Ministry of Justice (MoJ) Cyber Security Guidance: Supplier Edition

Contents

Getting in contact

Reporting an incident

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

Information security policies

Management direction for information security

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

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

The Standard

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

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

IDENTIFY

IDENTIFY is a prerequisite standard that requires:

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

PROTECT

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

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

DETECT

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

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

RESPOND

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

- development and maintenance of an incident response & management plan (including reporting, roles and responsibilities);

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

RECOVER

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

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

IT Security Policy (Overview)

Introduction

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

Who is this for?

This policy is aimed at three audiences:

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

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

Associated documentation

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

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

Principles

All MoJ users **MUST**:

- Comply with the MoJ's Acceptable Use Policy wherever they work.
- Report all security incidents promptly and in line with MoJ's IT Incident Management Policy.
- Make themselves aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other MoJ guidance.

- Be aware of the need for Information Security as an integral part of the day to day business.
- Protect information assets under the control of the organisation.

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

Technical users

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

Service Providers

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

Enforcement

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

Incidents

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

Operational Security Team

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

Contact details

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

IT Security All Users Policy
Introduction

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

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

Who is this for?

This policy is aimed at three audiences:

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

General users	All other staff working for the MoJ.

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

Approach

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

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

Assets

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

Security classification

All MoJ Staff are responsible for ensuring data is:

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

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

Physical and personnel security

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

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

Further information on physical and personnel security is available from MoJGroup Security (mojgroupsecurity@justice.gov.uk) and CPNI Guidance.

Identity and access control

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

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

The MoJ Access Control Guide addresses access control principles such as identification, authentication, authorisation, and accounting.

Password management

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

Email security

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

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

Remote working and portable devices

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

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

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

Malware protection

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

The MoJ Malware Protection Guide addresses the following relevant domains:

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

Roles and responsibilities

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

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

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

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

Role	Responsibility	Which includes...
Senior Information Risk Owners (SIROs)	The MoJ SIRO is responsible for the overall MoJ information risk policy and guidance, and ensures it continues to provide appropriate risk appetite and a suitable risk framework.	Implementing and managing information risk management in their respective business groups.
		Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.
		Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.
Delegated Agency SIROs	The delegated agency SIRO is responsible for the information risk policy and guidance as it applies to their systems and personnel, and ensures the agency adheres to the MoJ's risk appetite and risk framework.	In line with the MoJ SIRO, but for Agency systems and personnel.
Information Asset Owners (IAO)	IAOs, also known as IA Leads, must be satisfied that all required technical, personnel, physical and procedural security controls are in place and followed. IAOs are responsible for ensuring the management and security of their information asset over the whole asset lifecycle.	Logging and monitoring.
		Reviewing access permissions.
		Understanding and addressing risks associated to their information assets.
		Ensuring secure disposal of information when it is no longer required.
System Owners	System Owners are responsible for managing access control rules for their particular system.	Verifying access rights in order to assist a scheduled review audit of User accounts and permissions.
Contract Owners	Contract Owners are responsible for ensuring contractors adhere to the IT Security Policy set out here and in associated documentation.	Verify that contracts are written to reflect the MoJ's IT Security Policy.
		Ensure contractors comply with the requirements set out by this policy and associated documentation.

Role	Responsibility	Which includes...
		Being responsible for escalating the risk of non-compliance by a supplier, and seeking guidance on suspected non-compliance with security requirements in a contract. Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the MoJ, is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.

Incidents

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

Operational Security Team

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

Contact details

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

IT Security Technical Users Policy
Introduction

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

Who is this for?

This policy is aimed at:

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

Vulnerability scanning and patch management

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

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

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

Technical controls

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

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

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

Cryptography

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

However, where staff have procured key material or hardware through the United Kingdom Key Production Authority (UKKPA) or any other cryptographic items where National Cyber Security Centre (NCSC) dictate that national cryptographic policy applies, the NCSC dictate the policy and the Government Functional Standard - GovS 007: Security (previously HMG IA Standard No. 4, Protective Security Controls for the Handling and Management of Cryptographic Items, IS4) applies.

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

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

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

Software development

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

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

Security incident management

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

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

Suppliers and procurement

IT Security

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

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

Further advice can be found in the Information Classification, Handling and Security Guide.

Physical and personnel Security

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

Privileged users

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

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

Risk management

Technical risk assessment and information assurance

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

Audit

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

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

When conducting an audit:

- Documentary evidence must be made available to auditors upon request.
- Details provided should include the implementation of any technical security control in an IT system. Documentary evidence of changes must be reviewed.

- The evaluation should cover all types of changes, including configuration changes, to IT systems, and the IT security implications of those changes. This includes the case where no significant IT security impacts are identified.
- Evidence of operating effectiveness for technical controls must be provided, and the desired risk mitigation as documented in the Information Assurance Framework Process.
- Activities involving verification of operational systems should be carefully planned and agreed to minimise disruptions to business processes.

Incidents

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

Operational Security Team

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

Contact details

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

Media handling

Removable Media

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

What is 'removable' media?

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

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

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

USB memory sticks

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

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

   - Removable media business case form
   - Data Movement form

   Additional guidance information is available about the Data Movement form. When the form is ready, send it to: OperationalSecurityTeam@justice.gov.uk.

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

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

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

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

What's expected of you

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

Contact details

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

Secure Disposal of IT Equipment

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

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

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

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

Equipment or asset type	Data deletion method	Disposal method
Flash (USB)	Delete the data, or erase using manufacturer instructions.	Destroy using commercially available disintegration equipment, to produce particles of a maximum of 6 mm in any direction.

Equipment or asset type	Data deletion method	Disposal method
Hard disk drive	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Break the platters into at least 4 pieces. This can be done either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a Lower Level degauss and then apply a destructive procedure that prevents the disk from turning. For example, punch holes into the platters, or twist or bend them.
Magnetic tapes and floppy disks	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Destroy using a commercially available shredder that meets a recognised international destruction standard. Particles of tape should be no larger than 6 x 15 mm. Alternatively, apply a Lower Level degauss and then cut the tape to no larger than 20 mm in any direction.
Optical media	Data deletion is not possible.	Shred or disintegrate using equipment that meets a recognised international destruction standard. Particles should be no larger than 6 mm in any direction. A high capacity CD and DVD shredder is available at 102 Petty France, suitable for items up to `TOP SECRET`. Contact OperationalSecurityTeam@justice.gov.uk for help with this option.

Owners of the data storage devices are responsible for procuring services that meet the necessary destruction outcomes as described above. Assurance shall be required that the appropriate destruction has taken place for any locally procured MoJ assets, and that an audit trail is available for inspection upon request by MoJ security.

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

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

Contacts

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

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

Contact details

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

Access control

Business requirements of access control

Access Control guide

Introduction

This guide explains how the Ministry of Justice (MoJ) manages access to its IT systems so that users have access only to the material they need to see. This guide has sub-pages which provide in-depth Access Control guidance.

Who is this for?

This guide is aimed at two audiences:

1. The in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation.
2. Any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the MoJ.

Related guides

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

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

Information security principles for access control

These are the Access Control principles you need to know.

- **The 'need-to-know' principle:** Restricting access to information based on a business requirement.
- **Non-repudiation of user actions:** Holding a user accountable for their actions on an IT system.
- **The 'least privilege' principle:** Assigning the least number of privileges required for users to fulfil their work, usually done through Discretionary Access Controls (DAC).
- **User Access Management:** Managing user access to systems and services through a formal user identity lifecycle process.

Access control principles

Effective access control should be implemented by following these four principles.

1. **Identification:** The MoJ should provide a single, unique ID assigned, named and linked to a private account for each user. For example, Lesley is issued a user account that only Lesley uses, and only Lesley can access. This is important so that logging information is accurate (see the Accounting section below for further information).
2. **Authentication:** To access MoJ systems, users must authenticate themselves. They can do so using:

   - something they know (such as a password - the primary authentication method used at the MoJ)
   - something they have (such as a smart card)
   - something they are (biometric authentication such as a fingerprint, voice recognition, iris scan and others)

   Systems holding sensitive information, or systems that are mission critical to the MoJ, must use Multi-Factor Authentication (MFA) to prove user identity. See the Multi-Factor Authentication Guide for further information. If you wish to use an additional method of authentication you should review the National Cyber Security Center's

(NCSC) guidance and contact the Cyber Assistance Team (CAT). For information on authentication methods including OAuth, refer to the Managing User Access Guide.

