the public with a genuine grievance but lacking the skills to air their concerns more constructively. Consider the risk of 'denying access to the criminal justice system' to an individual. If in doubt, refer to the [Data Privacy Team](#) or Chief Information Security Officer (CISO).

Documentation for internal blocklists

Use the MoJ incident management and change management process to add emails to internal blocklists. This includes documenting expected impact, and other relevant information.

As part of the documentation steps, the assessment and justifications for blocking specific objects **SHOULD** be included. Ensure the information is brief but contains sufficient relevant information. The relevant information **SHOULD** include:

- The specific items to be added to the internal blocklist.
- The classification of the email, and justification for blocking.
- Summary outcomes from the impact assessment.
- Summary actions taken to triage and resolve the incident, before resorting to blocking.

One ticket might contain multiple different blocking objects.

If an item is blocked without a corresponding ticket and justification as described in this guidance, then that object **SHALL** be removed from the internal blocklist with immediate effect.

Review of existing blocks

The MoJ **SHALL** review items manually added to the internal blocklist, on a regular basis, to determine if they are relevant or not. Regular means at least every quarter. Any item included in the list and which is considered irrelevant **SHOULD** be removed. An irrelevant item is one that blocks legitimate emails from entering the MoJ email system.

A review of internal blocklist **SHOULD** also be done frequently, in line with the time for which blocked email messages are kept. This ensures the MoJ is able to recover incorrectly-blocked emails, and avoid them being deleted automatically.

Spam emails

The [ICO website](#) provides general information about spam, and gives advice about the steps to reduce spam.

A spam email does not necessarily require automatic and instant inclusion on the internal blocklist, although it might be included as part of the external blocklists, as highlighted in this policy.

Blocklist listing policies

The MoJ email platforms **SHOULD** have the ability to deploy automatic blocking of traffic. This includes blocking the following email classifications:

- Spam traffic.
- Malware traffic.
- Open proxy or open relays.
- Shared cyber threat intelligence.

- Spoofed domains.

Reporting incidents to external companies

The MoJ reserves the right to forward any email suspected of being added to the blocklist to external organisations for verification.

Organisation that are trusted by the MoJ for this purpose include:

- Google.
- ICO
- Microsoft.
- Netcraft.
- NCSC.

In such cases, after forwarding, the MoJ **CAN** delete email messages from affected mailboxes.

Contact details

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

Email Security Guide

This guide sets out the requirements for implementing and maintaining email security across the Ministry of Justice (MoJ).

Related information

- [Email Authentication Guide](#) on page 338
- [Email blocking policy](#) on page 342
- [Email blocking process](#) on page 344
- [Secure Email Transfer Guide](#) on page 358
- [Spam and Phishing Guide](#) on page 364

Who is this for?

This guide is aimed at two audiences:

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

These audiences are referred to as "technical users".

Roles and responsibilities

All technical users are responsible for maintaining and using the MoJ's email communications securely, in line with the requirements set out in this guide. In particular:

- Where possible, automate checks of the sender's authenticity by implementing the controls in the [Email Authentication Guide](#).
- Ensure all email communications are protected according to the classification of the information held within them. There is more information in the the [Information Classification Handling and Security Guide](#).
- Discourage people from downloading data to mobile devices. Instead, encourage and enable the use of cloud services such as Office 365.
- Make it easy for people to send suspected or actual phishing emails to the IT Service Desk, so that the emails can be handled safely.
- Keep operating systems up-to-date, to prevent susceptibility to viruses.

- Scan email attachments to detect viruses and other malware.
- Ensure email services are appropriately authenticated. Refer to the [Email Authentication Guide](#) for more information.
- Ensure secure email messaging services, and, where necessary, encryption tools, are used to transfer sensitive information and system secrets. Refer to the [Secure Email Transfer Guide](#) for further information.
- Ensure that email configuration is secure, and that all necessary technical controls, including those set out in the [Malware Protection Guide](#), are implemented and kept up to date.

Note: Suppliers **MAY** use their own email services if agreed by the MoJ but, as a minimum, they must meet the MoJ security requirements.

Authorised access to user accounts

By default, users **SHALL NOT** access the email accounts of any other users, unless they are authorised to do so as required by their role. Access is authorised on a case-by-case basis only, and is normally aligned to the following circumstances:

- After a criminal investigation has been opened by a law enforcement agency.
- After an employee investigation has been opened relating to misconduct or a security incident, for example IT misuse.
- Upon the death or unexpected exit of an employee, for example to enable retrieval of business information or closing down an account.
- For long-term archiving of information no longer in current use.

Anyone required to enable or carry out authorised access to a user account should follow the guidance in the [Privileged User Guide](#).

Monitoring

The MoJ does monitor Email services for security purposes.

Delegate access

Ensure that standard end users do not by default have the permissions necessary to provide another user with delegate access to their account. There will, however, be occasions when an MoJ IT user might need to give another user access to their email account.

Examples would be where a mailbox owner has a legitimate requirement for another user to:

- Read, send, or delete messages on their behalf.
- Manage their calendar.

In this situation, the user **SHALL** first seek permission from their line manager. When permission is granted, technical users **SHALL** ensure secure delegation by:

- Enforcing mailbox owners to limit delegate access to pre-defined periods of time.
- Enabling mailbox owners to manage and revoke access themselves.
- Prevent federated sharing, where users in one organisation can share free or busy calendar information with recipients in other organisations.
- Preventing auto-forwards to external email services, including personal email accounts.
- Preventing delegate access to unauthorised users, such as people outside the MoJ), by enforcing Role Based Access Control (RBAC).
- Implementing [Access Control Policy](#), in particular regarding access to email as a result of forwarding or delegation.

For individual accounts, the IT Service Desk can configure delegate access. Administrators of group inboxes can also configure delegate access to those inboxes.

For further details, refer to the [Privileged User Guide](#).

- We can transfer records to The National Archives.

Always store MoJ information in MoJ systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate MoJ system. Guidance on what you must keep is available on the Intranet [here](#). At regular and convenient intervals, transfer the information to an appropriate MoJ system. Do the same when you finish the work. Don't forget to remove any redundant information from a tool by clearing or deleting data if it has been preserved in an MoJ system.

Many tools let you export your data. You can then store it on an appropriate MoJ system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the [Information Management](#) section on the Intranet. There is also help on [responding to requests for information](#).

Acceptable Use

You must use communications tools for business purposes in an [acceptable way](#).

Be sensible when using communications tools for MoJ business purposes:

- Be extra careful with sensitive and personal information in tools.
- Try to avoid using the same tool for business and personal use - you can get confused who you're talking with.
- If the message you're about to send might cause problems, upset, offence, or embarrassment, it's not acceptable.
- Context is important - a message you might think is funny could be upsetting to someone else.
- If something goes wrong, report it.

The bottom line is:

If there is doubt, there is no doubt - ask for help!

Approved tools

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Apple Facetime	Communication tool: Video	Avoid personal or sensitive data	Smartphone App	Internal/ External
Apple iMessage	Text messaging	Avoid personal or sensitive data	Smartphone App	Internal/ External
Google Meet (was Google Hangouts)	Communication tool: Video and/or voice	MoJ use approved for OFFICIAL and OFFICIAL-SENSITIVE	IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Microsoft Teams	Communication and collaboration tool: Video and/or voice	MoJ use approved for OFFICIAL and OFFICIAL-SENSITIVE	Dom1 Software centre, IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Miro	Collaboration tool: Whiteboarding	Avoid personal or sensitive data	Web browser.	Internal/ External
Skype for Business	Communication tool: Video and/or voice	MoJ use approved for OFFICIAL and OFFICIAL-SENSITIVE	Dom1 Software centre, IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Slack	Text messaging, Voice/Video calls, etc.	Avoid personal or sensitive data	IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Slido	Q&A tool during presentations	Avoid personal or sensitive data	Web browser.	Internal
Trello	Project management tool, 'Kanban' cards	Avoid personal or sensitive data. An enterprise-wide MoJ licence is available. Ensure you create Trello boards in the MoJ workspace. Do not use a personal Trello account.	Web browser based use. Log in using your MoJ single sign-on account, for example a Digital & Technology Google account, or a Microsoft Office 365 account.	Internal
Twitter	Text Messaging, Video transmission	Approved for 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, or dedicated and installed app by approval	External meetings. For Internal meetings, use Microsoft Teams.

NHS Track and Trace

The official [NHS Covid-19](#) app was designed by the NHS. Both NCSC and Cabinet Office have been involved in the security of the system. The app provides contact tracing, local area alerts and venue check-in. It enables you to protect yourself and your loved ones. Installation is optional, but recommended.

After installing the app, you'll receive an alert if you have been in close contact with other people who have tested positive for coronavirus. You can then take action to avoid passing the virus on, for example by self-isolating.

From a security perspective, it is safe for you to use the app on your personal or MoJ issued devices. There are no extra risks for colleagues with security clearance, such as SC and DV.

If you wish to install the app, start at the [NHS site](#).

Note: The NHS app may not work on some older MoJ devices. Installation might not be possible, for example on Quantum smartphones.

You might have both a personal and an MoJ issued device. Think about which device makes most sense to use with the app. It's best to install on the device that you carry with you and use most of the time. You could install on all your devices if you prefer.

To reduce the likelihood of false alerts on the app, turn off the app's Bluetooth mode. Do this when:

- You are working in environments with protective Covid measures in-place, for example plexiglass separators.

- You need to leave your personal or work device in a locker, for example during a sports activity or to work in a secure MoJ facility.

Other tools

Some tools, such as Facebook, Instagram and LinkedIn, are approved for specific corporate accounts to use, for corporate communications messages. General use of these tools for work purposes is not permitted.

If you wish to use a tool that is not listed in this guidance, please consult our [Guidance for using Open Internet Tools](#) and [speak to us for help](#).

Requesting that an app be approved for use

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

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

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

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

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

Other information

Government policy and guidance

[GDS Social Media Playbook](#)

NCSC

[Video conferencing services: using them securely](#)

[Secure communications principles](#)

[Using third-party applications](#)

Secure Data Transfer Guide

Introduction

This guide outlines the security procedures and advice for Ministry of Justice (MoJ) staff wanting to send or receive data securely from external sources.

This is important to the MoJ, because personal and sensitive data is regularly transmitted between departments. Legislation such as GDPR, and industry standards such as PCI DSS, affect the MoJ's responsibility to secure this data. It is also important to recognise the damage that leaked sensitive data could cause to the vulnerable people the MoJ works to protect.

Who is this for?

This policy is aimed at three audiences:

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

Distribution

Internal within Authority:

Action:

- Authority Security & Privacy

Information:

- Director of Authority Service Delivery
- Head of Service Delivery
- Authority Commercial

External:

Action:

- <ORGANISATION SHORTNAME>

Supplier corporate IT

The Ministry of Justice (MoJ) does not by default prohibit the use of supplier organisation corporate IT for processing MoJ data. The expectation is that the supplier corporate IT environment is well designed, maintained, governed, and defended, in line with large scale commercial threat models.

Subject to the requirements described in this document, the MoJ does not require suppliers to create or maintain dedicated or segregated IT solutions for processing MoJ data classified at OFFICIAL.

For MoJ data classified at OFFICIAL-SENSITIVE, additional comprehensive security assurance is required. The assurance **SHALL** include controls and governance processes. The assurance **SHALL** be appropriate to the information sensitivity. Contact the [Cyber Assistance Team](#) for assistance regarding acceptable security assurance for OFFICIAL-SENSITIVE MoJ data.

Technical security

Supplier corporate IT systems are expected to maintain appropriate levels of technical security defences. These defences **SHALL** protect appropriately all types of MoJ data. This includes MoJ data processed or stored in any way by supplier corporate IT systems.

Examples of appropriate defences include, but are not limited to:

- Use of current Transport Layer Security or IPSec for in-transit encryption.
- Hashing and cryptography mechanisms for data stored at-rest.

The defences **SHALL** scale from individual data items in a database, up to entire storage facilities.

Supplier systems **SHALL** be proportionally resilient to malware. This might be achieved by ensuring segregation between systems, users, and data. Other industry standard best practices, such as email attachment scanning or filtering, might also be suitable.

Email security

Supplier corporate email systems processing MoJ data **SHALL** align to the [UK government secure email policy](#), thereby following widely accepted best practices.

Supplier corporate email systems are not required to integrate to the Public Services Network (PSN).

Data Governance

Data offshoring

Supplier's **MAY** process MoJ data, including Personal Data for which the MoJ is responsible, outside of the United Kingdom, subject to the maintenance of acceptable information controls and governance.

MoJ data **SHALL NOT** be processed within a legal framework that is incompatible with that of the United Kingdom.

Working overseas

Supplier staff are not prohibited from working overseas while processing OFFICIAL MoJ data, subject to implementing and maintaining acceptable information controls and governance. In particular, the controls and governance **SHALL** align and comply with MoJ policy on [remote working](#) and [working overseas](#).

When working overseas, it might be necessary to limit access to information while the user travels. Alternatively, it might be appropriate to use secondary, temporary accounts, to avoid primary account compromise. Contact the [Cyber Assistance Team](#) for assistance regarding acceptable security assurance when working overseas.

Data backups

Supplier corporate IT systems **MAY** backup data for extended retention times. An example would be 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, but instead are subject to a system-wide backup rotation or retention schedule.

Suppliers **SHALL** discuss and agree these cases with the MoJ.

Local end-user device data

The MoJ acknowledges that corporate users typically "download" files, for example from local email client caching to file downloads using a web browser. These files might remain within `Downloads` folders, until explicitly deleted by the user.

Suppliers **SHALL** include and address these types of data locations in data governance regimes.

Contact details

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

Supplier service delivery management

Azure Account Baseline Templates

The lowest acceptable common denominator to appeal to the largest possible number of people for security-related promises, capabilities and configurations of Ministry of Justice (MoJ) Azure accounts.

Baseline

The baseline for Azure accounts is formally published as part of the Security Guidance from the MoJ Digital and Technology Security and Privacy team.

Background

As an organisation expands its use of Azure services, there is often a conversation about the need to create multiple Azure subscriptions to ensure separation of business processes or for security, compliance, and billing. We tend to use separate Azure subscriptions for each business unit so that it can meet the different needs of the organisation. Although creating multiple subscriptions has simplified operational issues and provided benefits like security and resource isolation, a smaller blast radius, and simplified billing, it results in widely varying security posture across the subscriptions and there is the need to align all of these subscriptions to a baseline secure standard.

Areas of Concern

[Azure Security Center](#).

[Azure Identity Management \(PIM\)](#).

[Azure Defender](#).

[Web Application Firewall](#).

[Monitor](#).

[Advisor.](#)

[Regions.](#)

[Azure Storage Encryption.](#)

[Key Vault.](#)

[Tagging.](#)

This section provides the definition of baseline controls and list of templates that cover the baseline and governance guardrails that can be implemented in new accounts.

Azure Security Centre

Use Azure Security Centre to ensure workloads are secure and to strengthen the security posture of the Azure estate. With continuous assessment, newly delivered resources are assessed and scored based on recommendations against Azure Security Benchmark.

Azure Identity Management (PIM)

Enabling PIM helps to mitigate the risk of excessive, unnecessary or misused access rights by allowing administrators to discover, restrict and monitor access to Azure Active Directory resources. Essentially, it means that any user with access to the MoJ data is only allowed access to certain files or services, assigned by the global and privileged role administrators.