3. **Authorisation:** Authorisation is the function of specifying access rights/privileges and resources to users, which should be granted in line with the principle of least privilege. Reducing access privileges reduces the "attack surface" of IT systems. This helps to prevent malware and hackers from moving laterally across the network if they compromise a user account.
4. **Accounting:** Successful and unsuccessful attempts to access systems, and user activities conducted while using systems must be recorded in logs. Please see the Security Log Collection Guide for more information. This will help to attribute security events or suspicious activities to users who can be supported to improve their behaviours or held accountable for their actions.

Consider the following points when creating activity logs.

Logs should be:

- stored securely
- backed up, so that data are not lost if there is a system unavailability
- managed according to the sensitivity of the data they hold, for example personal information. Contact the Data Privacy Team for advice on protecting sensitive personal information - privacy@justice.gov.uk.
- stored for a minimum of 6 months

Logs should not be:

- retained for longer than 2 years unless otherwise stipulated. Retention rules may vary on a case by case basis so check with the Data Privacy Team, the Cyber Assistance team, and the MoJ Data Protection Officer if a Log involves personal information. See the Accounting Guide for further information.
- tampered with under any circumstances, for example through modification or removal.

See the Security Log Collection Guide for more information.

Segregation of duties

In some parts of the MoJ, segregation of duties is used to help to reduce the possibility that malicious activity takes place without detection.

You can segregate duties in various ways, including:

- implementing manual or automated Role Based Access Control (RBAC), to enforce user authorisation rights.
- regularly reviewing audit logs to check for suspicious activity
- ensuring strict control of software and data changes
- requiring that a user can perform only *one* of the following roles:
    - identification of a requirement or change management request (Business function)
    - authorisation and approval of a change request (Governance function)
    - design and development (Architect or Developer function)
    - review, inspection, and approval (another Architect or Developer function)
    - implementation in production (System Administrator function)

Contact details

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

Enterprise Access Control Policy

All Ministry of Justice (MoJ) staff (including contractors and agency staff) are entitled to be granted access to the information which is required for their work, subject to their level of clearance and employment status.

Access control mechanisms provide the ability for MoJ IT systems to control the levels of access granted to an individual User or defined groups of individual Users. This section outlines the process for managing User access

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

Legacy information

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

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

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

User and Information Access management

Access control is primarily about enforcing three information security principles:

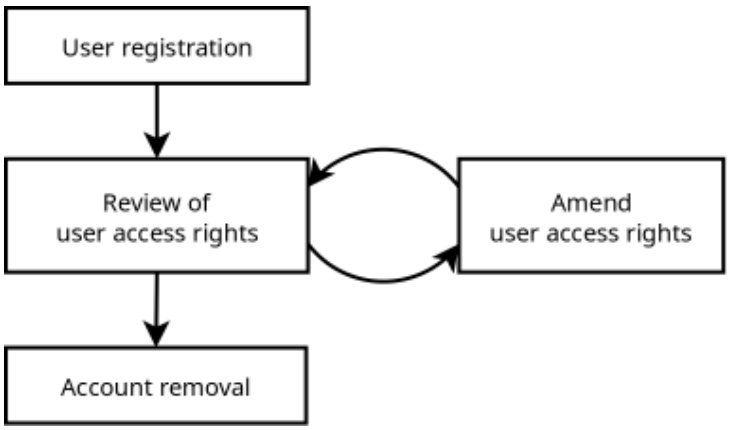
- The *'need-to-know'* principle – restricting access to information based on a business requirement.
- *Non-repudiation* of User actions –holding a User accountable for their actions on an IT system.
- The *'least privilege'* principle – assigning the least number of privileges required to fulfil their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

At a high level, access control in MoJ is based on Role Based Access Control (RBAC). Each user is assigned a role (or set of roles) and access to a piece of information is granted on a per role basis. In general, information will either be subject to RBAC or classified as open access (for example, a HR policy document made available on the MoJ intranet).

Information made available on an open access basis (i.e. not subject to any RBAC restrictions) must be treated as an exception to general access control rules. It is important to ensure any information made available in this way has been validated by the Information Asset Owner (IAO) to ensure that the information does not have 'need-to-know' constraints that impede it's sharing beyond a defined RBAC group (see herefor further details on the role of the IAO).

Management of User access control

The following diagram depicts the 4 stage management lifecycle for managing user access control.



The rest of this section describes each of the 4 stages and outlines what activities are required.

Note: This lifecycle aligns with the MoJ HR processes for new joiners (see: https://intranet.justice.gov.uk/guidance/hr/induction/) and leavers (see: https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/).

User registration and account creation

The following activities must be undertaken for each new User registration:

- The identity of the new User must be confirmed – for an MoJ member of staff this is confirmed by MoJ HR;
- The access rights required must be supplied (for example, the list of RBAC groups and/or applications);
- Confirmation of clearance level (see here for further details);
- The application for User registration must be authorised by a MoJ senior manager.

  Note: This authorisation is used as confirmation of the Users identity and the access rights requested are correct.

In general, individuals who are MoJ staff (including contractors and agency staff) will be provisioned with a User account and a number of roles applicable to the nature of their work so that they can access the relevant MoJ IT systems, application and information. Temporary use of a MoJ IT system may be permitted where a specific business need exists (e.g. to allow an external trainer to train MoJ staff in a new application) subject to clearance checks and a Non-Disclosure Agreement (NDA). A MoJ senior manager must assume total responsibility for the actions undertaken by that temporary User while they are using a MoJ IT system using a temporary account.

Minimum user clearance requirements

Most MoJ IT systems operate at IL3 where information with a protective marking of REST* can be processed. As these systems process HMG protectively marked data, Users must attain a certain clearance level before they can be granted access rights, the exact level depends on the type of access rights required and job role.

For the purposes of this standard, access rights have been broken down into three User account types. Table 1 provide a description for each type and the minimum clearance required.

Table 1: User account type and clearance required

User account type	Description	Minimum Clearance Required
Normal User	Include all Users with entry-level access; includes read/write and read-only Users.	BPSS
Application Administrator / Privileged User	Typically an application system manager, i.e. those with the rights to create/remove user accounts, and provide internal support.	BPSS

User account type	Description	Minimum Clearance Required
Systems Administrator	A systems administrator does not necessarily have a 'need-to-know' over any of the business information held on the systems they support however they do have administrative privileges which allows them to view data held on those systems and change their configuration.	SC

Note: The clearance level indicated in Table 1 is separate to the clearance level required for a particular job role and sets the minimum requirement for access to a MoJ IT system. Most job roles at the MoJ require an individual to attain BPSS however; some job roles require an individual to have a higher clearance such as SC or DV.

Privilege management and review of user access rights

In order to ensure that privileges are assigned on a least privileges basis, the following information must be supplied when requesting a new User account or additional privileges:

- A statement of the access required, for example, a path to a folder or functionality within an application;
- The name/identity of the User requiring access and their associated User account identify (where the request relates to an existing User account);
- Business justification; and
- Approval from a MoJ senior manager.

Review of user access rights

Access rights must be reviewed on a regular basis and may need to be updated as a result of any change in job role, security clearance, or employment status. The review schedule is captured in Table 2.

The following sub-sections outline the key roles involved in the review process and highlights further consideration which should be undertaken when granting privileges for access to knowledge repositories or remote access connectivity.

IT System owner / Information Asset Owner responsibilities

An IT System Owner or Information Asset Owner (IAO) is responsible for managing access control rules for their particular system.

The actual review and implementation of any access control changes may be performed by MoJ service management along with the relevant IT service provider on their behalf however they may be required to verify access rights in order to assist a scheduled review audit of User accounts and permissions.

IT service provider responsibilities

MoJ IT service providers operate as access control custodians (as they retain top-level administration rights) acting on the direction of an IT system manager, IAO's and MoJ senior managers.

The IT service provider will only amend access rights based on either an automatic joiners / leavers notification or from requests made from an authorised individual (as described at the start of this section). In performing these activities on behalf of the MoJ, the IT service provider has the responsibility to:

- Retain a record of all authorised users (granted accounts);
- Retain a record of all access approvals and changes.
- Retain a record of all users granted administrative privileges on any network, system, or application under their administration.

Granting system administrator privileges

Systems administrators by their very nature have privileged access to MoJ IT systems, it is important that the use of system administrative accounts is kept to a minimum, as such:

- Systems administrators must be provisioned with two system accounts, one operates as a normal user, the other as a systems administrator.
- A systems administrator must ensure that they use their normal account as their main working account and only use the elevated privileges of their systems administrator account when required.
- Further details can be found in IT Security SyOPs - System Administrators.

Non-IT service provider Users are not normally permitted to hold system administrative privileges. Exceptions may be granted where there is a legitimate business justification endorsed by a MoJ senior manager or Senior Civil Servant (SCS). Further advice must be sort from the MoJ ITSO.

Access to knowledge repositories

Knowledge repositories such as TRIM, are intended to host generally accessible information (but still internal to the MoJ), however certain categories of personnel may not be entitled to access these repositories (or subsets of information held within them) if they are deemed to contain any information that has a specific or implied access control restriction (e.g. based on clearance level or job role).

The relevant IAO is required to ensure that all information is suitable for sharing without access controls or alternatively shall restrict access to authorised personnel with an appropriate need-to-know.

Remote access

Remote access to a MoJ IT system requires the use of an authentication token (such as an RSA token) in addition to the standard network logon. Each token is unique to a particular individual and must only be issued to those Users who have a business need to access MoJ IT systems remotely, for example, home workers.

Account removal

An individual's User account and any associated access rights must be removed once that individual has either left the organisation or no longer requires access to the IT system (or application) that the account was created for.

It is the responsibility of the line manager to request account removal. The leavers process can be found on the HR intranet page (see: https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/). As part of the HR process, the line manager must inform all relevant IT service providers when a member of staff leaves the organisation and as such instruct them to deactivate and remove their user account. The leavers guidance linked above gives detail on how to contact IT service providers.

Review of User privileges and accounts schedule

Table 2 outlines the review schedule which must be applied to all MoJ IT systems. All User privileges and accounts must be audited in accordance with this schedule, Table 2 states the review activity required with an associated frequency.

Note: It is anticipated that most MoJ IT system will be able to comply with this schedule, however it is recognised that this may not be feasible on some. Any deviation from this schedule must be approved by the system Accreditor and MoJ ITSO (for example a copy of Table 2 with revised schedule can be placed within the relevant system RMADS).

Table 2: Review of User privileges and accounts schedule

Activity	Description	Schedule
Review existing user accounts	Review all the user (and system user) accounts and identify accounts which have not been used in the last 3 months.The list of identified accounts must be reviewed with MoJ HR to identify which accounts can be removed (as the User has left the MoJ) or require deactivation (as the User is on long term leave).	Every 3 months

Activity	Description	Schedule
Review of user access / authentication tokens	Review the usages of remote access authentication tokens (e.g. RSA token) and identify accounts where a token has not been used in the last 3 months. These token must be disabled.	Every 3 months
Review of user account privileges	Review the roles and privileges assigned to a User and remove any which are no longer required.	Every 6-12 months (exact review period to be agreed with the system Accreditor and MoJ ITSO)

User access management

Managing User Access Guide

Introduction

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

Managing access to MoJ systems

The following methods can be used to manage access to the MoJ's systems. They are in order of preference for their use, with 1 providing more secure management features than 3.

Rank	Method	Comment
1	Application Program Interface (API)	Where possible, APIs should be used instead of remote server configuration tools such as Secure Shell (SSH) and Remote Desktop (RDP). This is because APIs offer greater technical control over security systems without the need for parsing commands required by remote server configuration tools.
2	Automated diagnostic data collection	It should be considered the exception for administrators to directly administer a server/node when there is automated diagnostic data collection. Diagnostic data collection allows the underlying technical data to be easily correlated and analysed.
3	Remote server configuration tools	If you cannot use APIs then remote server configuration tools can be used with the following controls.

Use of bastion or 'jump' boxes for access into systems is a useful technical security design that also helps 'choke' and control sessions.

The need to use remote server configuration tools to interact with a server or node can be reduced through improved infrastructure and server design. For instance, the use of stateless cluster expansion or contraction, and the automated diagnostic data capture, can reduce the need to use SSH.

System Admins should only login to a server or node via SSH to execute commands with elevated privileges (typically, root) under exceptional circumstances.

- SSH must be strictly controlled, and environments should be segregated so that no single bastion or 'jump' SSH server can access both production and non-production accounts.
- Do not allow direct logging in as root through SSH. Administrators must have a separate account that they regularly use and `sudo` to root when necessary.
- SSHs must be limited to users who need shell, in contrast to users who might use SSH as a port forwarding tunnel.
- Joiners/Movers/Leavers processes must be strictly enforced (optimally and preferably automated) on SSH servers, as they are a critical and privileged access method.
- SSH access should not be password-based. It should use individually created and purposed SSH key pairs. Private keys must not be shared or re-used.

The Government Digital Service (GDS) recommends the use of the open authorisation standard 'OAuth2' as a means to authenticate users. See the GDS guide for more information.

Contact details

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

Minimum User Clearance Requirements Guide

Introduction

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

Security clearance levels

The Ministry of Justice (MoJ) uses the national security vetting clearance levels:

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

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

Minimum user clearance requirements

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

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

- Has long term, regular, unsupervised access to data centres or communications rooms.
- Has regular privileged unsupervised and unconstrained access to systems which contain data for multiple MoJ systems, for example backups, or console access to multiple cloud services.
- Has cryptography responsibilities and handling, under advice from the Crypto Custodian.
- Has access to multiple system security testing outcomes which reveal vulnerabilities in live services.
- Has a role such as system support or IT investigation role, such that without further authority or authorisation, an individual might:
    - Act as another user.
    - Obtain credentials for another user.
    - Directly access other users' data.

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

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

Please contact the Cyber Assistance Team and refer to the Vetting Policy for further information.

Checking someone's clearance status

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

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

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

Contact details

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

Multi-Factor Authentication (MFA) Guide

Introduction

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

MFA

Users should have their identity authenticated through the following methods:

- something they know (such as a password)
- something they have (such as a mobile phone or smart card), and/or
- something they are (biometric authentication such as a fingerprint).

MFA can be used as a possession-based factor for authentication, by checking for something 'you have'. MFA is sometimes referred to as Two-Factor Authentication (2FA) if it involves a second form of authentication. MFA is referred to as 3, 4, or 5 Factor Authentication if it includes additional authentication requirements. Different methods of additional authentication identify users with varying degrees of accuracy. Care should be taken to ensure true MFA. For example, password and security questions are both dependent 'something the user knows' and therefore are just one factor of authentication.

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

Note:

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

Preference	Type
1.	Hardware-based (for example, Yubikeys or TPM enabled devices)
2.	Software-based (for example, Google Prompt on a mobile device)
3.	Time-based One Time Password (TOTP)-based (the code is held by a dedicated app such as Google Authenticator on a mobile device)

Preference	Type
4.	TOTP-based (the code is held within a multi-purpose app, for example, a password manager app that also holds other factor information)
5.	Certificate-based (a digital certificate used to authenticate a user)
6.	Email-based (a one-time code/link sent to the registered on-file email address)
7.	SMS-based (a one-time code sent via SMS)
8.	Phone-call based (a phone call providing a one-time code or password)

Contact details

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

Privileged Account Management Guide

Introduction

This guide explains how to manage privileged accounts in order to minimise the security risks associated with their use. This is a sub-page to the Access Control Guide.

How to manage privileged accounts

Holders of privileged accounts, such as system administrators, have privileges to perform most or all of the functions within an IT operating system. Staff should have privileged accounts only when there is a business need, in order to prevent malicious actors gaining privileged access to Ministry of Justice (MoJ) systems. The MoJ requires that ownership and use of privileged accounts must be monitored and audited on a monthly basis.

Privileged accounts should be protected with the following controls.

DO
✓ Ensure that privileged users only use their system administrator account when elevated privileges are required. Their general user account should be used for all other work activities.
✓ Ensure that management or administrative access is limited to users who have been suitably authenticated and have been authorised to perform the specific action. Only those with a genuine business need should have an administrative account, however there should be a sufficient number of administrators that there is not a single point of failure due to absence or administrators leaving the MoJ. This should be enforced through the principle of least privilege.
✓ Ensure that Multi Factor Authentication (MFA) is used where possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. MFA should also be used to access enterprise level social media accounts. See the Multi-Factor Authentication Guide for details of preferred MFA types. Where MFA cannot be used on a system, this is considered an exception and should be logged in the risk register.
✓ Ensure that MFA is mandated for a privileged user to conduct important or privileged actions such as changing fundamental configurations including changing registered email addresses or adding another administrator.
✓ Ensure that MFA is used as a validation step, to confirm actions requested by users, such as a MFA re-prompt when attempting to delete or modify data.
✓ Ensure that default passwords are managed securely and safely.