Recommendations to improve overall Azure security posture by monitoring at a minimum include:

- Block or secure risky user accounts.
- Require users to register for [Multi-Factor Authentication \(MFA\)](#).
- Enable the use of Just-in-Time access, so that administrators can create privileged access for a specific time frame.

Refer also:

- [Azure AD Privileged Identity Management](#).
- [Activate my Azure AD roles in PIM](#).

Azure Defender

By enabling Azure Defender and integrating with Azure Security Center, you get an additional layer of security with which you can protect workloads hosted in Azure. Defender provides protection from most advanced threats, such as brute force, remote desktop protocol (RDP) or SQL injection attacks.

Refer also:

- [Enable Azure Defender](#).
- [Enable Defender for Key Vault](#).
- [Enable Defender for SQL](#).

Web Application Firewall

Azure Web Application Firewall (WAF) on Azure Application Gateway is a cloud-native service that provides centralised protection to web applications from common cyber attacks. Azure WAF protects against crawlers and scanners, SQL and command injection, cross-site scripting, HTTP protocol violations, anomalies, and other common web attacks. A WAF can support configurable request size limits and custom rules, exclusion lists, and geo-filtration of traffic.

Refer also:

- [Azure WAF deployment](#).

Monitor

Azure Monitor is the centralised console where you can create alerts around various resources in your subscription and also manage them. Alerting in Azure Monitor includes creating and managing alert rules, and creating and managing action groups.

Refer also:

- [Create, view, and manage activity log alerts by using Azure Monitor.](#)

Advisor

Azure Advisor takes the guesswork out of optimising your Azure deployments. Specifically, providing highly-personalised recommendations and best practices which are both actionable and proactive. Azure Advisor helps you find ways to reduce costs related to Azure service subscriptions, improve the performance, security, and availability of resources that are in use.

Refer also:

- [Azure Advisor.](#)

Regions

The MoJ does not use non-EU Azure regions, for strategic compliance and performance reasons. For more information on regions, refer to [Conditional Access : Block by region](#).

Azure Storage Encryption

Azure Storage data encryption and decryption is transparently done using 256-bit AES. Azure Storage encryption is for all storage accounts, including both Resource Manager and classic storage accounts. This cannot be disabled, as the data is secured by default. All Azure Storage resources, such as blobs, disks, files, queues, and tables, including all object metadata, are also encrypted at rest.

Refer also:

- [Azure Storage encryption for data at rest.](#)

Key Vault

Azure Key Vault protects encryption keys and secrets stored in Azure. The material might be certificates, connection strings, and passwords. However, steps should be taken to maximise the security of your vaults and the data stored within them while storing sensitive data, including enabling Defender for Key Vault to safeguard your data.

Refer also:

- [Best practices to use Key Vault.](#)
- [Defender for Key Vault.](#)

Tagging

Assigning tags to Azure resources is essential in creating a well-organised and transparent classification, and achieving significant cloud cost optimisation. When implemented, this practice can provide a consistent basis for applying policies across the organisation.

Refer also:

- [Assign policy definitions for tag compliance.](#)

Contact details

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

Baseline for Amazon Web Services accounts

The Ministry of Justice (MoJ) has a 'lowest common denominator' for security-related promises, capabilities and configurations of MoJ Amazon Web Services (AWS) accounts.

The baseline is not a holistic 'do' and 'do not' list, but a minimum line in the sand for what 'at least' **SHALL** be done.

The base principle

All MoJ AWS accounts **must** use a series of agreed configurations to enable and support good tenancy within AWS and a suitable cyber security posture.

Anti-solutionising

This baseline discusses outcomes not *how* the baseline will be achieved/implemented.

The 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 Cyber Security team should be added as a security contact for all Information security incidents generated by AWS. The contact details for an AWS Account can be updated using the reference [here](#).

- Full Name: Operational Security Team
- Title: Mx
- Email Address: OperationalSecurityTeam@justice.gov.uk

Baseline

IAM Access Analyzer

Use [IAM Access Analyzer](#) to audit and identify resources that are shared with an external entity.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
IAM Access Analyzer is enabled on all accounts, in all used regions, all of the time.	Alerts fire for new findings.	Findings are archived (if intended) or resolved (if unintended) within 7 days.

GuardDuty

Use AWS' commodity IDS solution to detect/protect from malicious or unauthorised behavior.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
GuardDuty is enabled on all accounts, in all regions, all of the time.	Alerts fire when GuardDuty is not enabled in a MoJ AWS account. Alerts fire for at least HIGH and higher (or some version of) GuardDuty matches.	GuardDuty is automatically re-enabled.

CloudTrail

Use AWS' native activity audit platform (with adequate non-repudiation) to capture what AWS user (IAM etc) activity and changes are made within our AWS accounts

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
CloudTrail is enabled within all accounts, all of the time. CloudTrail logs are carbon copied to an AWS account controlled by Cyber Security.	Alerts fire when CloudTrail is not enabled in an MoJ AWS account.	CloudTrail is automatically re-enabled.

Config

Use AWS' native AWS configuration activity audit platform to capture what changes are being made to AWS configurations.

Encryption

Use native AWS configuration options to make reasonable efforts to protect data.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All AWS objects supporting encryption must have it enabled.	S3 buckets without suitable SSE-* encryption enabled are alerted to resource creator and account owner.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and 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.

Compute (for example, EC2 or ECS) instances should not be directly accessible from public networks unless through specific intentional design and should be behind CloudFront and/or applicable load balancing (preferring AWS LB technology). It must be truly exceptional for common service ports (for example, TCP80 or TCP443) to be served directly from compute resources.	Compute instances are programmatically reviewed to ensure they are not internet-accessible unless explicitly designed and documented to be so. If there is a mismatch the resource creator and AWS account owner notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. After 7 days, the relevant security groups are forcefully and automatically changed to remove 'world' access.
---	--	--

Security Hub

[Security Hub](#) enabled where possible.

Over time we will be able to use this more, but in the immediate future this will enable us to do CIS-based scans.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
Security Hub is enabled on all accounts, in all regions, all of the time.	Alerts fire when Security Hub is not enabled in a MoJ AWS account.	Security Hub is automatically re-enabled.

Implementation

Various [AWS account baseline templates](#) have been developed and published for use.

How to use this document

Each policy statement outlines a security requirement and where applicable, a reference is provided to further material. A unique identify is associated with each statement for easy reference. The format of each statement is as follows:

POL.FR.PXXX

Policy statement text.

The policies outlined in this document form the baseline standard. Where exceptions are required, this is captured on a case by case basis in Tier 4, where approval is required from both the business group SIRO and MoJ ITSO.

Forensics Readiness Policy

Introduction

The aims of this policy are to:

- Maximise the effectiveness of any digital incident investigation which may be required, normally as a result of a security incident;
- Help protect MoJ information assets through the application of best practice in IT Forensics;
- Minimise the cost and impact on the business of a forensic investigation;
- Manage the risks associated with forensic investigations, and, the risks inherent in the incident(s) that occurred, necessitating the investigation.

IT forensics is the application of techniques to detect and react to types of security incidents that require the collection, storage, analysis and preparation of digital evidence that may be required in legal or disciplinary proceedings.

The use of IT forensics as a course of action is linked to decisions made during an IT security incident. As such, this policy is linked to, and should be read in conjunction with, the [IT Security - IT Incident Management Policy](#).

This policy outlines the requirements to collect, preserve and analyse data in a systematic, standardised and legally compliant fashion to ensure the admissibility of evidence in a legal case, dispute or disciplinary hearing relating to an incident.

POL.FR.P.001

Each IT system or IT domain **must have** (or be explicitly covered by) a Forensic Readiness Plan which implements this policy.

Note: In general, where an IT system (or IT domain) has an IT Security Incident Management Plan, there should be a corresponding Forensic Readiness Plan.

A template Forensic Readiness Plan is [available](#) with further guidance provided in [IT Security - Forensics Readiness Guide](#).

Scope

This Policy applies to all users of MoJ IT systems; this includes contractors and third parties who have access to MoJ information assets or IT systems.

Planning principles

Detection

Skilled perpetrators may attempt to cover up their unauthorised or malicious actions. An investigator, using IT forensic tools, can detect these actions and take suitable actions to limit the risk exposure from an incident.

POL.FR.P.002

The MoJ **must have** the capacity to conduct a forensic investigation (as required), whether it involves the use of internal or external capability and resource.

Deterrence

IT Security awareness training ensures staff are aware of the [IT Security Acceptable Use Policy](#) and that the MoJ has the right and ability to monitor all IT systems for conformance to this policy. This may deter staff from inappropriate,

illegal or malicious actions. Additionally, external awareness of MoJ system monitoring capability may also deter unauthorised users from attempting to access or attack MoJ facilities and IT systems.

POL.FR.P.003

All users of an IT system **must be** made aware that their access is monitored and that as part of an investigation into a security incident, IT forensic techniques may be used to capture evidence.

Consistency

An IT Security Incident Management Plan documents a set of pre-planned procedures and methods for instigating and conducting an investigation. Part of this plan is concerned with the criteria for forensic monitoring and investigation. This is to ensure that all forensic investigations are conducted in a consistent, repeatable fashion.

POL.FR.P.004

Each IT security incident management plan **must outline** the criteria for initiating a forensic investigation.

POL.FR.P.005

A Forensic Readiness Plan **must contain** a defined set of procedures and methods for conducting a forensic investigation.

Business continuity

It is essential that the MoJ is able to resume or continue business operations after an IT security incident event. It is therefore important that a forensic investigation is conducted in a manner that supports the restoration of IT services. For example, a forensic investigation may involve the removal of hardware assets; steps should be taken to inform the relevant IT supplier to ensure replacement assets are installed.

POL.FR.P.006

The procedures and methods outlined in a Forensic Readiness Plan **must consider** the business continuity arrangements required to support the restoration of IT services.

Evidential ownership and responsibility

Digital evidence can be exceptionally fragile and must be handled extremely carefully to remain admissible. It is essential that at all stages of an incident's investigation, there is a clearly documented chain of custody for all evidential items, including a clear record of who was responsible for carrying out actions upon these evidential items.

POL.FR.P.007

For all stages of a forensic investigation, there **must be** a clearly documented chain of custody for all evidential items captured.

POL.FR.P.008

Each forensic investigation **must have** a named forensic investigation owner who is responsible for conducting the investigation and the integrity of any evidence captured.

POL.FR.P.009

Any investigative action taken on an evidential item (e.g. an analysis of a hard drive) **must be** captured and recorded. This record **must include** details of the action taken and the person responsible for undertaking that action. Responsibility for the integrity of evidence resides with the Forensic Investigation Owner and MoJ Operational Security Team (OST). In addition, responsibility for any evidence captured, by or passed to an external forensic provider at the start of an investigation, resides with the MoJ and the Forensic Investigation Owner.

POL.FR.P.010

Admissibility of evidence in a court of law varies with the method of capture. Advice **must be** sought from the

- A reactive investigation - Where a suspicious incident has been identified (or reported). These investigations require the appropriateness, legality, effects of business disruption, cost and availability of key resources to be considered before the investigation is started.

Forensic investigations are only to be carried out under the following circumstances:

- Risk Management of a system has revealed a particularly sensitive/vulnerable area which needs to be proactively monitored. Any discovered security incidents would then be escalated through the IT security incident management process.
- A business function has issued a request to gather forensic investigation evidence directly to the MoJ Defensive Security Operations Team (DSOT). Results of such an investigation will be handed back to the requesting business function. Any request will be processed through the appropriate incident management process and escalated to the ITSO, DSO or SIRO as required.
- An investigation is requested as part of the IT security incident management process. Results of the investigation will be reported back through the incident management process, but other subsidiary processes may also be invoked. Further details available in the [IT Security – Forensic Readiness Guide](#).
- A forensic investigation is requested by the DSO as part of a leak investigation. Results of an investigation under these circumstances will be reported back to the DSO, who will report to the Permanent Secretary. Further information is available from the [Corporate Security and Business Continuity Branch](#).

POL.FRP.017

Each Forensic Readiness Plan **must include**, in the criteria for conducting an investigation:

- An assessment of the risk management benefits;
- The investigation has been authorised by the ITSO, DSO or business group SIRO;
- The consideration of a forensic investigation is in line with the corresponding IT security incident management plan process.

POL.FRP.018

Where a forensic investigation has been requested in response to a leak investigation. This investigation **must be** requested by the DSO where the DSO is responsible for that investigation.

Note: This may fall outside of the IT security incident management process.

Capability to collect evidence

MoJ forensic principles

The following forensic principles are based on [ACPO guidelines](#):

- Preservation of Evidence - The forensic investigation process needs to preserve the integrity of the original evidence by providing sufficient security, legal advice and procedural measures to ensure that evidential requirements are met. Any processes applied to copies of evidence must be repeatable and achieve the same results.
- Aptitude for the task - Any task in a forensic investigation will need to be conducted by a person who is suitably trained and competent to carry out that task.
- Documented Methodology – All investigations need to follow a documented methodology, as outlined in a Forensic Readiness Plan, with an audit trail of all processes applied to collect evidence. A chain of evidence will need to be created and preserved to demonstrate where evidence has been stored and under whose responsibility from capture until presentation. This allows other investigators to repeat those processes to obtain the same results as required.
- Conformance - Investigations need to be conducted in a manner which is inline with MoJ policies (this includes all MoJ corporate policies, not just IT Security policies).

Responsibility for escalation normally resides with the Information Asset Owner (IAO) who may also be in charge of the incident investigation. Where responsibility for an investigation has been escalated to the DSO or SIRO, further escalation responsibility will also reside with them.

The impact upon any relevant ongoing operational activity has to be considered before external reporting and escalation is invoked. The forensic investigation process needs to allow for the chain of evidence to be passed to outside agencies (e.g. a law enforcement agency).

POL.FRP.023

Each Forensic Readiness Plan **must include** details of any external (non MoJ) entities which form part of the reporting structure and escalation path.

References

ID	Title	Version / Issue
1	IT Security - Technical Controls Policy	V1-00
2	IT Security - Acceptable Use Policy	V1-00
3	IT Security - Information Classification and Handling Policy	V1-00
4	IT Security - IT Incident Management Policy	V1-00
5	HMG Security Policy Framework	Version 8, April 2012
6	MoJ Accreditation Framework	V0-01
7	BS 10008:2008 - Evidential weight and legal admissibility of electronic information	November, 2008
8	Corporate Security and Business Continuity Branch	n/a
9	Good Practice Guide for Computer-Based Electronic Evidence – Published by ACPO.	Version 4, 2008
10	IT Security - Forensics Readiness Guide	V0-01
11	IT Security – IT Asset Disposal Guide	V0-01

Incident Management Plan and Process Guide

Legacy information

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

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

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

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

About this document

This document is the Ministry of Justice (MoJ) IT Security – Incident Management Plan and Process Guide. It is designed to help protect the information assets of the MoJ through the formal documentation of procedures surrounding the management of IT security incidents.

How to use this document

This document provides guidance on implementing the MoJ [IT Security – Incident Management Policy](#). It should be used to guide the development of a MoJ business group level IT Security Incident Management Plan whose scope covers all IT systems used to support that business group.