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

Contact details

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

Physical and environmental security

Secure areas

Physical Security Policy

Audience

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

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

This Physical Security Policy applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ-occupied premises.

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

Objective

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

Scope and Definition

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

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

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

Context

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

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

Responsibilities

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

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

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

- Perimeter control.
- Guarding.
- Site access.

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

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

Policy statements

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

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

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

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

Compliance

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

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

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

Physical security advice

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

Equipment

Clear Screen and Desk

Clear Screen

Users shall comply with the following:

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

Clear Desk

Users shall comply with the following:

- Where possible, paper and computer media shall be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, particularly outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, doors must be locked if rooms are left unattended. At the end of each session all `OFFICIAL` and `OFFICIAL-SENSITIVE` information shall be removed from the work place and stored in a locked area.
- When handling `OFFICIAL` documents security shall follow the requirements laid down in the Government Classification Scheme (GCS).
- `OFFICIAL` or `OFFICIAL-SENSITIVE` information, when printed, should be cleared from printers immediately.

It is good practice to lock all rooms and office areas when they are not in use.

Information left on desks is also more likely to be damaged or destroyed in a disaster such as fire or flood.

Laptops

Storing data on laptops

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

If you need to store data on your computer you should always remember to move it into:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An MoJ shared drive.
3. Your MoJ-provided 'home' drive.

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

Where should I save data when using a laptop?

It is best to avoid saving any data on a laptop hard drive. However, if you absolutely must, you should always remember to copy or move the data to the MoJ network as soon as you next can connect to it, either via secure remote access or by direct connection.

In order to avoid potential data loss, save data in:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An MoJ shared drive.
3. Your MoJ-provided 'home' drive.

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

What is the impact of hard drive failures?

Hard drive failures can lead to the irrecoverable loss of data. Any data loss can have security implications for the MoJ, and a significant impact on:

- Our business opportunities.
- Our reputation.
- Our ability to deliver services to the public.

If you experience any issues with your laptop or IT service, ask for help.

How to reset your password

To reset your password, you will need to contact the IT Service Desk. They will carry out checks to confirm your identity. This might include asking your line manager or court manager to confirm your identity, by sending an email to the IT Service Desk. Once your identity is confirmed, your password will be reset and you will quickly regain access to your laptop.

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

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

Digital & Technology - Digital Service Desk

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

HMPPS Information & security:

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

Contact details

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

Locking and shutdown

General

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

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

How do I shutdown my desktop computer?

- Close all applications.
- Shut down the computer by clicking the 'Start' button at the bottom left hand corner of the screen. Next, click 'Shut Down'.
- A pop-up box will appear with a drop-down box. Select 'Shut Down' and click 'OK'. After a short delay, your computer will automatically shut down.
- Switch off your monitor screen.

What are the benefits?

By switching off our computers at the end of each working day, we are contributing towards being energy efficient and environmentally friendly. We are all responsible for our own Carbon Footprint. So, please switch off your PC monitor along with your desktop computer at the end of each working day. In addition, please switch off any other PC monitors if you notice they too have been left on overnight.

What if there are any issues preventing you from switching off your computer?

If there are any issues preventing you from switching off your desktop computer overnight, then please raise this with the IT Service Desk immediately as there could be an underlying fault that needs resolving.

If you require any further information regarding this policy, ask for help.

Locking your computer sessions

Access to most computer systems is controlled by a user name and password. If you have the correct information, you are able to 'log in' or 'log on'. The user name identifies the user as a valid user of the system and the password authenticates that the user is who they say they are.

You are responsible for what you do with an MoJ system or service. You might be held responsible for any actions carried out using your user name and password. You must therefore not allow any one else to do work on any system using your user name and password. If you leave your computer logged on when you are away from it, it might be possible for sensitive information held on the computer system to be used, read, changed, printed or copied by someone not authorised to see it.

If you are leaving your computer unattended for a short period of time, 'lock' the computer by activating the password protected screen saver or similar 'locking' facility. A simple and quick way to lock a Windows computer is:

1. To LOCK - press the Windows key and L key, at the same time.
2. To UNLOCK - press the Ctrl, Alt and Delete keys, at the same time, then log in as normal.

A simple and quick way to lock a Mac computer is:

1. To LOCK - press the Ctrl, Cmd and Q keys, at the same time.
2. To UNLOCK - move the mouse or press any key, then log in as normal.

Laptops
Background

All MoJ laptops have hard disk encryption installed. This protects the entire contents of a laptop's hard disk drive to prevent any data stored locally from being accessed in the event the laptop is either lost or stolen.

Incident

Investigations into security incidents indicate that a common reason for problems is where the correct security procedures are not being followed. For example, laptops are being left logged on overnight.

This is not good security practice.

If a device is lost or stolen whilst the machine is in locked mode, the data on the machine is more vulnerable to a potential security breach.

Leaving the laptop in MoJ premises is not sufficient to guarantee the equipment's security. Laptop losses do sometimes occur within MoJ offices. There is a greater risk of data loss when a laptop is left partially logged on overnight, so you should always fully log off the laptop at the end of your working day.

What you need to do

- Switch off the machine completely at the end of each usage.
- Do not attach the password to the machine or keep the password with the machine.

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

General enquiries, including theft and loss

Dom1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

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

Digital & Technology - Digital Service Desk

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

HMPPS Information & security:

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

Contact details

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

Operations security

Operational procedures and responsibilities

Offshoring Guide

Legacy information

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

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

- CESG (Communications-Electronics Security Group), refer to the National Cyber Security Centre (NCSC), contact security@justice.gov.uk.
- CINRAS (Comsec Incident Notification Reporting and Alerting Scheme), refer to the NCSC, contact security@justice.gov.uk.
- ComSO (Communications Security Officer), contact the Chief Information Security Office (CISO) (security@justice.gov.uk).
- `CONFIDENTIAL`, an older information classification marking.
- CPNI (Centre for the Protection of the National Infrastructure), contact the CISO (security@justice.gov.uk).
- DSO (Departmental Security Officer), contact the Senior Security Advisor (security@justice.gov.uk).
- GPG6 (Good Practice Guide 6: Outsourcing and Offshoring: Managing the Security Risks), refer to the NCSC, contact security@justice.gov.uk.
- IS1 (HMG Infosec Standard 1 Technical Risk Assessment), see the Government Functional Standard - GovS 007: Security.

- IS2 (HMG Infosec Standard 2 Information Risk Management), see the Government Functional Standard - GovS 007: Security.
- IS4 (HMG Infosec Standard 4 Communications Security and Cryptography), see the Government Functional Standard - GovS 007: Security.
- IS6 (HMG Infosec Standard 6 Protecting Personal Data and Managing Information Risk), see the Government Functional Standard - GovS 007: Security.
- ITSO (Information Technology Security Officer), contact the CISO (security@justice.gov.uk).
- `RESTRICTED`, an older information classification marking.
- SPF (Security Policy Framework), see the Government Functional Standard - GovS 007: Security, contact security@justice.gov.uk.

Introduction

Document Purpose

This document is the Ministry of Justice (MoJ) IT Information Assurance (IA) Policy and Guidance for offshoring of MoJ Information Systems, development, or other support services. The document states the IA requirements that must be complied with for offshore developments, and presents considerations to be taken into account when deciding whether to offshore an element of MoJ capability.

This document has not been developed in isolation. It draws heavily and intentionally on other guidance, particularly HMG Good Practice Guide (GPG) 6: Outsourcing & Offshoring: Managing the Security Risks. This document collates the high-level points from the CESG and CPNI guidance, and interprets these in the context of the MoJ.

The target audience for this document includes MoJ personnel with a requirement to make offshoring decisions; and MoJ suppliers who are considering, or currently engaged in, delivery of MoJ capabilities with an offshore element.

Background

General

Some suppliers are keen to offshore elements of IT service delivery, due to a perception that this will reap strong financial benefits. Reasons often cited for offshoring decisions include: cost savings in wages and other business expenses relative to the domestic (UK) market; access to specific specialist technical skills; and access to a large labour pool to support peak loading or large-scale projects.

Offshoring is not, however, without its potential issues. Badly managed offshoring of a project can lead to over-runs in project costs and timescales which eclipse any anticipated benefits. In the worst cases, project over-spend, over-run and quality issues can lead to project failure. Also, there are a number of scenarios where offshoring would introduce unmanageable risks; and/or result in a direct breach of UK law; and/or result in unexpected financial exposure for the MoJ. These risks are not necessarily a blocker to offshoring, but must be balanced carefully against the anticipated benefits.

Quality, Cost and Time

Offshoring presents a range of ubiquitous project risks which must be considered. There can be a tendency to over-estimate the savings that can be made, and to underestimate the potential configuration management and integration issues. Much of the cost saving from offshore development comes from the labour-cost-differential between the UK and favoured offshore locations. High levels of inflation as those economies expand, often through development as offshore centres, can shrink or even overwhelm any predicted cost savings. This may make the supplier's position untenable. Cultural differences can also exaggerate normal project stress points that occur during integration and handover of outsourced elements. Customers and suppliers often fail to fully appreciate increased incidental costs, e.g. due to the additional testing overhead incurred. The long delivery chain can also become a difficulty to manage. In some less stable locations, risks due to war, civil uprising and the availability of Critical National Infrastructure also lead to unique business continuity issues.

Legal Risk

Offshore projects may also fall foul of more pedestrian but no less severe risks due to local laws at the offshore location. It is important to ask questions such as: to what extent are the contractual conditions legally binding for an offshore company in a proposed location; how difficult and expensive would it be to mount a legal challenge in the case of contract breach, and is this any less likely to be successful; and who would have priority over information and other assets in the event of a dispute. This is not just an issue which the MoJ will face when engaging an offshore

supplier directly; it is also an issue that MoJ's suppliers will face, but may not be aware of, when subcontracting elements of delivery.

Risk to "UK PLC"

Many MoJ information systems handle HMG Protectively Marked and/or personal and sensitive personal data. These add a number of specific risks over-and-above the more usual project risks. Local data protection laws may not provide an appropriate level of legal protection, for the data or data subjects involved, against rogue individuals and criminal groups who misappropriate personal data. This may be more of a problem for countries outside of the European Economic Area (EEA), where the legal framework may not be familiar. Commercially sensitive information may be similarly at risk. Political instability may lead to facilities being over-run, which as well as having business continuity implications may also have severe consequences from potential disclosure of Protectively Marked information. Also, organised criminals are able to operate more actively and openly in some overseas jurisdictions. Such activity may be driven by political or economic advantage. It is not only the physical site but also application development that can present a risk to data. A vulnerability or backdoor, engineered into an application either maliciously or inadvertently, could be used to leak information over an extended period or even indefinitely without being identified. The Open Web Application Security Project (OWASP) presents a list of common vulnerabilities that occur due to careless programming and ineffectual testing. Deliberately engineered vulnerabilities and backdoors are considerably more difficult to identify and address.

Personnel Risks

Most people are reliable and honest. However, for work on systems which will handle sensitive Government information, a small number of unreliable or dishonest individuals can cause a disproportionate amount of harm. It is critical, therefore, to identify such high-risk individuals. Pre-employment screening is a critical element in helping to do this, along with aftercare to balance risks identified during screening, and monitor changes to an individual's status that may affect their reliability. Similarly, legal defences provide a complementary means to deter inappropriate behaviour.

Scope

This document covers offshoring of MoJ business activities. Offshoring is defined here to include development or provision of services, from outside the UK or otherwise using non-UK resources, for domestic (UK) consumption.

The scope of offshoring is a broad one. This may involve, for example:

- Development of applications, and/or provision of second-line and/or third-line support for these applications, from non-UK locations and/or by non-UK Nationals.
- Follow-the-sun technical support for commercial products, so that suitable technical resources are available at times when domestic support would be unsociable.
- Remote managed services for wholesale provision of MoJ capabilities from non-UK locations and/or by non-UK Nationals.
- Other provision of support to the MoJ from non-UK locations and/or by non-UK Nationals.

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

Captive centres	Refers to an office that forms part of a Government department but is physically located outside the UK.
Far-shoring	Covers scenarios where development is to be transferred to locations outside of the EEA. Far-shoring may enable more cost-effective development than near-shoring, or may enable access to specific technical skills. However, far-shoring may require additional National Security and/or legislative considerations to be taken into account relative to near-shoring.
Landed resources	Covers scenarios where resources from outside the UK are brought to the UK. This may be, for example, to provide: low-cost labour, specialised skill-sets, and/or support for peak loads. Use of landed resources makes

	it possible to obtain considerably more control over the working environment of non-UK Nationals on HMG programmes, and can enable a more robust screening and aftercare regime for personnel, traded off against increased development costs.
Near-shoring	Covers scenarios where development is to be transferred to other countries within the European Economic Area (EEA), where legislation on key issues such as data protection, electronic communications and human rights is broadly aligned with UK legislation. It should be noted that although key legislation is broadly aligned across the EEA by a requirement to meet common EU Directives, the legislation that has been implemented by different EEC nations in order to comply with these directives has some important differences.
Other	Any other activity using non-UK locations and/or non-UK Nationals to deliver elements of HMG capability.

Exclusions from Scope

Exclusion 1: This document does not address UK or overseas legislation. The MoJ legal team, the MoJ Data Access and Compliance Unit (DACU), and the MoJ Data Protection EU and International Policy Teams must be consulted on legal issues. Contact privacy@justice.gov.uk for assistance.

Exclusion 2: This document also does not address protection of individuals' personal data, except within the context of HMG Security Policy. The Data Access and Compliance Unit (DACU) must be consulted on personal data, the DPA, and related issues.

With the exception of Landed Resources, deployment to locations within the UK does not count as offshoring and is therefore beyond the scope of this document. It is noted, however, that there will be other geographical factors to be taken into account even within the UK. For example, there are special security arrangements for Northern Ireland, and different freedom of information legislation between England and Scotland. These differences should in no way be considered as a justification not to outsource to other UK locations, but would need to be addressed in the local controls deployed.

Outsourcing is beyond the scope of this document, except insofar as outsourcing arrangements are directly related to offshoring requirements (e.g. contractual obligations to be included in supplier contracts and subcontracts). Outsourcing is defined by HMG GPG6 as:

> a contractual relationship with an external vendor that is usually characterised by the transfer of assets, such as facilities, staff or hardware. It can include facilities management (for data centres or networks), application development and maintenance functions, end-user computing, or business process services.

Document Overview

The remainder of this document is structured as follows:

- The relevant IA Constraints and Considerations for offshoring.
- A checklist of assessment activities at different points in the development lifecycle.

IA Constraints and Considerations
General

There are a number of specific IA Constraints which must be satisfied by any MoJ offshoring arrangements. There are also a number of key considerations that must be borne in mind in deciding whether to offshore a particular capability or service.

This section of the document sets out the general IA requirements and constraints that must be complied with when offshoring MoJ capabilities. This document is derived from some of the good but generic CESG and CPNI documentation on the subject, outlined in the Further Reading section. This guidance should not be used as a

substitute for engagement with the MoJ Accreditor or with MoJ IT IA, who will be able to provide tailored guidance to support individual decisions; it is intended more as general guidance on MoJ policy, to support initial decision-making and project planning.

Accountability

The development or management of a capability can be outsourced, however, ultimate accountability and responsibility for a capability remains with the end-customer for that capability: in this case the MoJ. The MoJ remains accountable for work performed by third parties on its behalf, whereas outsourcing and offshoring can make it difficult to directly identify and manage information risks and issues. Strong governance and clear lines of accountability and responsibility are required to address this.

REQUIREMENT 1: The MoJ remains ultimately responsible for the security and overall delivery of offshore application development and other services. All supplier and subcontractor contracts must ensure that the MoJ retains overall control over all security-relevant elements of the delivery. The enforceability of supplier and subcontractor contracts in overseas jurisdictions must be ratified by MoJ legal experts.

If a capability is delivered late, is substandard, fails completely or is compromised, then the MoJ will need to put measures into place to ensure business continuity while a remedial plan is developed and worked through, otherwise essential public services may not be deliverable in the interim. In some cases, the MoJ may find itself financially or legally liable for shortcomings in supplier subcontracts. Also, the MoJ rather than the supplier will almost certainly suffer the brunt of any bad publicity.

The core function of the MoJ is to deliver services for the general good, rather than commercial commodities. As such, the impact of failure is not quantifiable in purely financial terms. Failure or compromise of MoJ services cannot therefore be fully remedied through financial penalties in supplier contracts, although financial penalty clauses can nonetheless serve as a motivation for suppliers to deliver on time and to quality.

The responsibility of the MoJ for its own security and overall delivery is reinforced within the HMG SPF, at Paragraph 7, under Roles and Responsibilities:

> Accounting Officers (e.g. Head of Department/Permanent Secretary) have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. This responsibility must be supported by a Senior Information Risk Owner (SIRO) and the day-to-day duties may be delegated to the Departmental Security Officer (DSO), IT Security Officer (ITSO), Information Asset Owners (IAOs), supported by the Lead Accreditor.