For the purposes of this document, the following term will be used:

- **IT Security Incident Management** will be referred to as **ITSIM**.

Overview

Introduction

The ability of the MoJ to react quickly to IT security incidents will ensure that losses are minimised and the business will be able to resume or continue operations as quickly as possible.

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful incident management and all MoJ systems will rely upon the development and implementation of an IT Security Incident Management (ITSIM) plan as described in this guide.

The [HMG Security Policy Framework](#) mandatory requirements 4 states that:

Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business.

The policy on IT Security Incident Management is covered in [IT Security Policy - IT Incident Management Policy](#) while this document set outs the MoJ guidance for creating an ITSIM plan. This guide must be read in conjunction with [CESG GPG No. 24 – Security Incident Management](#).

Aim of this guide

The aim of this guide is to ensure all MoJ business groups develop, implement and maintain an ITSIM plan.

This guide is split up into four sections:

All MoJ staff (including contractors and agency staff)	All MoJ staff (including contractors and agency staff) play a role in identifying and reporting IT security incidents. All staff must report any concerns especially when the IT security policy is not being adhered to, or where suspicious activity may indicate a security incident is being (or highly likely to be) committed. Moreover, if there is a strong likelihood that a security incident may occur, this must also be reported.
MoJ Senior Managers	MoJ Senior Managers hold a position of responsibility and can form part of the decision making process during the management of a live IT security incident. MoJ Senior Managers must ensure that all IT security incidents or personal data breaches are taken seriously and sufficiently investigated, and where necessary, corrective, disciplinary and or legal proceedings are actively pursued.
Senior Information Risk Owner (SIRO)	MoJ Business Group SIROs are responsible for implementing and managing information risk in their respective business groups and, reviewing the application of policy and guidance regularly thereafter to ensure it remains appropriate to their business objectives and risk environment. In the context of ITSIM, the SIRO forms part of the escalation path where incidents which are categorised as having a high impact or involve personal data (refer here) are reported to the SIRO as a matter of course. They are also responsible for ensuring that their business group has an ITSIM plan.
Information Asset Owner (IAO)	IAOs are senior individuals involved in running business units. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. MoJ IAOs must understand and address risks to the information, and ensure that information is fully used within the relevant laws, and provide written input and assurance to the SIRO annually on the security and use of their asset. They will be informed of any security incidents which compromise any information assets under their ownership.
MoJ IT Security Officer (ITSO)	The MoJ ITSO is responsible for IT security across the MoJ and is the first point of escalation. The ITSO performs two functions with regards to ITSIM; Firstly, a source of advice and guidance on MoJ IT security policy and secondly, forms part of the decision making process during the investigation and resolution phase of an IT security incident.

IT Security

Preparation and
Planning



Prepa

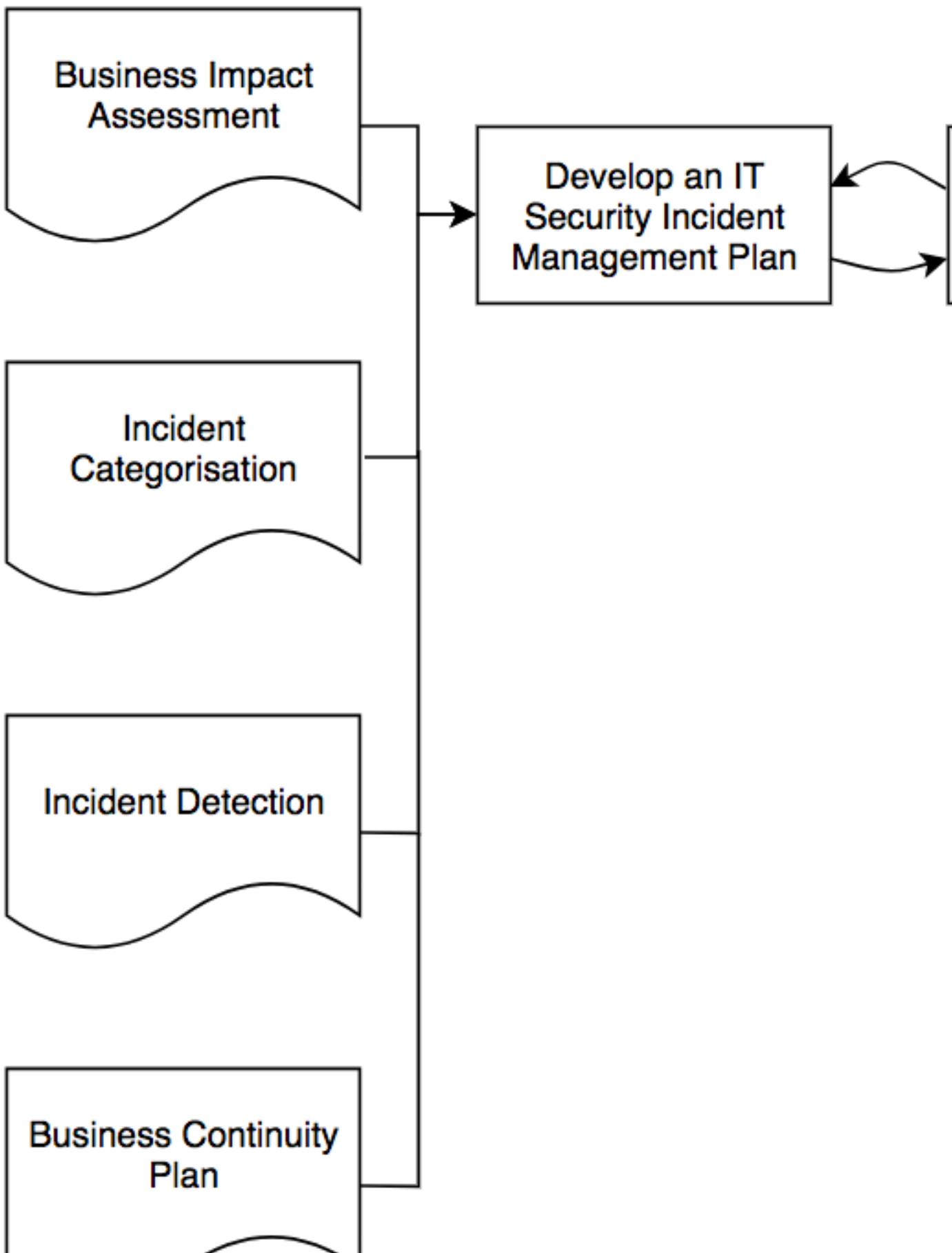


Figure 2 – Preparation and planning

Developing an ITSIM plan

A good ITSIM plan requires a good understanding of the business, the information assets and IT systems involved, the impacts to the business were an incident to occur and the overall business continuity requirement.

Input	Role
Business Impact Assessment (BIA)	The BIA provides the core rational on how the business views the impact to their information assets and services from a loss of Confidentiality, Integrity or Availability. Where this is useful in the development of an ITSIM plan is that the BIA provides a steer on what types of incidents result in the highest impact to the business and how tolerant the business is to a loss of service provision.
Incident Categorisation	The IT Security – IT Incident Management Policy and this guide (refer here) provides a generic incident categorisation schema. This generic scheme should be used to develop final schema contained within the ITSIM plan. The aim at this phase of developing the ITSIM plan is to: <ul style="list-style-type: none"> • Explore the different types of incidents which could or have occurred. For example a good starting point is a review of relevant system RMADS to identify possible incident types. • Compare the incident types identified with the information assets and services which could be impacted and broadly align each type to impact category (high impact, medium impact or low impact, refer here for further details on the response level for each category).
Incident Detection	It is unlikely that an ITSIM plan will be developed in isolation and the IT systems which fall under the scope of the plan will have security controls and procedures which directly or in-directly support incident detections, for example an anti-virus client or intrusion detection system (IDS).
Business Continuity Plan (BCP)	Though the ITSIM plan concentrates on the management of IT security related incidents, ITSIM sits within an overall BCP. It is vital that the relevant BCP is factored in the creation of the ITSIM plan and it is advised that both teams work together as both plans are closely linked and need to be aligned.

Table 2 – Inputs to the IT Security Incident Management plan

Test and refine

Before implementing an ITSIM plan, it is generally good practice to test out as many aspects of the plan as possible in-order to refine its processes and operations. This is likely to involve a number of iterations and include the testing of any automated detection tools.

Implementing the plan

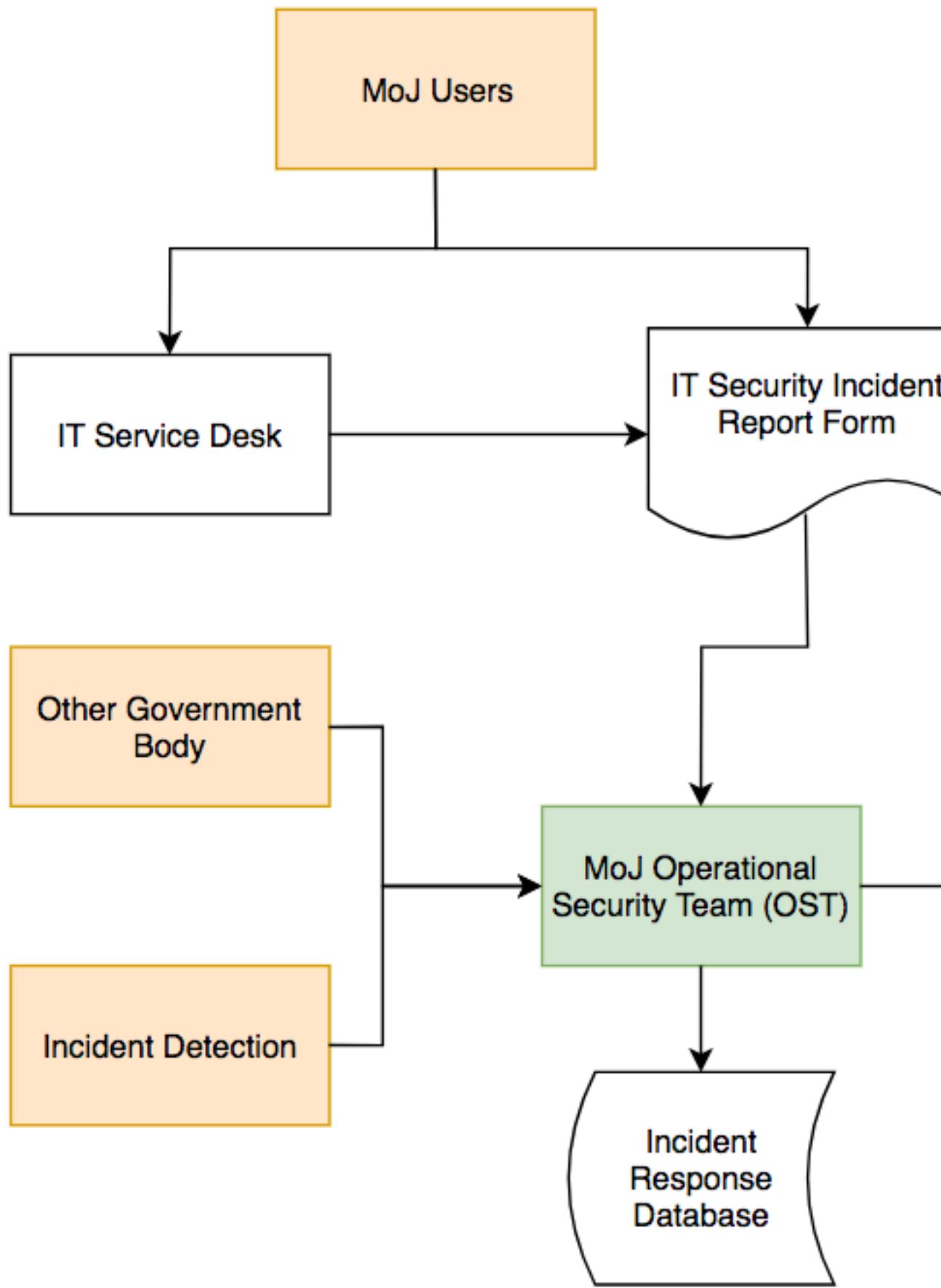
Table 3 following provides a list of the main outputs required to implement an ITSIM plan.

Outputs	Role
IT Security Incident Management Plan	Though obvious, a final released version of the ITSIM plan is the primary output. It must be approved by the business group SIRO and ITSO. It must be released to all Users and stakeholders identified in the plan.
Security Controls	The development of an ITSIM plan may lead to the requirement for further security controls to be introduced. For example the ability to collate anti-virus detections centrally.
Monitoring Services	For an ITSIM plan to be effective, a consummate incident detection and monitoring service must be in place and active. For most MoJ ITSIM plans, this will involve the MoJ Operations Security Team (OST) acting as the centralised monitoring and management service where incident reports are fed to them, for example, from automated security controls (such as virus detection alerts from an anti-virus client) or manually by a User reporting the loss of a MoJ laptop to the IT Service Desk.
Training and Awareness	All Users must be provided with awareness training which covers the ITSIM plan and their role in incident detection, reporting and management. For those who perform specific roles within the plan such as a Senior Manager, they should undertake additional training to ensure they are prepared to fill their aspects of the plan.

Table 3 – Outputs from implementing the IT Security Incident Management plan

IT Security Incident Management

Incident management requires a variety of decisions to be made, drawing on expertise from a variety of backgrounds, including technical, administrative and managerial depending on the nature of the incident. The incident management process supports the decision making process and subsequent courses of action taken to resolve an incident.



Key

Figure 3 – IT Security Incident Management flow

The ITSIM process essentially consists of three elements:

- Incident reporting – This is shown as a source of incident information on Figure 3. Generally there are three sources, MoJ Users reporting incidents using an IT Security Incident Report Form, alerts from other government bodies such as GovCERT and incident detection controls such as an IT supplier reporting the release of an emergency critical patch or an automated alert from an Intrusion Detection System (IDS).
- Incident management – This is a function perform by the MoJ Operational Security Team (OST), it involves conducting an initial assessment of the incident, incident categorisation and management of the incident escalating where appropriate. Note that the process continually examines the categorisation of an incident as it is being investigated. An incident may move up or down the impact scale as more information is discovered.
- Incident resolution – Where an incident has been through the management process and resolved.

What constitutes an 'incident'?

For the purpose of this document, an incident is defined as any event or action that results in an actual and/or potential compromise of personal and sensitive personal data, MoJ information assets and/or the MoJ IT infrastructure.

Types of Incidents

The list of incident types provided in this section is not exhaustive and mirrors the list provided in the [IT Security – IT Incident Management Policy](#). Each ITSIM plan must contain a definition of what constitutes an incident which results in the plan being activated, this definition can solely refer to the list provided in the policy, however there may be incident types which are specific to a particular business area which need to capture. The list of incident types includes (but is not limited to):

- Breaches of the [IT Security - Acceptable Use Policy](#);
- Detection of malicious code (e.g. a piece of malware);
- Network attacks or Denial of Service (DOS) attacks;
- Scanning and probing of a network (where significant network resources are consumed);
- Inappropriate use of MoJ IT assets as defined in the [IT Security – Acceptable Use Policy](#);
- The discovery of a new network vulnerability or release of a patch or software update which is considered critical or an emergency;
- The results of a penetration test on a live operational IT system that reveals critical vulnerabilities;
- Unauthorised access to an IT system;
- Accidental loss of personal or other information assets;
- Deliberate release of personal or other information assets;
- Compromise of integrity;
- Any alerts or suspicious activity report generated by an IT system that proves to be a real security alert.