REQUIREMENT 2: The MoJ SIRO remains accountable for information risks, including risks to Protectively Marked and personal data, in an offshore context. These risks must be documented and presented to the SIRO, and must be explicitly agreed to before any contract with an offshore element is accepted. In some cases, a submission to the Cabinet Office IA Delivery Group may be necessary. The MoJ Accreditor, MoJ IT IA, DACU and Legal experts must be engaged by the project team as soon as a potential offshoring requirement is identified, to enable identification of these information risks. Close engagement with these Special Interest Groups must be maintained for the delivery lifetime. This engagement must be formally set out in the delivery plan.

The MoJ will bear the main impact of any compromise of the Confidentiality, Integrity and/or Availability of public services that are delivered or managed on its behalf.

The ultimate decision on whether the IA risk of outsourcing is acceptable will therefore be made by the SIRO, as advised by the IAO and the MoJ Accreditor. HMG security policy requires that the SIRO must personal approve all large-scale information-related outsourcing and offshoring decisions. The SIRO is also required to approve the offshoring of personal data sets and, in some cases, submit plans for scrutiny by the Cabinet Office IA Delivery Group. The MoJ Accreditor, MoJ IA function and SIRO must be involved as soon as a potential offshoring proposal is identified, so that a decision on whether the proposal presents an acceptable level of information risk can be made at the earliest opportunity. This limits the likelihood of nugatory work by the project team.

The requirement for early and ongoing engagement with the MoJ Accreditor and MoJ IA function is reinforced by HMG GPG6 :

> The risk assessment and treatment plan must be reviewed by the Accreditor and presented to the SIRO at each stage of the procurement process.

Risk Assessment

Before any sensible dialogue can be had around whether or not offshoring is acceptable, the value of the assets to be offshored and the threats for the offshore location and/or personnel must be properly understood. Asset valuation and threat assessment must therefore be conducted as an upfront activity for any proposal, and will require early engagement with all interested parties. Risk assessment must be conducted as an initial activity, and regularly revisited as the project progresses. All threat assessment and risk assessment activities will need to be conducted in collaboration between the supplier as risk manager, and the MoJ as the owner of the threat and the risk.

REQUIREMENT 3: All MoJ assets and/or activities to be offshored must be identified, and a Threat Assessment for those assets/activities at the proposed offshore location carried out. This includes not only physical and software assets but also information and service assets. The value and business impact of compromise for each information asset must be determined against the HMG Business Impact Table and MoJ Business Impact guidelines; valuations must be agreed with the Information Asset Owner for each asset. A Privacy Impact Assessment (PIA) is also required, as discussed further in REQUIREMENT 5 below.

The set of assets to be offshored not only includes any specific capabilities to be developed or managed, but will also include any incidental assets which are required to support these activities. For example:

- Development will require test data and schemas which may in themselves attract a Protective Marking or have other particular sensitivities.
- Some development activities may be deemed to require real or anonymised data, rather than fully synthetic test data, to ensure the robustness of critical applications or to test revised applications against historical data from extant capabilities.

  Wherever it is considered that there may be a requirement to use real or anonymised data, rather than synthetic data, the MoJ "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, see this guidance.
- Effective application development may require knowledge of real configuration information to support pre-integration-testing activities, or of broader MoJ network infrastructure designs in order to tailor and optimise development. Some of this information may attract a Protective Marking or have other particular sensitivities. The information shared with offshore developers should be minimised to the fullest extent that is possible.
- Poor coding practices often result in sensitive information such as network configuration information, user and administrator credentials, and other sensitive details being hard-coded into applications. Support for development, for third-line support and application maintenance, and for upgrades to MoJ IT capabilities may therefore necessitate some unavoidable access to sensitive information for which there is no specific need-to-know by the development or maintenance team.

REQUIREMENT 4: Sensitive MoJ assets and/or activities should not be offshored to Countries where Special Security Regulations Apply, or to Countries in which there is a Substantial Security Threat to British Interests.

It is the policy of the MoJ that Protectively Marked or otherwise sensitive MoJ assets, and development or support activities relating to these assets, should not be offshored to Countries where Special Security Regulations Apply, or to Countries in which there is a Substantial Security Threat to British Interests. The MoJ ITSO can provide further details of these, on a need-to-know basis, in response to specific requests. It is the policy of the MoJ that activities involving Protectively Marked or otherwise sensitive MoJ information should not be offshored to these locations. In cases where there is an exceptionally compelling business case for offshoring to one of these locations, the MoJ ITSO must be consulted and will advise the business on suitability, weighing up all of the relevant factors and assessing the extent to which the proposed compensating controls mitigate the risk.

REQUIREMENT 5: MoJ assets and/or activities should not be offshored to countries where political stability, practical considerations and/or legal issues (e.g. compliance with the DPA) may result in a significantly-above-baseline risk to the confidentiality, integrity and/or availability of Protectively Marked or other sensitive data, or where there is not an adequate level of protection for the rights of data subjects in relation to their personal data.

Not all countries which have issues with political and/or economic instability are listed as CSSRA or Substantial Security Threat countries. There are several other countries that are not on the list which nonetheless present a high risk for offshore development and operations. These countries should be avoided on the general principle of avoiding development environments where the local threat is significantly above baseline. Also, as discussed above, the

CSSRA and the list of Substantial Security Threat countries change from time to time. By not offshoring in unstable locations, the risk of outsourcing to a country that subsequently ends up on one of these lists is reduced.

In addition to the above, there are some politically stable locations where it is nonetheless difficult or impossible to meet other essential requirements for the handling of Protectively Marked or other sensitive data (e.g. personal data). Inability to assure the identity and history of personnel, and local legislation on disclosure of data (for example, in response to local FoI or law enforcement obligations), are common examples which can lead to issues with screening and with retaining control of information.

In addition to countries with political and/or economic issues, as discussed above, there may also be threats and risks as a result of other nations' legal systems. Legal constraints in some countries may:

- Conflict with IA requirements under the HMG SPF and supporting guidance;
- Conflict with requirements under the Data Protection Act (DPA) and/or other UK Law; and
- Expose the MoJ to untenable legal liabilities in the event that something goes wrong.

A particular consideration for offshoring is DPA Principle 8: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

Legal advice must be engaged, separately to IA advice, to identify any potential legal issues in advance of making any offshoring decision.

REQUIREMENT 6: An information risk assessment for each offshore location must be conducted by the Offshoring Company or organisation. This risk assessment must be subject to review and acceptance by MoJ IA. This should include an IS1 Risk Assessment, an assessment against ISO27001 controls, and a "Delta Assessment" setting out any HMG requirements that may be unenforceable, any variations to HMG policy that may be required, and how it is proposed to address these Deltas. A Privacy Impact Assessment (PIA), taking into account local legal considerations at the offshore location, must also be conducted. The risks, and the costs of mitigating the risks, must be balanced against the benefits to be gained from outsourcing. A Risk Management Plan must be developed and maintained to identify the mitigations required to address offshoring risks and estimate the costs of implementing these mitigations.

An information risk assessment for the offshore location must be conducted. This must include an IS1 Risk Assessment in line with current HMG guidance. It must also include an assessment of physical, procedural, personnel and technical measures at the offshore location set against the ISO27001 requirements and highlighting the additional controls in place to address the concerns set out within HMG Good Practice Guide 6 for specific ISO27001 controls. It must also include a "Delta Assessment" setting out any HMG requirements that may be unenforceable, any variations to HMG policy that may be required, and how it is proposed to address these deltas.

The high-level information risk assessment is required at the proposal stage, prior to contract negotiations. This must be developed incrementally into a more detailed risk assessment as the project progresses. This risk assessment must take into account all assets to be offshored and the specific Threat Assessment for the offshore location and/or personnel. The risk assessment must meet the requirements of both HMG IS1 and HMG GPG6. The requirements of HMG IS6 relating to personal data can be more difficult to meet in an offshore context, so particular care must be taken to ensure that the PIA takes the offshore location into account and offshore elements of the contract are compliant with IS6.

A Risk Management Plan is essential to address the risks identified through offshoring. As well as providing evidence that the supplier has adequately considered these risks, this will also provide the basis for estimating the cost overhead of mitigating offshoring risks, enabling a more accurate assessment of whether offshoring truly represents value for money. For example, the cost of provisioning a suitably segregated technical environment to support offshore development work; combined with the cost of providing a suitably secure link to enable remote access for offshore workers; and the cost of sending out suitably trained personnel for regular inspections of an overseas site; may significantly erode any cost savings.