Business related IT security incidents include (but is not limited to):

- Harm to an individual as a result of the compromise of MoJ information assets;
- A significant loss of availability at the MoJ site at which processing and storage of MoJ information takes place;
- The theft or loss of MoJ information;
- The likelihood that a MoJ department or function will be brought into disrepute or might suffer reputational damage;
- A significant impact on the ability of the MoJ to perform its duties;
- A long recovery period either in terms of practical matters or reputation;
- An event that is of interest to local/national press;
- Evidence of espionage activities;
- Accidental loss of personal or sensitive personal information;
- Deliberate release of personal or sensitive personal information.

Incident Detection and Recording

Security incidents may come to light from a variety of sources, including through active system monitoring and the MoJ staff reporting suspicious activity or security incidents. All IT security incidents must be reported to the OST, who will conduct an initial assessment and manage the incident through to resolution.

Note – All incidents involving personal data must also be reported to the MoJ Data Access and Compliance Unit (DACU).

The [MoJ IT Security Policy](#) defines the requirements for capturing and recording security events and monitoring them for suspected malicious activity or breaches of security.

The MoJ Operational Security Team (OST) is responsible for maintaining a centralised database and view of all IT security incidents across all MoJ IT systems. This database contains information on:

- Security incident reports;
- An up to date status of all reported security incidents;
- An up to date status of any actions taken with respect to a particular security incident.

This database and the effective reporting of security incidents which populate it are important in managing the MoJ's overall risk exposure. This is both in the short term, to identify any major deficiencies with an IT system which requires immediate remedial action and in the long term, to capture lessons learnt to improve Information Assurance maturity and the ITSIM plan itself.

Categorisation of Incidents

Incidents need to be categorised to assess their impact and the required level of escalation and reporting. This is mainly done to manage resources and make investigations cost effective. The initial assessment for all IT security incidents will be made by the OST with support from the ITSO and the relevant system Accreditor as required. The assessment will be in terms of the potential impact of the incident with each incident categorised in terms of Low, Medium or High impact.

The three following sub-sections provide a description for each category. It is expected that the business group ITSIM plan will contain a tailored version of this description and confirm the escalation route which will be followed.

Low Impact Incident

These would typically be minor such as low level breaches in security through an accident or carelessness, or a minor loss of service from a service provider e.g. temporary loss of power or connectivity.

A low impact personal data incident would typically include an incident where no loss has occurred but a weakness in a system may potentially have led to a loss, and with a small amount of remedial action the weakness in a process can easily be addressed.

Incident categorised as low will be typically managed by the MoJ OST who will engage with the relevant parties within the business and IT supplier community to resolve the incident. Any escalation (refer to Figure 4) will be predominantly to the level of the MoJ ITSO and relevant system Accreditor.

Medium Impact Incident

Examples of medium impact incidents include (but not limited to):

- Deliberate disregard for the [IT Security Policy](#) leading to minor breach in security or the potential of data loss;
- Inappropriate use of MoJ IT assets as defined in [IT Security - Acceptable Use Policy](#);
- Loss of data or IT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Theft of data or IT asset (where the data or asset does not contain any personal data and is not protectively marked);
- Damage to any MoJ IT asset;
- Connecting unauthorised equipment to an IT system (where there is no intent or suspicion of malicious activity);
- Prolonged or permanent failure of an IT system;
- Prolonged set of unsuccessful attempts to scan an IT network or instigate a denial of service attack;

- Any alert or reported suspicious activity on an IT system (note this may need to be escalated to High Impact upon investigation);
- Compromise of IT system integrity;
- The recognition of a new critical security vulnerability in an IT system (this may be the result of a penetration test);
- The release of a critical patch by an application or IT equipment vendor;
- Localised report of malicious code (e.g. the detection of a virus or malware of a desktop terminal);
- Serious case of equipment theft;
- The theft or loss of HMG cryptographic material.

Medium impact incidents require escalation to the MoJ ITSO who will determine whether the IAO and relevant system Accreditor also need to be informed. In the case of personal or sensitive personal data, the MoJ Data Access and Compliance Unit (DACU) also need to be informed. If deemed appropriate, a forensic investigation will be requested by the MoJ ITSO in line with the [Forensic Readiness Policy](#).

High Impact Incident

High level IT incidents require immediate escalation to the Senior Information Risk Owner (SIRO) and relevant Information Asset Owner/s.

Examples of incidents requiring this level include (but are not limited to):

- Evidence of espionage activities;
- An incident that is of interest to local/national press;
- A significant impact on the ability of the MoJ to perform its duties;
- The likelihood that MoJ function will be brought into disrepute or might suffer reputational damage;
- Any successful network intrusion to MoJ IT facilities;
- Widespread malicious code attacks;
- The release of an emergency patch released by a manufacturer used by the MoJ (as described in the Security Patch Management Policy);
- The loss of a MoJ, or suppliers, site at which processing and storage of MoJ information takes place for more than one working day;
- The theft or loss of MoJ protectively marked information which could include CONFIDENTIAL and higher, or a significant quantity of RESTRICTED material.

It is highly likely that an incident of this magnitude would require the MoJ ITSO to instigate a forensic investigation and start collecting evidence.

Further Escalation Requirements

The decision to escalate an incident beyond the MoJ business group SIRO remains with that SIRO where advice will be provided by the MoJ ITSO.

Incidents that require this type of escalation include (but are not limited to):

- Issues of national security;
- If the incident has received local or national press coverage;
- If the incident has caused or might cause harm to MoJ Staff;
- There is a high likelihood the MoJ will be brought into disrepute or might suffer reputational damage;
- If the incident involves (or is suspected to involve) Foreign Intelligence Services (FIS) or Organised Crime;
- Where there is a HMG requirement to report to central incident management bodies, the OST will co-ordinate reporting for example, the reporting of network security incidents to GovCERT;
- Where there is a significant, actual or possible loss of personal data, the Information Commissioner's Office and the Cabinet Office Central Sponsor for Information Assurance need to be informed via the SIRO and ITSO

Investigation and Diagnosis Capability:

The MoJ Operational Security Team (OST) is responsible for organising the investigation of all IT security incidents. Where there is a need for evidence to be gathered for possible disciplinary or legal proceedings, a forensic

investigation may be required. Each impact category should have its own associated management process which consists of the following activities:

- Investigating an incident as directed by the ITSO or SIRO;
- Proactively monitoring any IT system involved in the incident to capture suspicious behaviour;
- Where authorised by the MoJ SIRO, providing evidence to disciplinary hearings, industrial tribunals, civil courts and criminal courts when required;
- Maintaining files on investigations inappropriate security storage and in accordance to privacy laws;
- Conducting investigations into information security incidents at any of the MoJ locations;
- Recovering and securely store evidence when required;

The distinction between the management processes is the priority and level of resources assigned. For example, a low impact incident involving a MoJ user attempting to access a blocked website will be processed at a slower rate than a high impact incident where a confirm and active network intrusion has been detected.

It is important to ensure that a diagnosis of the events surrounding each incident is recorded and shared with the relevant stakeholders.

Where there has been a personal data incident or where possible disciplinary or legal proceedings may be required, the following actions must be taken:

- The relevant MoJ Senior Manager must collect detailed information on the incident;
- Refer any possible disciplinary action to HR;
- Maintain records on the investigation appropriately preserving evidence.

Resolution, Recovery and Closure of Incidents

Based on the investigation and diagnosis of an incident the recovery and closure of the incident can involve many stakeholders. It is important that all stages of resolution are recovered and recorded before an incident is formally closed.

When an IT system has had a significant compromise, that system may require a review of its accreditation status in light of the circumstances of the incident. This is a decision normally made by the relevant system Accreditor.

Lessons learnt and continuous improvement

Adequate information relating to security incidents, such as types, volumes and costs must be recorded in order to identify recurring or high impact incidents or malfunctions. This may indicate the need for additional or enhanced security controls to limit the frequency, damage and cost of future occurrences or may indicate the need for a change in policy, the design of an IT system or implementation of SyOPs.

IT security incident statistics must be presented in conjunction with an assessment of top security risks and details of any significant compliance gaps on a monthly basis to the ITSO to assist risk management. Each ITSIM plan must be reviewed on a yearly basis and re-approved by the SIRO and ITSO.

Appendix A – IT Security Incident Management Plan - Template

IT Security Incident Management Plan	
Overview	
MoJ Business Group	[Enter the name of the MoJ Business Group.]
System Description and Scope	[This section must describe the scope of the ITSIM plan. Diagrams may prove useful where there is a complex interaction between systems and business processes covered by this plan.]

Escalation Path		[This section must describe the escalation path for an IT security incident (refer to Figure 4).]
Incident Categorisation		
Low Impact Incident	Description	[Provide a description of what a Low impact incident constitutes; refer here for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consultant the OST and ITSO when completing this section.]
Medium Impact Incident	Description	[Provide a description of what a Medium impact incident constitutes; refer here for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consultant the OST and ITSO when completing this section.]
High Impact Incident	Description	[Provide a description of what a High impact incident constitutes; refer here for further details.]
	Priority and escalation	[Provide details of the priority and standard SLAs which will be applied to incidents at this impact level. Consultant the OST and ITSO when completing this section.]
Plan Approval		
Business Group SIRO		[Enter the name of the Business Group SIRO] [DATE OF APPROVAL]
IT Security Officer		[Enter the name of the ITSO] [DATE OF APPROVAL]

Completing this plan can form part of the Accreditation process and must be included and maintained as part of the relevant RMADS.

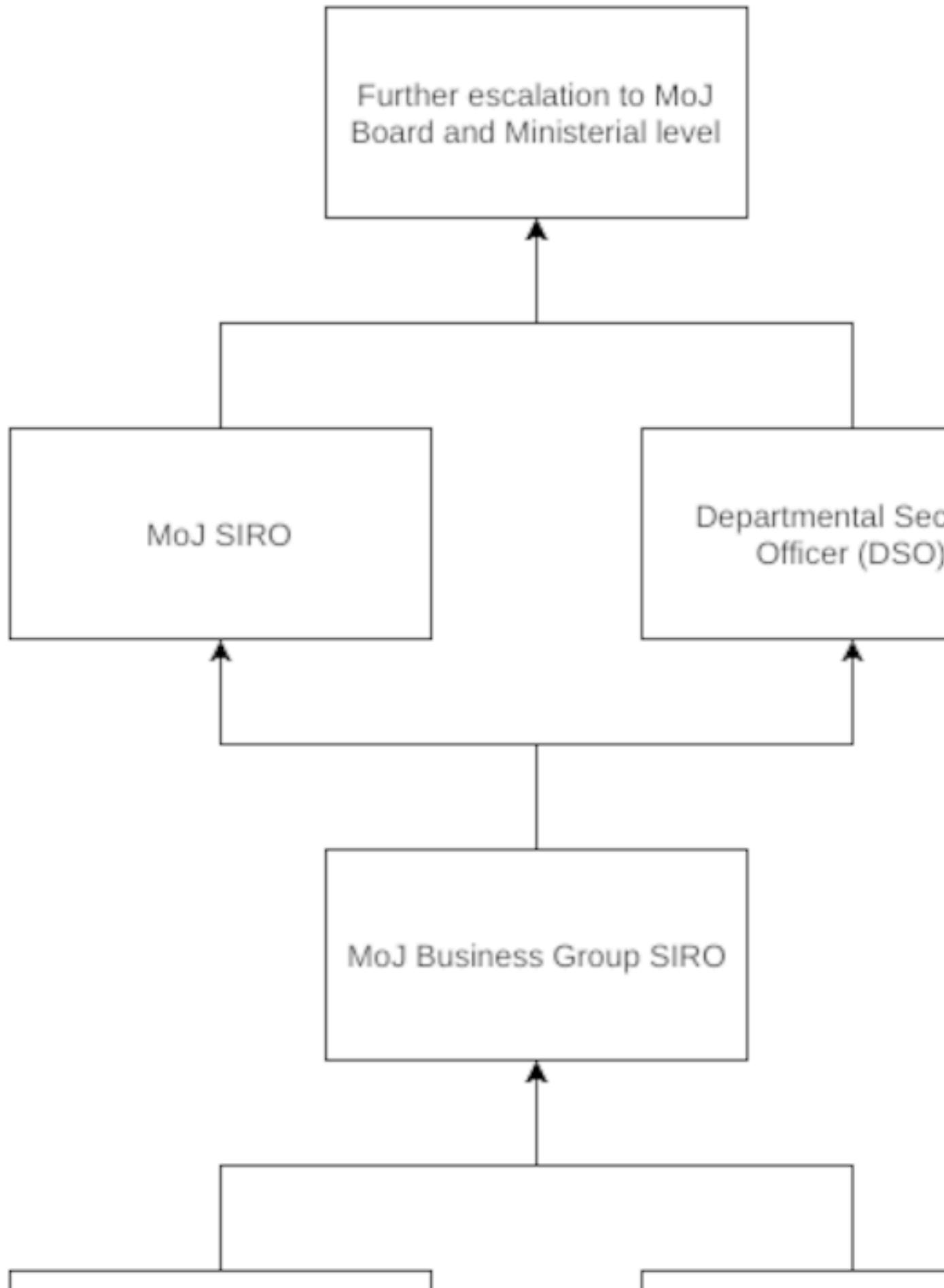
Appendix B – Escalation path

Figure 4 – ITSIM Escalation path

IT Incident Management Policy

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful information security management and all Ministry of Justice (MoJ) systems rely on Incident Management Plans for safe and secure operations.

The aim of this policy is to ensure best practice is followed by all IT systems when dealing with security incidents, in particular, those pertaining to data loss, in a timely and efficient manner.

POL.IMP.001:

Each MoJ Business Group **must have** an IT Security Incident Management Plan which aligns to this policy. This plan must be common to all IT systems within a particular business group.

A template plan and guidance on the construction of an IT Security Incident Management Plan is provided in [IT Security – Incident Management Plan and Process guide](#).

Related information

[Technical Controls Policy](#) on page 36

Legacy information

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

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

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

Scope

This policy is concerned with IT related security incidents outlining the roles and responsibilities, escalation path and criteria for escalation.

Relationship with wider MoJ functions

An IT system is one element of a number of supporting elements which sustain MoJ business functions and delivery of services. The MoJ [Corporate Security and Business Continuity Branch](#) is responsible for overall MoJ Incident Management policy and plan. This policy is designed to sit within the overall MoJ incident management structure.

Incident Management Process

An incident management process is a prepared course of actions that will be instigated upon the detection or report of a security incident. Incident management requires a variety of decisions to be made, drawing on the experience of a number of roles, depending on the nature of the incident.

The incident management process supports the making of informed decisions following a consistent approach designed to reduce the consequences of any incident.

Definition of an Incident

For the purposes of this policy, an incident is defined as any event or action which results in an actual and/or potential compromise of a MoJ IT asset or MoJ Information Asset (including personal data).