Supplier Arrangements

REQUIREMENT 7: IA constraints and requirements for offshoring must be made clear to suppliers prior to contract award and explicitly set out in contractual arrangements with suppliers to the MoJ. These constraints and requirements must be flowed down to all subcontractors along the chain of supply. Conversely, Intellectual Property Rights must flow up contractually from the offshore supplier or suppliers to the MoJ.

IA requirements must be determined as an integral part of the initial requirements for any capability, and an assessment of competing solutions against IA requirements must be a critical part of supplier selection during the tender process. Offshoring is no exception to this. Offshoring constraints and requirements must be made clear to suppliers prior to contract award, so that there can be no ambiguity during costing for any solution to be delivered to the MoJ. There will almost certainly be additional time, effort and cost involved to implement the required physical controls, testing and decommissioning activities required to meet IA requirements in an offshore development environment.

Some suppliers with UK bases may wish to offshore and/or subcontract elements of their contracts with the MoJ. If elements of a contract have been offshored to a subcontractor working in one location, that subcontractor may themselves wish to offshore elements of their subcontract to a different offshore location. IA constraints and requirements must be applicable to all of those who are party to the contract. For example, an offshore organisation based in Country A, which provides second-line support for an MoJ application from Country A, might rely on teams from its offices in Country B to conduct development and third-line support activities. This would have an impact on the Threat Assessment and hence the risks to the capability.

The MoJ is responsible for all offshore activities that are being conducted on its behalf, and must retain oversight of these activities. This requirement must be enforced within supplier contracts, through robustly worded requirements for contractual flow-down of IA responsibilities through the supplier chain. The MoJ must be given both visibility and an over-riding right of approval or veto for subcontractor arrangements. A right of audit without warning must be maintained by the MoJ, including full access to all physical sites, logical capabilities, accounting logs, etc.

Ownership of all information assets, and all Intellectual Property Rights, developed as part of MoJ contracts must flow up to the MoJ. All MoJ information, including vestidual information, which is held on a supplier's physical assets, must be erased and/or disposed of to the satisfaction of MoJ IT IA during decommissioning. Again, legal limitations on the enforceability of contractual conditions in some locations must be taken into account and specialist legal advice will be required to ensure that all necessary contractual conditions are enforceable at offshore development locations.

The above issues with contractual flow-down of responsibilities and flow-up of ownership are best managed if the MoJ retains control of the subcontract chain. Ideally, wherever practicable, MoJ supplier contracts should only allow further subcontracts to be let with the explicit permission of the MoJ. This enables the cost and complexity of due-diligence checking and contractual enforcement, not just for offshoring considerations but also more generally, to be more effectually bounded and controlled.

REQUIREMENT 8: Suppliers must ensure that offshore development is conducted according to UK and other relevant IA standards and legislation.

The requirements of the HMG SPF must be adhered to for offshore development. This may require significant changes to local working practices in some cases. The requirements of other relevant British and International standards must also be adhered to. Most notably for IA considerations, this specifically includes ISO27001 (Information Security Management System) and ISO25999 (Business Continuity). Offshore sites and processes must be demonstrably compliant with ISO27001, and must be subject to a combination of scheduled and snap audits to ensure this. In addition to all of the usual ISO27001 conditions, particular considerations for offshore development are set out within HMG GPG6. Any issues found during audit must be addressed over timescales that are agreeable to MoJ IT IA, with formal progress tracking of issues as they are addressed and resolved. Business Continuity can introduce particular issues in some offshore contexts, where events such as natural disasters, pandemics, criminal activity, acts of war, etc. may be sufficiently probable to merit more rigorous mitigations than for UK development. Factors such as staff turnover may also present particular issues in an offshore context, particularly where Landed Resources are used.

REQUIREMENT 9: The robustness of development and integration testing activities must be reconfirmed. Regular development and integration testing activities by the System Integrator are particularly essential for offshoring, where there will potentially be less visibility or direct control over the development environment. Additional code review must also be conducted to a level that is agreed by MoJ IT IA to be commensurate with the value of the information that will be handled by the live application, or otherwise accessible to the live application.

REQUIREMENT 10: Security Enforcing Functionality elements of MoJ applications must not be offshored. For other elements of application code which process, store and transmit sensitive MoJ information assets, an onshore security code review must be conducted. This should be to a level that is agreed by MoJ IT IA to be commensurate with the

value of the information handled by the live application, or otherwise accessible to the live application. This is likely to include a combination of manual and automated testing, and should be supplemented by a more comprehensive ITHC scope where appropriate.

The basic principle of ensuring thorough testing during every stage of application development must be reinforced where elements of development and/or maintenance are to be offshored. Requirements for testing against internationally recognised standards (e.g. the OWASP standard for secure code development) must be secured in supplier contracts and flowed down to offshore and other subcontractors. A test data strategy must be agreed prior to contract award. A high-level test strategy must also be agreed prior to contract award, and should be developed and maintained as a living plan as the project evolves. There should be assurance that provision for testing is adequate to mitigate the Information Assurance and other System Integration risks identified.

Testing, including security testing, must be conducted at every stage of the development (unit testing, integration testing, acceptance testing, etc). The MoJ must retain executive control over the testing process, maintaining visibility of all test results and progress on remedial activities. This includes control by MoJ IT IA over security elements of testing. The MoJ must be contractually able to exert control over testing, through clauses to reject as substandard any delivery where test scopes are not agreed by the MoJ, where results are not fully disclosed or where remedial activities are deemed to be insufficient.

Some applications which are deemed to be relatively low value in themselves may be used to handle information with a significantly higher value, or may be able to easily access sensitive information (for example, other information within the same business domain or information that is directly accessible from connections to servers in other business domains). Additional code review must also be conducted as part of the development testing of these applications, with particular emphasis on Security Enforcing elements of the application. In some cases, the MoJ Accreditor and the IA Team may require the use of automated test tools and/or line-by-line code review for elements of the application to be conducted by UK Security Cleared personnel at onshore locations.

In some cases, the additional testing overhead required will outweigh the benefits gained by offshoring. This is most likely for particularly complex and/or sensitive applications. Back-doors and vulnerabilities become increasingly easy to engineer (either deliberately or accidentally) for complex applications, and increasingly difficult to identify. Based on experience, it is likely that suppliers will underestimate the true time and expense that would be necessary to test complex applications. It is important that supplier proposals are realistic about the benefits of any offshoring elements of the proposals, and have accommodated realistic costs for testing to address offshoring risks. Where test costs are not realistic, this does not represent a cost saving for the MoJ. If the supplier is not making an acceptable profit on a contract, then relationships between the supplier and the MoJ will undoubtedly deteriorate. The supplier is likely to try to recoup losses by streamlining test processes (driving operational risk); by reclaiming costs from elsewhere (driving project cost); or by delivering below expectations or not at all (driving project risk). Such unrealistic proposals should be either corrected or rejected during supplier selection and contract award.

Use of Landed Resources

REQUIREMENT 11: Where landed resources are used to support project activities they must be vetted to a level appropriate for the value of the information assets and collateral assets that will potentially be available to them. Where it is not possible to meet some BPSS evidence requirements, suitable alternative evidence must be obtained and compensating controls such as technical lockdown, supervision and monitoring must be applied. If it is not possible to lock down the physical environment to the satisfaction of MoJ IT IA then landed resources must not be used. For higher levels of clearance such as SC, if a landed resource cannot achieve the required level of clearance or if there are prohibitive conditions on the individual's clearance, then that landed resource must not be used.

The most basic level of Government security checking, the Baseline Personnel Security Standard (BPSS) check, is designed to provide an assessment of three key features of the individual to be vetted: their identity; their right to work; and the reliability, integrity and honesty of those individuals.

The BPSS requires that an individual's identity be confirmed, by matching some evidence of identity such as a passport or drivers licence, with evidence of address and activity in the community such as bills and bank statements. This provides a level of information that can be followed up for UK applicants if an individual raises any particular concerns. Further checks can be cheaply and easily conducted, to provide additional evidence that an individual with the asserted identity and address exists, and to confirm that the individual asserting that identity and address is not attempting identity theft. Where individuals originate from outside of the UK, and have not been in the UK for a suitably long period of time, it can be more difficult to obtain a suitably reliable history for those individuals (long-

term footprint) to support effective screening. The Baseline Standard requires at least three years' worth of previous employment history. From experience, it is considered that a commensurate length of time is also required to build up a suitably rich credit history and social footprint to enable reliable checks to be conducted.