Such events will result in the MoJ, individuals or IT systems and/or the information held on them being exposed, or potentially exposed, to illegitimate access. As a result, incidents have the potential to compromise MoJ business delivery, the Data Protection Act, as well as the confidentiality, integrity and availability of IT systems and the information held on them. This may, in turn cause harm, distress or other damage to individuals or organisations, and result in operational disruption or reputation damage to the MoJ.

Types of Incidents

IT Security related incidents include (but are not limited to):

- Breaches of the [Acceptable Use Policy](#);
- Detection of malicious code (e.g. viruses and malware);
- Network attacks or Denial of Service (DOS) attacks;
- Scanning and probing of a network (where significant network resources are consumed);
- Inappropriate use of MoJ IT assets as defined in the [Acceptable Use Policy](#);
- The discovery of a new network vulnerability or release of a patch or software update which is considered critical or an emergency;
- The results of a penetration test on a live operational IT system that reveals critical vulnerabilities;
- Unauthorised access to an IT system;
- Accidental loss of personal or other information assets;
- Deliberate release of personal or other information assets;
- Compromise of integrity; or
- Any alerts or suspicious activity report generated by an IT system that proves to be a real security alert.

Incident Detection and Recording

Security Incidents may come to light from a variety of sources, including through protective monitoring solutions, reports filled by MoJ staff or breaches of the MoJ IT Security Policy detected by an IT system.

The [MoJ IT Security Policy](#) defines the requirements for capturing and recording security events and monitoring them for suspected malicious activity or breaches of security.

This section of the policy is concerned with taking those security events and ensuring that if an event relates to an actual IT Security incident, this incident is appropriately recorded.

POL.IMP.002:

- Theft of data or IT asset (where the data or asset is does not contain any personal data and is not protectively marked);
- Damage to any MoJ IT asset;
- Connecting unauthorised equipment to an IT system (where there is no intent or suspicion of malicious activity);
- Prolonged or permanent failure of an IT system;
- Prolonged set of unsuccessfully attempts to scan an IT network or instigate a denial of service attack;
- Any alert or reported suspicious activity on an IT system (note this may need to be escalated to High Impact upon investigation);
- Compromise of integrity;
- The recognition of a new critical security vulnerability in an IT system (this may be the result of a penetration test);
- The release of a critical patch by an application or IT equipment vendor;
- Localised report of malicious code (e.g. the detection of a virus or malware of a desktop terminal);
- Serious case of equipment theft; or
- The theft or loss of HMG cryptographic material.

High Impact Incident

IT Security incidents at this level require immediate escalation to the relevant MoJ Business Group Senior Information Risk Owner (SIRO) in addition to the OST and where applicable, the MoJ Data Access and Compliance Unit: [Data.access@justice.gov.uk](mailto>Data.access@justice.gov.uk).

Incident at this impact may warrant forensic investigation.

Examples of incidents at the level include (but are not limited to):

- Evident of malicious activity, intent or espionage;
- An incident which comes to the attention of local or national media;
- Any successful network intrusion;
- Widespread malicious code attacks (e.g. a worm spreading across an IT system);
- The release of an emergency patch by an application or IT equipment vendor;
- The theft or loss of personal or protectively marked data from an IT system.

Further escalation requirements

The decisions to escalate an incident irrespective of its impact up through the chain from ITSO, MoJ SIRO, DSO, and higher (possible to Ministerial level) may include the following factors:

- Issues of national security;
- If the incident has received local/national press coverage;
- If the incident has caused harm to a member of staff or public;
- There is high likelihood that the MoJ has suffered reputational damage or been brought into disrepute;
- Where there is a HMG requirement to report to another Department or central management function (e.g. GovCERT for network incidents or CINRAS for incidents involving HMG cryptographic material);
- Where there is a significant actual or possible loss of personal information where the Information Commissioner's Office and Cabinet Office need to be informed.

Incident Management Stakeholders

This policy outlines the general incident management stakeholders and escalation path principles. Each MoJ business group implementation of this policy (which is the creation and acceptance of an IT Security Incident Management Plan) will need to consider how this is practically implemented, all the individual stakeholders involved (including others such as IT suppliers), and escalation path.

All MoJ staff (including contractors and agency staff)

It is important that all MoJ staff are aware of what a security incident is and how to correctly report it.

POL.IMP.006:

Where the IT Service Desk receives a report of a security incident, this **must be** reported and escalated to the OST immediately.

Escalation Path

As a rule, all IT Security incidents are reported to OST. As depicted in Figure 2, OST then progress the incident according to its categorisation (refer [here](#)). Depending on the category and nature of the incident, this can involve escalating the incident to other stakeholders.

POL.IMP.015:

Each IT Security Incident Management Plan **must include** a pre-arranged escalation path where each stakeholder is named and aware of their role in the Incident Management Plan.

A generic escalation path is provided [here](#). This generic path is intended to provide a starting point where further guidance on tailoring and customisation is provided in the [IT Security – Incident Management Plan and Process Guide](#).

Investigation and Diagnosis capability

The OST is responsible for the investigation of all IT Security incidents. Where evidence gathering is required for possible disciplinary or legal proceedings, a forensic investigation may be required, further details are provided in the [Forensic Readiness Policy](#).

In the course of investigation, the OST may:

- Investigate incidents at the direction of the ITSO;
- Proactively monitor suspected targets or IT systems to capture potential suspicious behaviour for analysis;
- Undertake or oversee an investigation requested by an outside agency (e.g. CESG) where authorised by the ITSO;
- Recover and securely store evidence where required;
- Require a SIRO or Senior Manager to collect more information on an IT Security incident.

POL.ITSEC.016:

The OST **must maintain** files on any investigation undertaken.

POL.ITSEC.017:

Any diagnosis of an IT Security incident and the events surrounding it **must be** shared and reported to relevant stakeholders.

Resolution, Recovery and Incident Closure

Based on the investigation of an IT Security incident, remedial action may be required to ensure appropriate incident resolution and the recovery of any IT services or information assets compromised as a result of the incident.

POL.ITSEC.018:

An IT system which has a significant compromise (Medium or High impact, refer [here](#)) **must be** reported to the system Accreditor and a review of that system's risk assessment and accreditation must be conducted.

POL.ITSEC.019:

All IT Security incidents for an IT system **must be** collated and provided to the system Accreditor during the re-accreditation process.

Recovering from an IT Security incident

There may be occasions when it is appropriate to restore a system that has been attacked or compromised from its backup since it might be the only way to ensure system integrity.

Checks must be made to ensure the IT system being restored pre-dates the incident and does not contain any exploitable weaknesses, for example, ensure the IT system is fully patched before it is brought back into service.

POL.ITSEC.020:

The IT Security Incident Management Plan for an IT System or overarching IT Domain **must include** details on how that system or IT domain IT services are restored (or recovered) following an IT Security incident.

Note – The detail of how an IT system recovers from an incident event should be captured in that systems disaster recovery plan. Refer to the [IT Security – Disaster Recovery Policy](#) for further information.

Preventing re-occurrences

Once the cause of an IT Security incident has been identified, steps must be taken to reduce the risk of its reoccurrence, for example eradicate any computer viruses, block firewall ports, and install any missing system patches, as necessary.

Learning points

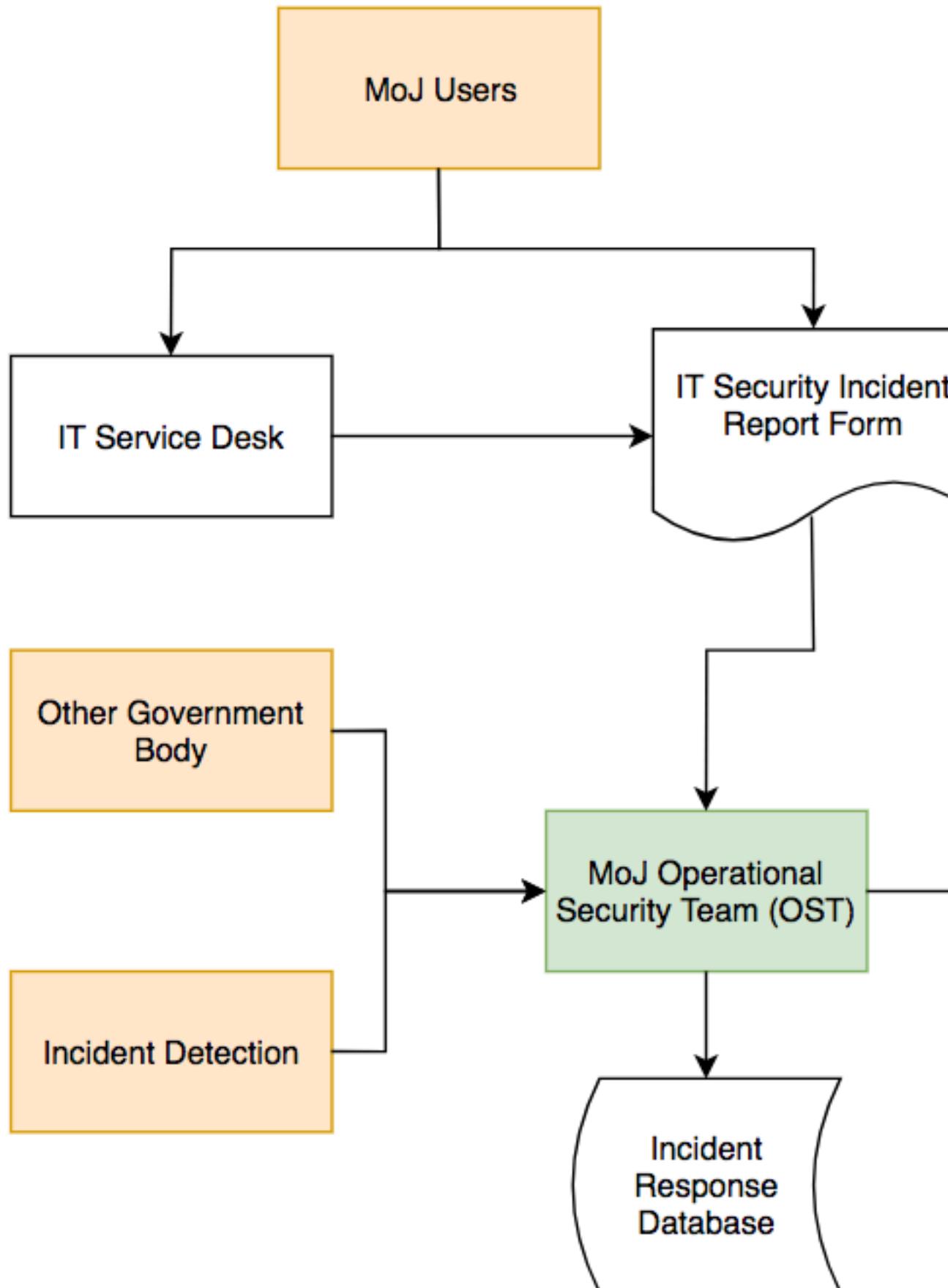
When an IT Security incident has been resolved and closed, a management report needs to be prepared outlining the incident, the outcome of the investigation, actions taken, and recommendations about how to improve the business systems to reduce the likelihood of a reoccurrence.

Copies of the report must be sent to the ITSO who has a responsibility for forwarding the report onto any HMG central reporting functions, for example CESG, GovCertUK or CINRAS, as appropriate.

POL.ITSEC.021:

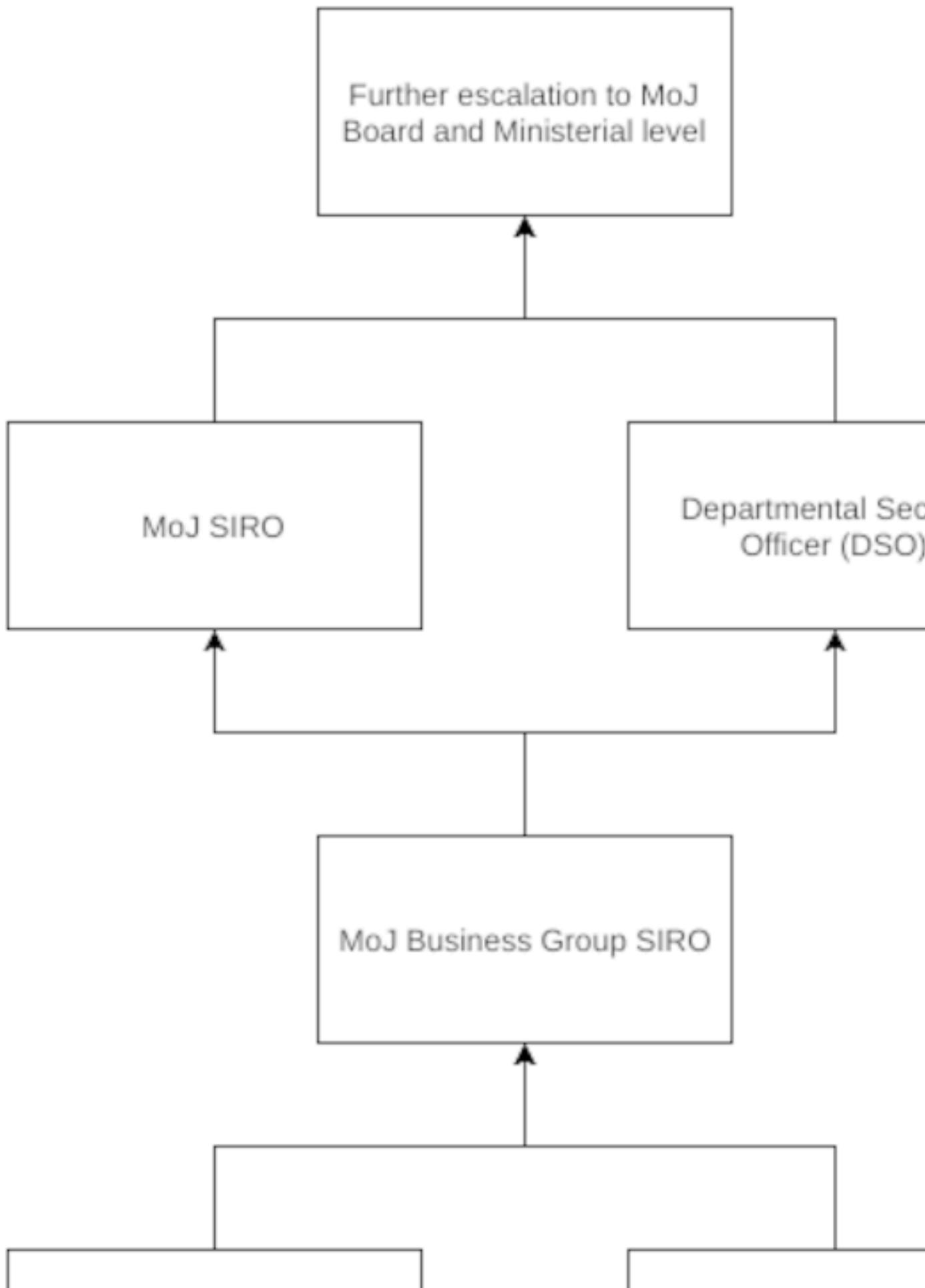
For each Medium and High impact (refer [here](#)) IT Security incident, a management report **must be** prepared covering:

- A description of the incident;
- The outcome of the incident investigation;
- Actions raised (or taken) with associated action owners;
- Any recommendations made.

IT Security Incident Recording and Categorisation**Key**

IT Security Incident Escalation Path

The following is a generic IT Security incident escalation path which provides a starting point for the creation of a tailored version in an IT Security Incident Management Plan. Further information is provided in the [IT Security – Incident Management Plan and Process Guide](#).



Lost devices or other IT security incidents

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

Related information

[Laptops](#) on page 212

What to do if your device is lost, stolen, or compromised

If MoJ data or information is lost or compromised, you should always [report it as a data incident](#).

Note: You can help reduce problems by making sure that devices used for MoJ tasks are always shut down before leaving Government premises. Locking a laptop, or 'putting it to sleep' is not completely secure. A lost or stolen laptop can be accessed more easily if it is only locked or sleeping. A shut down makes sure that all security measures are in place, such as full disk encryption.

If you think your device is lost, stolen, 'hacked', or in some way compromised, you must:

1. Contact your IT Service Desk. The analyst will ask the relevant questions and note responses on the ticket.

Technology Service Desk - including DOM1/Quantum, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

Note: The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses, and the Digital & Technology Digital Service Desk Slack channel (#digitalservicedesk), are no longer being monitored.

2. Tell your line manager as soon as possible.
3. For a lost or stolen device, contact the Police and make sure you get the incident reference number.

Summary

Find out more about how to [report a security incident](#).

Contact details

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

Information security aspects of business continuity management

Information security continuity

IT Disaster Recovery Plan and Process Guide

Legacy information

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

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

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.

Feedback



Step 1:
Requirements
Gathering

Requirements and Planning

Incident Management

Step A:
Declaring a
Disaster

Step B:
Invoking the
Plan

Gathering requirements for ITDR

The ITDR process is based on understanding the Recovery Time and Point Objectives; these form the basic requirements for ITDR. This section outlines the process to identify a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and the information gathering activities required in order to create an ITDR plan.

ITDR requirements

Recovery Time Objective (RTO)

The RTO is the maximum business-tolerable time that an IT system can be unavailable. This time must be considered from the business' point of view where the RTO covers the entire period from initial failover to successful restoration of the business operations. Simply taking this time to recover a single server is not sufficient.

Recovery Point Objective (RPO)

The RPO is the amount of data loss which can be tolerated by the business after a system failover. As such, a business can either re-type or re-generate this amount of information without a significant impact on their business process.

Information gathering

The following table provides details on the base set of information sources required to support the development of an ITDR plan.

Table 13: Information sources

Information source	Description
ITDR asset register	The group of IT systems that are subject to the ITDR planning process must be captured in an ITDR asset register. The RTO and RPO for each individual IT system must be less than or equal to the overall business group RTO and RPO.
Business Impact Assessment (BIA)	For each IT system identified on the ITDR asset register, a Business Impact Assessment (BIA) is carried out. A BIA considers what impact would occur to the business in the event that the IT systems were unavailable or data were lost. This BIA may be created as part of the Risk Management and Accreditation Document Set (RMADS).

Writing an ITDR plan

This section provides guidance on writing an ITDR plan with a template provided [here](#). Each sub-section is an element of the ITDR plan.

IT System Description

For the purposes of the ITDR plan, an IT system is the collection of applications and supporting infrastructure which provides IT services to a MoJ business group. In turn, this business group supports a number of business processes – it is these processes which must be restored, not just the IT system.

In order make clear the role of the IT system with relevance to the BCP, this section must clearly list the IT system's constituent components, as well as details of the business processes it supports. This in turn defines the scope of the ITDR plan.

Site List

This section of the ITDR plan must contain details of all the physical sites relevant to the recovery process. It must also include details of any secondary business sites, in case the primary site is affected by a disaster and IT system services need to be made available at a secondary site.

Dependencies

A list of dependencies (internal and external) must be included in the ITDR plan. Restoration of a business process may be more complex than restoration of a single IT system, and the bottlenecks or miscommunications which can

occur here are often the critical points of failure in the process. The impact of the dependency must be captured, in terms of risk, time and cost.

This information can be used in a disaster event to provide an accurate estimate time for recovery.

Internal Dependencies

Internal dependencies are those which may materialise as part of the recovery actions of the ITDR plan itself, for example:

- When a step in the plan must be completed before a subsequent step can be taken, such as restoring access to a database before conducting login testing.
- If the data centre is in a remote part of the country, and so it may take time for staff to reach the location.

External Dependencies

External dependencies are those which may affect the success of an ITDR plan and lie beyond the area of control of the ITDR Team Lead (refer to the [IT Security – IT Disaster Recovery Policy](#) for a role description).

For example:

- Where a previous service, such as power, communication or sanitation facilities, must be restored before this system can be restored;
- Where the recovery of this system must be completed before the Incident Management team can notify staff to return to work at some location.

Invocation

Definition of a 'Disaster'

The ITDR plan must include a clear statement on what set of incidents constitute a disaster. Certain components of the IT system may be replaceable without invocation of the entire ITDR plan, whereas an apparently 'small' incident may have a wider reach which does require the plan to be invoked. This section must clarify the situations in which the ITDR plan will be invoked; it may be useful to reference incidents which may have occurred in the past.

Note: This definition must be consistent with corresponding ITSIM plan.

Invocation

The ITDR plan does not need to be invoked in its entirety. A disaster event may not require the invocation of all the procedures in the plan, and so the level of response must be assessed and clearly communicated and agreed between the business and IT leads before implementation.

This section must list those with authority to invoke the ITDR plan.

Staff Notification

Provisions must be made to inform the correct staff of the need to begin recovery procedures; this should usually be captured in the corresponding ITSIM plan.

IT supplier staff may require a different form of notification, and therefore this procedure should be clearly noted in the ITDR plan if they are not contained within the corresponding ITSIM plan.

Key Contacts

This section of the ITDR plan should detail the individuals who currently hold the roles listed in the previous section. As mentioned previously, this information may be better kept in an annex.

Recovery procedures

This section of the ITDR plan must list the functions of the IT system and the business processes it supports, and relate them to a specific set of recovery actions. Functions should be categorised (into primary and secondary functions) allowing for critical business processes to be restored ahead of others.

A generic set of ITDR incident management steps is [provided](#) which should be used as the basis to structure the more granular recovery actions (refer [here](#)).

Primary functions

Primary functions are those which **must be** restored in the event of a disaster. The primary functions are the business-centric and mandated processes which must be restored for the business to successfully complete its work.

Secondary functions

Secondary functions are those which **should be** restored in the event of a disaster. Priority should be aimed at the primary functions; secondary functions should be restored only after all the primary functions are restored.

Recovery actions

This section of the ITDR plan should list any actions which are to be used in the recovery effort and where possible should be cross-referenced with the relevant primary and secondary functions. It is recommended that the ITDR plan contains a high level set of actions (e.g. recover file server) with technical details contained in a referenced work instruction or pre-existing operational procedures document.

Review

The ITDR plan is a constantly evolving document, and therefore must be subject to change control and review. This should be in line with the review schedule for the corresponding ITSIM plan.

This section of the ITDR plan must define those responsible for the reviews, as well as the conditions under which the review must be undertaken.

ITDR testing

This section outlines the steps required to develop an effective approach to ITDR testing.

Types of test

There are five main approaches to testing an ITDR plan:

- Paper-based testing
- Walkthrough testing
- Component testing
- Parallel testing
- Cutover testing

Each approach is summarised in the following table.

Table 14: ITDR plan test types

Test type	Description
Paper-based Test	A paper-based test collects together all of the available documentation for the system; most importantly, the ITDR plan for the system. An analyst with experience of conducting ITDR will then ascertain from examining the documented processes and interviews with staff, whether all of the necessary provisions exist to meet the recovery requirements for that IT system.
Walkthrough Test	A walkthrough test is a non-technical, real-time test involving a role-play exercise where all relevant stakeholders walk through an ITDR scenario. All resources need to be available and set aside to test a specific scenario; these include business staff, IT staff and accommodation. Where possible it is recommended that the individuals who would be used in a true disaster scenario are used to conduct the test, with the various parties responding as per their role.
Component Testing	Component testing starts to test individual components of processes and technology that will be identified in an ITDR plan. Component testing provides an opportunity to gain confidence that the individual components of the IT system can be restored successfully. This type of testing often takes place before progressing to an end-to-end form of testing.

Test type	Description
Parallel Testing	Parallel testing involves the use of hardware which has been sourced or set aside for the purposes of testing. Essentially, this form of test is operating a full restoration of an IT system in a non-live setting. In this type of testing, the ITDR process is run in parallel alongside the live system, ensuring that the business process can continue to function, while identifying hardware-based, physical and practical limitations of the plan.
Cutover Testing	Cutover testing focuses upon putting a disaster recovery system into a live setting. Therefore this involves the complete dependence on the backup system rather than the primary. It is strongly recommended that all previous types of tests are considered and undertaken and reviewed or not taken with formally agreed reasoning to assure confidence before adopting this approach. Care must also be taken to ensure that the live service is not affected during the setup and execution of this test. As with any live service testing, it will be imperative that appropriate service or maintenance windows are identified and agreed with the business, in order to minimise risk to business operations.

Planning a test

Objectives

The main objectives of testing an ITDR plan are to determine whether:

- IT services can be recovered after an incident;
- IT continuity provisions can minimise the impact to the business and their operations, in response to an incident;
- The ITDR procedures for a return to 'business as usual' operations are validated;
- Additional factors, such as communication, and incident and alert management are sufficiently robust; and
- To allow staff to become familiar with the ITDR plan.

The test results must show:

- Gaps in the level of service compared to the ITDR requirements (refer [here](#)).
- Actions to address these gaps must be identified and assigned to responsible staff.
- A consolidated report for management should be compiled, in order to illustrate the results of the tests, along with actions taken to address any issues that arose.
- The process of examining the results against the requirements should identify 'defects' in the Plan documentation and process. These defects must be identified and fed back into the planning documents.

Success criteria

A test can only be declared a success if the following conditions are met:

- The business processes which are covered by the ITDR plan are proven to be recovered to working use at the end of the test period.
- The entire IT system, including data, can be accessed by users within the period of time specified by the agreed RTO limit (refer [here](#)).
- Where applicable, users can access the IT system from a necessary site after the failover has been tested.
- The amount of data loss can be specified exactly, and is within the RPO limit.

Note: This is not an exhaustive list, this should be discussed and criteria should be reviewed and agreed with the business group Senior Information Risk Owner (SIRO) in advance.

Review and update

Subsequent review of the test must be undertaken to ensure that all test results are reflected in the ITDR plan. It is recommended that this be undertaken as soon as possible after the test is completed. It is important that any unexpected results arising from the test, which have not been rectified or are still outstanding issues, are documented in the ITDR plan including any actions to rectify any defects or issues.

ITDR Incident management

The following table provides a generic set of incident management steps which should be followed when the ITDR plan is invoked. As the ITDR plan sits under an ITSIM plan, it is important to ensure that the steps encapsulated in the ITDR plan aligns to the ITSIM plan.

Table 15: Information management steps

Step	Name	Description
A	Declaring a Disaster	An incident is declared a 'disaster' which requires the ITDR plan to be invoked.
B	Invoking the ITDR plan	The IT Disaster Recovery Team Lead identifies the critical resources required to manage the disaster, and puts forward a communications strategy to ensure that all personnel can co-ordinate actions appropriately.
C	Executing the DR Plan Procedures	The scope and extent of the disaster is assessed and the ITDR plan is executed following the set of recovery procedures set out in the plan.
D	Status Updates	During the recovery process, regular communication points are recommended as part of the ITDR plan to keep the business updated.
E	Incident Resolution	Once the IT system is considered restored to a sufficient level, a final communication to indicate completion should be made to the business. At this point, it is the responsibility of Service Management to declare the system restored.
F	Review Results	After the incident has been closed off the 'lessons learned' from the recovery procedure must be reviewed and addressed. In some cases defects in the procedure or plan may come to light. The aim and objectives of the invocation and requirements must be analysed in light of the information gathered from conducting the execution of the plan. These results will establish if the aims and objectives were met and whether the response to the outage was sufficient.

Training and awareness

Introduction

All staff should be subject to training in order to raise an awareness of the ITDR plan and their individual roles within it.

Staff training requirements

The following table defines several categories of staff and outlines the recommended training and awareness requirements.

Table 16: Staff training requirements

Category	Requirements
General staff awareness	<ul style="list-style-type: none"> • To know that an ITDR plan exists. • To know how they will be impacted by the range of scenarios covered by the ITDR plan. • To know what to do in the event of an incident or invocation.

ITDR Representatives	As for general staff, plus: <ul style="list-style-type: none"> • To know the responsibilities of a ITDR representative. • To know how their departments will be impacted by the range of scenarios covered by the ITDR plan. • To ensure their business requirements are communicated and accommodated within the ITDR plan.
Incident management team	As for general staff, plus: <ul style="list-style-type: none"> • To understand the requirements of the ITSIM and ITDR plans. • To know their roles in the ITSIM and ITDR plans.
ITDR recovery staff	As for general staff, plus: <ul style="list-style-type: none"> • To understand the IT recovery priorities, plans and processes. • To know their roles in the recovery process.

IT Disaster Recovery Plan - Template

IT Disaster Recovery Plan	
Overview	
MoJ Business Group	[Enter the name of the MoJ Business Group.]
System Description and Scope	[This section must describe the scope of the ITDR plan. Diagrams may prove useful where there is a complex interaction between systems and business processes covered by this plan. Refer here for further details]
Site List	[Refer here]
Definition of a 'Disaster'	[Refer here]
Authorised to invoke the plan	[Refer here]
Staff notification	[Include details of how staff and IT suppliers are notified that ITDR plan has been invoked, refer here]
Roles and responsibilities	[For each role outlined in the IT Security – IT Disaster Recovery Policy , a named individual must be entered here.]
Dependencies	
Internal Dependencies	[Include each dependency, recommend the following format: <ul style="list-style-type: none"> • Dependency ID; • Description; • Impact (time, resource, effort). Refer here]
External Dependencies	[Include each dependency, recommend the following format: <ul style="list-style-type: none"> • Dependency ID; • Description; • Impact (time, resource, effort). Refer here]

Recovery Procedures	
Primary Functions	[Include each primary function, recommend the following format: <ul style="list-style-type: none">• Function ID;• Function;• Description. Refer here]
Secondary Functions	[Include each primary function, recommend the following format: <ul style="list-style-type: none">• Function ID;• Function;• Description. Refer here]
Step [X]	[For each step outlined in ITDR Incident Management , list the corresponding recovery procedures in this section; refer to the Recovery procedures for further details.]
Recovery Actions and Review	
Recovery Actions	[Refer here]
Review	[Refer here]
Plan Approval	
Business Group SIRO	[Enter the name of the Business Group SIRO] [DATE OF APPROVAL]
IT Security Officer	[Enter the name of the IT Security Officer (ITSO)] [DATE OF APPROVAL]

Completing this plan can form part of the Accreditation process and must be included and maintained as part of the relevant RMADS.

Contact details

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

IT Disaster Recovery Policy

Legacy information

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

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

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

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

Introduction

IT disaster recovery is a crucial element of the Ministry of Justice (MoJ) overall business continuity plans.

Definition of a disaster event

An IT 'disaster' event is defined (for the purposes of this policy) as any incident which results in an actual or potential loss of availability or integrity of an IT system or a business process supported by an IT system. That event would result in a system being unable to operate in an acceptable manner to the business.

POL.ITDR.001:

Each IT system or IT domain **must have** (or be explicitly covered by) an IT Disaster Recovery Plan which implements this policy.

A template Disaster Recovery Plan is available in the [IT Security - IT Disaster Recovery Plan and Process Guide](#).

Note: In general, where an IT system (or IT domain) has an IT Security Incident Management Plan, there should be a corresponding IT Disaster Recovery Plan.

Roles and responsibilities

An effective IT Disaster Recovery Plan requires the clear allocation of responsibility. Defining the roles and responsibilities of those involved with IT disaster recovery is also an important part of the overall recovery effort.

Note - The roles outlined in this policy are aligned with and support the [IT Security – Incident Management Policy](#).

POL.ITDR.002:

Each IT Disaster Recovery Plan **must outline** how the roles and responsibilities in this policy are fulfilled. This includes recording named individuals (and associated contact details) for each role.

POL.ITDR.003:

All staff **must be** made aware of the relevant IT Disaster Recovery Plan/s and where applicable, their role within it.

Note: Further guidance on training and awareness can be found in [IT Security – Disaster Recovery Plan and Process Guide](#).

Senior Information Risk Owner (SIRO)

A SIRO acts as an advocate for managing risk for Business Continuity and IT Disaster recovery.

Departmental Security Officer (DSO)

The Departmental Security Officer is responsible to the Permanent Secretary for:

- Assurance of the management and completion of the Department's Business Continuity Plans.
- The MoJ's assessment of the National Threat Assessment in the context of business continuity planning.
- Setting direction for the MoJ's approach to Business Continuity and agreeing the maintenance and creation of plans across the business.
- The DSO has a MoJ wide view of Business Continuity Plans and is able to report on the maturity of these plans. This IT Disaster Recovery Policy supports these Business Continuity Plans.

Information Asset Owner (IAO)

The IAO's role in IT Disaster Recovery Planning is to understand the risks to the availability of their information assets in the event of a disaster and to ensure that they understand and can execute the relevant IT Disaster Recovery Plan.

Business Continuity Team Leader (BCTL)

The Business Continuity Team Leader is appointed to monitor and manage the MoJ's Business Continuity Plans.

IT Disaster Recovery Team Leader (ITDRTL)

The ITDRTL is responsible for the MoJ's IT Disaster Recovery Plans. This role works with the Business Continuity Team Leader to ensure that MoJ IT systems support MoJ's critical business processes.

The IT Disaster Recovery team leader is responsible for:

- Identifying where the IT Disaster Recovery Plan will need to be updated in line with changes to the MoJ Business Continuity Plan;
- Administering IT disaster recovery testing in accordance with agreed schedules;
- Providing regular reports of the IT disaster recovery status of the MoJ;
- Coordinating regular reviews and updates of IT Disaster Recovery Plans.

IT Security Officer (ITSO)

This role is responsible for identifying and managing Corporate-level IT disaster recovery risks, and maintaining the Corporate IT disaster recovery risk register.

System Accreditor

The role of an Accreditor is to act as an impartial assessor of the risks to information systems. Their function is to assure that systems are sufficiently secure to be placed into operational service. They accredit systems on behalf of the SIRO. There is also a role for Head of Accreditation who lead the accreditation team, and may accept the risk on their team's behalf.

Planning

The planning and generation of an IT Disaster Recovery Plan as described in the IT Disaster Recovery Guide support decisions and subsequent courses of action that reduce the consequences of any disaster event.

It is suggested that a Business Impact Assessment (BIA) is undertaken in order to identify the disaster recovery requirements of all the assets or business processes supported by a particular IT system:

In particular the BIA should contain:

Recovery Time Objective (RTO) – The time in which the business requires IT services to be restored. I.e. The time between a disaster event occurring and full IT system services being restored.

Recovery Point Objective (RPO) – The point in time in which an IT system's data asset/s can be rolled back to where the business can tolerate that period of data loss. I.e. How much historic data in the live IT system can the business tolerate losing in a disaster event.

POL.ITDR.004:

The IT Disaster Recovery Plan for an IT system or IT domain **must be** based on a Business Impact Assessment (BIA), Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

POL.ITDR.005:

Any disaster recovery measure outlined in an IT Disaster Recovery Plan **must ensure** the IT system (or IT domain) can recover from a disaster event within the stated Recovery Time Objective (RTO) as recorded in a BIA.

POL.ITDR.006:

Any disaster recovery measure outlined in an IT Disaster Recovery Plan **must ensure** the IT system (or IT domain) can recover from a disaster event within the stated Recovery Point Objective (RPO) as recorded in a BIA.

Testing and readiness review

An IT system (or IT domain) IT Disaster Recovery Plan needs to be tested regularly to ensure the plan is remains fit for purpose and those involved in executing the plan remain familiar with the procedures outlined in it. This increases the MoJ's preparedness in the event of a disaster.

POL.ITDR.007:

Prior to the commencement of live operations, an IT system **must have** its IT Disaster Recovery Plan tested where the outcome is supplied to the system Accreditor to form part of the accreditation decision making process.

POL.ITDR.008:

All IT Disaster Recovery Plans (whether for an IT system or IT domain) **must be** tested annually or when a significant change occurs to that IT system. The testing schedule **must be** outlined in the IT Disaster Recovery Plan.

POL.ITDR.009:

After each test, a review of the IT Disaster Recovery Plan **must be** conducted and updated where appropriate based on the test finding, outcomes or defects identified.

Invocation and escalation

The invocation of an IT Disaster Recovery Plan is closely aligned to corresponding IT Incident Management Plan.

In general, an incident categorised as High impact (refer [here](#) for more details) may in turn constitute a disaster event. Each individual IT Disaster Recovery Plan needs to outline the particular circumstances in which the plan is invoked.

POL.ITDR.010:

Each IT Disaster Recovery Plan **must define** the situations and circumstances under which the Plan is to be invoked.

Reporting and alerting

In general, the reporting and alerting structure of an IT Disaster Recovery Plan should align with that of the corresponding IT Security Incident Management Plan. However, depending on the nature of the disaster event, other stakeholders may need to be informed both internally and externally to the MoJ. This is where the MoJ Business Continuity Plan interacts with any individual IT Disaster Recovery Plan for an IT system or IT domain.

POL.ITDR.011:

Each IT Disaster Recovery Plan **must define** a reporting and alerting structure which aligns with the relevant IT Security Incident Management Plan and Business Continuity Plan.

Responsibility for business continuity resides with [MoJ Corporate Security and Business Continuity Branch](#) where further details can be obtained.

Recovery and review

Recovering from a disaster event is generally about the speed of restoring services to normal; however it is important to ensure that security vulnerabilities are not introduced (or re-introduced) during the restoration process and that any lessons learnt are fed back to appropriate stakeholders.

POL.ITDR.012:

Each IT Disaster Recovery Plan **must contain** a pre-defined and tested process and/or set of procedures for restoring the IT systems and services which have been disrupted or disabled during a disaster event.

POL.ITDR.013:

After each disaster incident, the following **must be** reviewed and any recommendations considered:

- The IT Disaster Recovery Plan to consider lessons learnt and any improvements;
- The design of the IT system and controls implements to reduce the impact of a disaster event or aid the restoration process;
- Any changes to the relevant IT Security Incident Management Plan.

Note – The [IT Security – IT Incident Management Policy](#) contains the provision for an incident report to be compiled. Any recovery and review work should be done in conjunction with the production of the overall incident report.

Contact details

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

Compliance

Compliance with legal and contractual requirements

Data destruction

Data Destruction

'Data destruction' is the process of erasing or otherwise destroying data stored on virtual/electronic or physical mediums such as, but not limited to, printed copies, tapes and hard disks in order to completely render data irretrievable and inaccessible and otherwise void.

The base principle

For legislative, regulative, privacy and security purposes, it **must** be possible to decommission and delete (irreversibly 'erase' or 'destroy') data and confirm to a degree of relative confidence it has been completed.

Data should be erased from all related systems, such as disaster recovery, backup and archival, subject to reasonable data lifecycle caveats.

Destruction standards

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: <https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning>
- NCSC guidance on secure sanitisation of storage media: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): <https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation>
- Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): <https://www.pcisecuritystandards.org>
- DIN: <http://www.din-66399.com/index.php/en/securitylevels>

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific Ministry of Justice (MoJ) guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific MoJ guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

Data lifecycle caveats

Automated systems involved in data management and associated lifecycles may not be capable of immediate destroying data on demand.

Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

There is generally no need to attempt to manually delete such data prior to the automated retention lapse as long as it is ensured that if the data is restored prior to data destruction it is not processed.

It is important that the final expected data where all data lifecycles will have completed to be readily identifiable with high confidence.

Definitions

The current draft of the definitions that are required by the current draft short and long format data destruction clauses.

Definitions to be added into definition contract schedule

Data Destruction - Data destruction is the process of erasing or otherwise destroying data or information whether in physical form (such as printed paper) or stored on virtual/electronic or physical mediums such as, but not limited to, tapes and hard disks; the purpose is to render data completely irretrievable and inaccessible, and therefore void.

Supplier - ?

Authority - ?

Buyer - ?

Data Process/Processing - means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Long format clause

The current draft of the Ministry of Justice (MoJ) commodity long format data destruction clause.

Highlighted words indicate potential requirement for contextual change, requirement of definition and so on.

Clause

The Supplier shall return all Authority Data in a machine-readable non-proprietary format defined by the Authority within 30 (thirty) calendar days of the end of the contract.

The Supplier must also state, ensure and warrant the final calendar date by which any associated data management lifecycle system(s) will be complete, including the manual or automated data destruction at the end of such period. Such data management lifecycle(s) may include, but are not limited to, the Supplier's supply chain and/or Data Processors, backup system(s) and/or disaster recovery and business continuity system(s). The Authority retains all applicable rights to instruct the Supplier to destroy all Authority Data according to the terms of this [G-Cloud] contract.

The Supplier is required to ensure adequate and complete Data Destruction of Authority Data, including any relevant and associated non-proprietary Supplier Data or work product stemming from the Buyer Data that the Supplier has not been otherwise permitted to retain or use.

Data Destruction must follow applicable guidance from the UK National Cyber Security Centre (NCSC) and/or the Payment Card Industry Data Security Standard (PCI-DSS) and/or DIN 66399.

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific Authority guidance: the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific Authority guidance: paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimetres squared with a maximum strip width of 6 (six) millimetres.

Instruction and Confirmation Letter

The current draft of a templated Ministry of Justice (MoJ) data destruction letter, that may be issued by the MoJ to a supplier. The letter describes required actions and information, followed by a responsive declaration from the supplier.

Letter issued by MoJ

Background

For legislative, regulative, privacy and security purposes, it must be possible for Suppliers to decommission and delete (irreversibly "erase" or "destroy") data and warrant the same. Similarly, any storage media holding such data must be securely and comprehensively erased before reuse or disposal (such as at end-of-life).

An example of a data destruction obligation is where a Supplier (acting as a "Data Processor", as defined by Data Protection legislation) working on behalf of, or supplying services to, the MoJ (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 MoJ, 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 MoJ 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 MoJ 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.

- You know where data for the system is stored. Ask which countries and jurisdictions hold the data. Check that the storage complies with GDPR/DPA18 requirements.
- The procedures to follow in response to a data breach are clear. Developed them with the help of the live service and cyber security teams.
- There is 100% confidence that data is backed up and protected against loss or other threat scenarios. Test and challenge this confidence frequently. Always test within the timescales defined in the retention schedule.
- The IA register lists the system. For potentially sensitive or risky data sets, check that the risk register also lists the system.

Sharing Information

Many systems depend on data from more than one source. For example, data might come from cross-estate and cross-government levels. This makes accountability for the data vital: who owns it, and who is responsible for it.

Acceptable information sharing involves two distinct perspectives:

1. Sharing with other systems. There must be public transparency and understanding about using the information. Similarly for any dependencies on the information. To provide this detail, create data maps with the help of the system technical architects. Make sure that the maps include correct links between the data controller who originated the information and any other processors of the data.
2. Sharing with other organisations. There must always be an auditable record of the agreement between the organisations. This could be part of a contract, a data sharing agreement, or other general memorandum of understanding. Review the record at regular intervals so that it still meets the user or business needs, and continues to be relevant.

Subject Access Requests

At any time, a person about whom we hold personal data can request a copy of all the information we hold about them. This is not a new requirement, and was part of original data protection legislation.

However, the £10 fee charged before is now waived. This makes it likely that there will be more Subject Access Requests in the future. Design your product to make it as simple as possible to perform Subject Access Requests quickly and easily. Authorised individuals from across all data storage locations should be able to respond.

Law Enforcement Directive (L.E.D.)

Some systems hold information about criminals or criminal offences. This is sensitive data. An additional regulation applies to them: the Law Enforcement Directive.

Affected systems must record whenever an individual record is viewed or amended. Keep this log for audit purposes.

Project Lifecycle Data Security and Privacy Expectations

When developing a system, there are some measures you can take that will simplify and ensure timely GDPR compliance.

Pre-Discovery and Discovery

Assess the data security and privacy implications of the project requirements thoroughly. Do this as part of the broader work addressing the project's strategic imperatives.

In particular:

- From the start of the project, and throughout its duration, think about how data security and privacy might affect the functionality and delivery of the project.
- Consult with technical architects to help inform and enhance the ways of delivering the work, whilst continuing to ensure compliance.
- Discuss any problems or ramifications that arise with legal or business experts. Identify areas where the required data security and privacy compliance might cause issues for functionality.

Alpha

During this stage of the project lifecycle, internal and external (GDS) teams will perform service assessments. These will specifically check for aspects of GDPR compliance.

In particular:

- That the majority of compliance considerations have been addressed at this stage.
- That the development team can say how their work ensures compliance.
- That the technical architecture choices can be tested against data security and privacy requirements. As an example, blockchain technologies might not be acceptable as they can prevent automated removal of information when it is no longer required.

Beta (Private and Public)

These are assessments performed as the service transitions from Private to Public availability. The assessments are again performed by internal and GDS teams. Use live systems for the assessments.

In particular:

- All manually actionable data security and privacy requirements must be met.
- Manual testing is expected.
- Automatic deletion is not required yet, because the service is unlikely to have enough data at this stage. However, plans and mechanisms for automatic deletion should be in place.
- Data should be backed up exactly as expected for a live service.

Live

These are the final (Live) service assessments. They are again performed by internal and GDS teams.

In particular:

- Data sharing aspects might not yet be fully defined. Other consuming or supplying systems might not have established dependencies on the information shared.
- Some aspects of reporting might still need manual action. The newness of the system makes business MI requirements a work-in-progress.

Post-Live (Ongoing)

These are the tasks that enable the final aspects of security and privacy for your project.

In particular:

- The final automated tasks are ready. The project cannot close until these are done.
- Data security and privacy compliance checks move to an ongoing status. Reporting takes place as required to internal stakeholders or the ICO.
- Schedule and run regular data mapping exercises. These ensure full and current understanding of data flows to and from any organisations or systems that depend on the information.

Information security reviews

Standards Assurance Tables

The Ministry of Justice (MoJ) Cyber Security team have developed a 'Standards Assurance Table' (SAT) in the form of a Google Sheet template.

The SAT measures technology systems (and surrounding information governance) against the [UK Cabinet Office Minimum Cyber Security Standard \(MCSS\)](#) and [UK National Cyber Security Centre \(NCSC\) Cloud Security Principles \(CSPs\)](#).

For transparency and open-working purposes, a [redacted copy of the Standards Assurance Table](#) has been published. Please note, this is not the functional template used within the MoJ.

SAT Template

The SAT itself is written to be self-explanatory to a cyber security professional who is already aware of the MCSS/CSP and has a familiarity with information risk management concepts.

- Black labelled sheets describe the SAT and how it should be used
- Blue labelled sheets are the ones to complete
- Yellow labelled sheets are automatically calculated, providing reports based on the blue labelled sheet data
- Green labelled sheets offer help/guidance on SAT components

Key SAT concepts

The SATs have measures including "Objectives", "Evidence", "Confidence", an overall "Delta" (which is the most pertinent SAT output) and "Further Evidence Required", with supporting commentary.

The primary SAT purpose is to help assess a system against the MCSS/CSP. It is used to determine confidence whether or not the evidence demonstrates the system is compliant (or not).

Evidence is analysed to determine confidence that the evidence demonstrates the system meets (or does not meet) the standards. It also indicates the 'gap' (delta) between the system's posture according to said evidence and the standards.

Objectives

The MCSS/CSPs have been distilled into 39 objectives. The Assessor (normally a cyber security professional) completes the SAT by evaluating the target system against the objectives.

The [categories used within the MCSS](#) are discussed separately.

Objectives are templated. This means they can be added to but existing objectives must not be deleted or edit in-place.

Evidence

To avoid assessments that are ultimately anecdotal, the assessor will only rely upon written evidence.

Evidence can come in the form of transcribed conversations, diagrams, documentation or other auditable information about a system.

Evidence might not be directly related to the system itself but form a part, for example, where there is a wider document that is not system orientated but which describes who is relevant role holders currently are.

Evidence is described as being 'Held', 'Partial', 'Not Held' or 'N/A' (where the Objective is not applicable to the system being assessed).

Confidence

The assessor reviews the evidence and uses their professional opinion to indicate a Confidence Score.

The Confidence Score uses a scale from 0 (no confidence at all) to 14 (high level of confidence), or 'N/A' (where the Objective is not applicable to the system being assessed).

Delta

The Delta Rating is the resulting 'distance' between the assessed system posture against an Objective and the confidence of the same.

Mathematically, the final Delta Rating is N/A (where the Objective is not applicable to the system being assessed) or 0 to 14 (inc).

A wide delta (higher numerical value) indicates that the Objective is not met. A narrow delta (lower numerical value) indicates that the Objective is closer to being met.

The Delta Rating is automatically calculated as '14 minus Confidence Score'.

Further Evidence Required

The assessor indicates what further evidence *types* in their view are required based on the evidence they have thus far.

The [Further Evidence Required \(Help\) sheet](#) has a calculator which the assessor will use.

The data point is currently a unique number to assist with future automated analysis. The format and range of values for the data point is currently under active review and so subject to change without notice.

Understanding the Objectives, gathering evidence for the assessor

Teams/individuals responsible for the design, creation, implementation, support and maintenance of systems should have viable written evidence (regardless of format) that should be made available to various teams on request, for example, security or to internal audit.

Using the [categories used within the MCSS](#) as a basis, some indicative questions and documentation expectations are discussed in this guidance.

IDENTIFY

Possible documentation

- Team organisation charts
- Data Privacy Impact Assessments (DPIAs)
- Information risk management documentation (for example, RMADS)
- Information flow diagrams

Thought questions

- Who is responsible and/or accountable for the 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)

Changes to an existing IT baseline

Any major design change to an existing IT service should include a review for a new ITHC to determine that the baseline change does not introduce security risks. ITHC's are normally performed prior to formal release/rollout of the changes being made and therefore identification and mitigation plans can be established and undertaken in a safe environment.

Scheduled ITHC for existing IT services

As technology continues to evolve, it is important to understand the impact that this might have on existing solutions. Therefore, it is recommended that Product and Service owners work with the CAT Team (Cyber Assistance Team) to review existing IT solutions and plan to undertake an ITHC on an agreed schedule. This helps to re-assess the security baseline, remediate any risks and issues as agreed, and therefore provide ongoing protection of systems and data.

What can be tested?

The ITHC is performed by highly trained pen testing specialists, and (typically) by an external 3rd party ITHC service provider.

There are many types of penetration tests that can be applied, including but not limited to:

- Network and host configuration
- Web application
- Wireless network
- Client-server application
- End User devices such as laptops or mobile phones
- Social engineering
- Build configuration

Vulnerability Scanning

A vulnerability scan is not the same as an ITHC however, it can be performed and used to help build on the overarching story of the product being tested.

A vulnerability scan is automated and is entirely software whereas an ITHC is conducted by trained, qualified professionals, and uses human interaction and human ingenuity to discover flaws that automated tools often miss.

Primary Points of Contact

The Cyber Assistance Team (CAT) Consultants are the primary points of contact for projects and Product/Service owners. The Consultants will work with the team to help ascertain the ITHC requirement and scope, as well as any forward schedule for ongoing ITHC requirements. You can contact the CAT Team directly to request Consultation support if one is not already working with your project already:

CyberConsultancy@digital.justice.gov.uk

How can I book an ITHC?

If you have a requirement to conduct an ITHC on your network and/or application, please complete and submit the New ITHC Request form:

[New ITHC Request Form](#)

The Cyber Security, Privacy and Live Service Delivery Team manage the engagement and planning coordination between yourself and the 3rd party ITHC Team. If you have any queries, you can contact the team via:

security@justice.gov.uk

Governance, workflow and timeline considerations

Timeline Consideration

It is recommended that an approximate timeline of 8 weeks is considered in your project plan to enable the planning and undertaking of the ITHC. Maturity, size, and complexity of the scope will influence this.

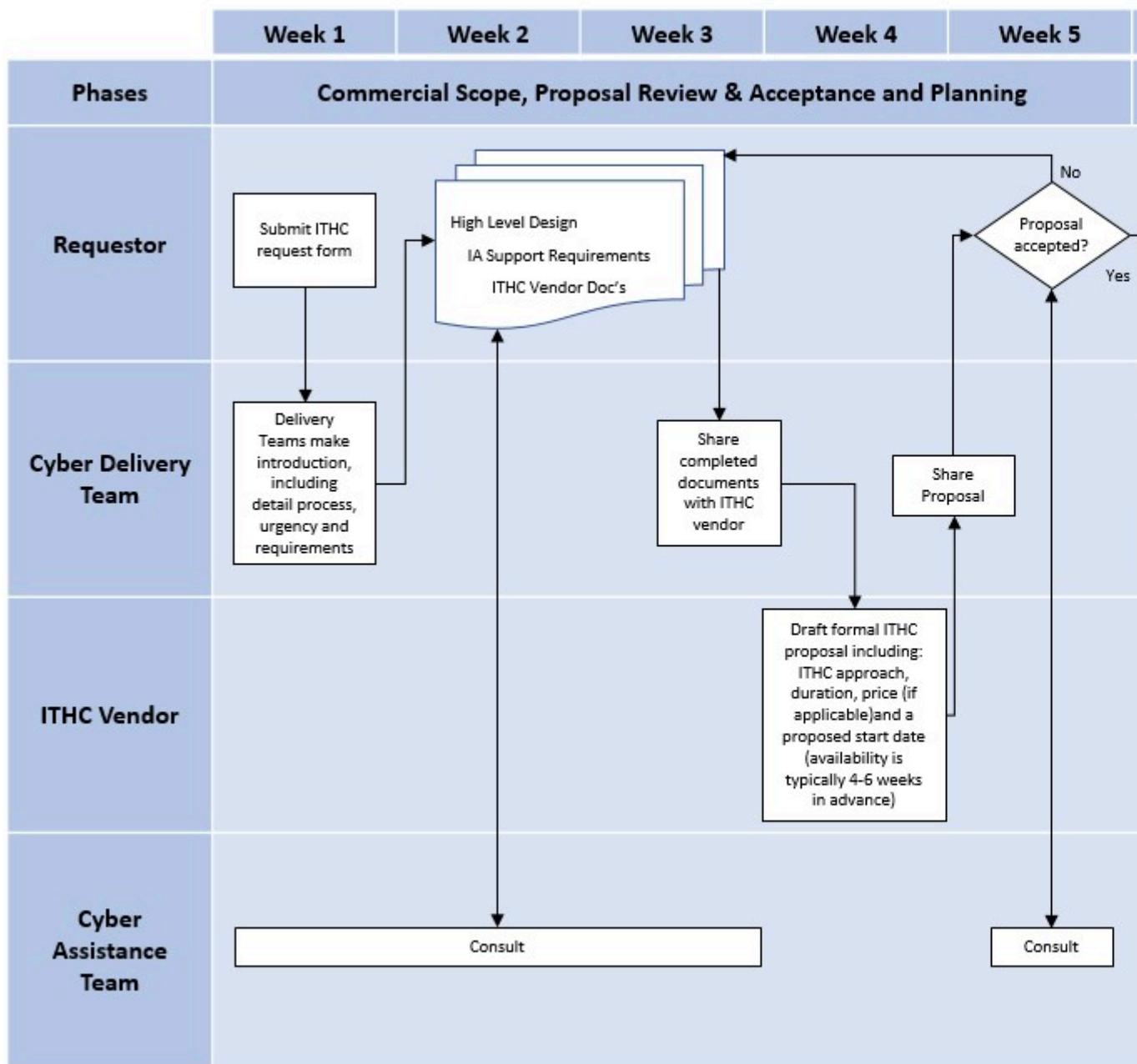
Scope Changes

Changes to scope can be reviewed and considered. However, there is a risk that this will affect delivery dates, ITHC Provider availability, and end quote price.

In scenarios where the formally agreed test dates are impacted, charges might be incurred for delays and cancellations. This is detailed within the Delayed/Cancellation Charges table on the [IT Health Check - Test cancellations and delays](#) on page 476 page.

It is strongly recommended that ITHC scope is understood and confirmed as much as possible, and prior to submission.

The following workflow aims to provide an overview as to the primary roles and action owners involved in the ITHC process:



How to reach us

Should you have any further queries about the ITHC process then please don't hesitate to contact the Cyber Security, Privacy, and Live Service Delivery Team:

security@justice.gov.uk

IT Health Check - Test cancellations and delays

Once IT Health Check (ITHC) execution dates are agreed, it is expected that all parties have:

It is essential that the MoJ identify its information security requirements. There are three main sources of these requirements.

- The legal, statutory, regulatory and contractual requirements that the MoJ, its partners, contractors and service providers have to satisfy.
- The principles, objectives and requirements for information processing that the MoJ and Government have developed to support their operations, for example the protective marking system and government baseline security standards.
- Assessed risks to the MoJ. Through risk assessment, threats to assets are identified, the potential business impacts of these threats are estimated, and the vulnerability to and likelihood of occurrence of the threats are evaluated.

Assessing information security risk

Security requirements are identified by a methodical assessment of security risks. Expenditure on security controls needs to be balanced against the business harm likely to result from security failures. Risk assessment is systematic consideration of:

- The business harm (the 'impact') which is likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.
- The realistic likelihood of such a failure occurring in the light of the threats to and vulnerabilities of the system, and the controls currently implemented.

Managing information security risks

The results of the risk assessment are identified risks and risk severities. These help guide and determine the appropriate management action, and priorities for managing information security risks. Risks with a high severity level would justify the expenditure of more resources to control them than risks with a low severity level.

Risk Management involves identification, selection and implementation of justified security and contingency 'countermeasures' to reduce risks to an acceptable level.

Countermeasures can act in different ways such as:

- Reducing the likelihood of attacks or incidents occurring.
- Reducing the system's vulnerability.
- Reducing the impact of an attack or incident should it occur.
- Detecting the occurrence of attacks or incidents.
- Facilitating recovery from an attack or incident.

Risk management requires a judgement about what is an acceptable level of risk. Although this is a business decision, it does require a thorough understanding of the nature of the risk and the effectiveness of the countermeasures implemented to manage the risk. For some systems or scenarios, specialist advice might be needed.

When taking risk management decisions, consideration must be given to the full implications of the decisions taken. Failure to implement some countermeasures might breach legal or regulatory requirements. This is unlikely to be an acceptable risk management decision. Failure to meet other countermeasures might breach Government information security standards; as a consequence it might not be possible to link the MoJ system with other systems. This might limit the usefulness of the MoJ system.

Consideration must also be given to what are tolerable financial losses, political sensitivities and adverse publicity. The cumulative effect of accepting high levels of risk should also be taken into account.

Information security in projects

Information security controls are considerably cheaper and more effective if incorporated at the system requirements specification and design stage. Information risk assessments must be part of the project process.

Ongoing information security risk management

Effective risk management does not end once a risk assessment has been done and the required countermeasures implemented. Checks need to be carried out to ensure that the countermeasures are being applied effectively. It is also important to carry out periodic reviews of security risks and implemented controls to:

- Take account of changes to business requirements and priorities.
- Consider new threats and vulnerabilities.
- Confirm that controls remain effective and appropriate.

The role of security in risk assessment and risk management

The MoJ security team can provide help in all areas of security risk management for systems. Examples include:

- Advice on risk assessments.
- Help with carrying out risk assessments.
- Assist with the risk management decision process.
- Help with creating and managing documentation compliant with MoJ standards.
- Assisting with mandatory Government risk assessments.
- Advice on compliance checking.

Contact details

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

Glossary and Acronyms

Glossary

This information is a reference list of Ministry of Justice (MoJ) terms and abbreviations.

A more extensive list of acronyms is available [here](#).

Terms

Term	Explanation
Authorised User	Any user of services covered as authorised by the MoJ.
Customer	Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term customers is also sometimes informally used to mean users, for example "this is a customer focused organisation".
Incident	Any event which is not part of the standard operation of a service, and which causes, or might cause, an interruption to, or a reduction in, the quality of that service.
Incident Management	The process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to return the IT service to users as quickly as possible.
Problem	A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.
Problem Management	The process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimise the impact of incidents which cannot be prevented.
Process	A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process might include any of the roles, responsibilities, tools, and management controls required to deliver the outputs reliably. A process might define policies, standards, guidelines, activities, and work instructions if they are needed.
Resolution	Action taken to repair the root cause of an incident or problem, or to implement a workaround.

Term	Explanation
Resolver Group	May include a wide range of IT teams, including support and development personnel, other Service Management Functions (SMFs), other units within the organisation, outsourcing providers, partners, and other third parties.
Service Desk	The single point of contact between the service provider and the users. A typical Service Desk manages incidents and service requests, and handles communication with the users.
Trend Analysis	Analysis of data to identify time related patterns. Trend analysis is used in Problem Management to identify common failures or fragile configuration items, and in Capacity Management as a modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.

Contact details

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



© Crown copyright 2022

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