Even confirming an individual's true identity may be problematic in some non-EU locations, where proofs of identity may be non-existent or considerably less reliable. It should also be noted that, for countries where record-keeping is managed locally rather than centrally, engagement at a local level to support checks can very quickly become prohibitively expensive for a moderately-sized workforce and/or where there is a high rate of staff turnover.

Personal and employers' references are used, partly to support confirmation of identity, and partly to enable checking of an individual's reliability, integrity and honesty. Criminal records declarations and supporting criminal records checks are also used as part of BPSS clearance. Criminal record checks for UK citizens are generally comprehensive and accurate. However, the accuracy of police and criminal records checks varies widely between different countries. The CPNI has compiled information on such checks for a reasonably broad set of overseas jurisdictions. The CPNI documentation also provides useful information on the reliability of identify checks overseas. A risk-balance decision by the SIRO is likely to be required on whether to accept the additional BPSS vetting risk for the offshore workforce.

To compensate for any shortcomings or uncertainty in vetting, landed resources brought to the UK are likely to require a heightened level of monitoring and supervision, as well as additional technical measures to limit and audit their physical and logical access to HMG information systems. HMG information systems to which landed resources have access must be locked down and supported by tight access controls over-and-above the usual HMG baseline.

Where higher levels of clearance such as SC are required it may not be possible for a specific landed resource to achieve the required level of clearance, or there may be prohibitive conditions on the individual's clearance. In those cases, the specific landed resource must not be used. For example, a non-UK National who has been within the UK for a sufficiently long period of time may be able to obtain an SC clearance. However, if a role requires handling of UK Eyes Only material, then the prohibitions on the SC clearance for that non-UK national would make them inappropriate to use for that role.

In exceptional circumstances, the use of landed resources from countries where Special Security Regulations Apply, or to countries in which there is a Substantial Security Threat to British Interests, depending on why that specific country is on the list. The MoJ ITSO should be consulted in such cases and will advise the business on suitability, weighing up all of the relevant factors and assessing the extent to which the proposed compensating controls mitigate the risk.

Assessment Activities

Every offshoring decision must be made on a case-by-case basis, after balancing all of the facts of the situation. The project activities required to ensure this are set out below.

REQUIREMENT 1 and REQUIREMENT 2

Project Scoping & Supplier Selection

MoJ Project Team:

- Ensure that the MoJ SIRO, MoJ Accreditor, MoJ IT IA and MoJ Central IA are engaged from project conception.
- Ensure that any contracts which may require personal data to be offshored outside of the EEA include suitable contractual clauses developed from reliable templates. For example, for personal data transferred outside of the EEA, the European Commission approved model clauses as per Directive 95/46/EC of the European Parliament and of the Council, provides a useful template. The legal framework for managing the export of Protectively Marked information must be no less restrictive than this. Consider whether additional contractual clauses are required to mitigate risk and avoid legal problems arising from local laws and jurisdictional issues.
- Ensure that offshoring elements of all Invitation To Tender (ITT) or other supplier requirements documentation are developed in consultation with MoJ Legal functions, DACU, and the MoJ Accreditor and MoJ IT IA. Ensure that these parties are key reviewers for all tender requirements.
- On the advice of the Accreditor, DACU, MoJ IT IA, and MoJ Central IA, present and obtain approval for a SIRO Submission comprehensively setting out the risks and mitigations of any offshoring proposals.
- Understand and advise the SIRO of any requirement that may exist for a submission to the Cabinet Office IA Delivery Group. Prepare any required submission on behalf of the SIRO, for approval.

- Ensure that the operational assessment and investment appraisal of competing supplier proposals factors in the additional MoJ IT IA effort requirement to address offshore elements of the proposal, as per Requirement 11 below.
- Reject any bids that do not meet IA, DACU or Legal requirements for offshoring.

MoJ Accreditor/IA:

- Develop the elements of tender requirements which cover offshoring constraints and requirements.
- Review outsourcing elements of supplier bids and other proposals.
- Advise the MoJ Project Team on the suitability of offshoring proposals.

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

Contract Award

MoJ Project Team:

- Ensure that offshoring requirements and constraints are worked up to a robust level of detail within the final supplier contract, and subject to a further round of review by the MoJ Accreditor and MoJ IT IA prior to acceptance and contract award.
- Update any SIRO Submissions and submissions to the Cabinet Office IA Delivery Group to reflect the changes in the information risk between project scoping and contract award. Obtain acceptance for any changes from the SIRO prior to acceptance and contract award. Engage MoJ IT IA to advise and liaise with the SIRO.

MoJ Accreditor/IA:

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

Development

MoJ Project Team:

- Use supplier audit as a mechanism to ensure that contractual requirements are being met. Where supplier indiscretions are found enforce remedial action.
- Where remedial action is not implemented, or ineffectually implemented, invoke contractual penalty clauses.
- Add and maintain any submissions to the SIRO and the Cabinet Office IA Delivery Group as necessary. Engage MoJ IT IA to advise and liaise with the SIRO.

MoJ Accreditor/IA:

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

In-Service & Beyond

MoJ Service Management:

- Use supplier audit as a mechanism to ensure that contractual requirements are being met. Where supplier indiscretions are found enforce remedial action.
- Where remedial action is not implemented, or ineffectually implemented, invoke contractual penalty clauses.
- Add and maintain any submissions to the SIRO and the Cabinet Office IA Delivery Group as necessary. Engage MoJ IT IA to advise and liaise with the SIRO.

MoJ Accreditor/IA:

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

REQUIREMENT 3
Project Scoping & Supplier Selection

Supplier:

- Identify what hardware, software and information assets need to be offshored.

- Set out asset valuations for the Confidentiality, Integrity and Availability of all assets. Core information assets must be valued according to the SAL and clarification sought for any ambiguities. Collateral information assets (crypto, credentials, etc) must be valued in line with MoJ and HMG guidance.
- Asset valuations for all hardware and software assets must be clearly justified in the proposal documentation, and submitted to the MoJ Accreditor for review.

MoJ Project Team:

- Ensure that supplier proposals include unambiguous asset valuations. Request clarification on any points of ambiguity. Ensure that the Information Asset Owner(s), the Accreditor and MoJ IT IA are engaged on an on-going basis.
- Reject any proposals that do not meet with Requirement 3.

MoJ Accreditor/IA:

- Ensure that a clear and detailed SAL is generated on a per-project basis, setting out the valuations for all information assets.
- Review hardware, software and asset valuations on supplier proposals.

Contract Award

MoJ Project Team:

- Ensure that the supplier contract includes an explicit requirement to develop and maintain hardware, software and information asset registers. The requirement should explicitly stipulate that registers be maintained in the MoJ standard format, or in an equivalent format which contains (as a minimum) all of the information in the MoJ standard format. Ensure that the supplier is supplied with a copy of this standard format in advance of contract award, so that they can take any additional overheads into account in their proposal.
- Ensure that the supplier contract includes a right of audit, including no-notice audit, by the MoJ. The scope of audit must encompass hardware and software asset registers, all hardware and software assets, and all other elements related to the provision (physical sites, personnel, etc.)

MoJ Service Management:

- Maintain a MoJ standard format for hardware and software asset registers.

Development

Supplier:

- Develop and maintain hardware, software and information asset registers, covering all hardware, software and information assets. This must be developed in the MoJ standard format, or in an equivalent format which contains (as a minimum) all of the information in the MoJ standard format.

MoJ Project Team:

- Maintain visibility of the hardware, software and information asset registers. Ensure that there is a regular joint (supplier/MoJ) activity to audit physical and software assets against these registers. Conduct irregular spot audits of assets against the registers. Ensure that remedial activity is time-lined, tracked and completed according to schedule by the supplier.

MoJ Accreditor/IA:

- Advise physical and logical audit of assets, and remedial activity.

In-Service & Beyond

Supplier:

- Ensure that the hardware, software and information asset registers are maintained as part of an ITIL service wrap for the delivered service. This must be maintained in the MoJ standard format, or in an equivalent format which contains (as a minimum) all of the information in the MoJ standard format.

MoJ Service Management:

- Maintain visibility of the hardware, software and information asset registers. Ensure that there is a regular joint (supplier/MoJ) activity to audit physical and software assets against these registers. Conduct irregular spot audits of assets against the registers. Ensure that remedial activity is time-lined, tracked and completed according to schedule by the supplier.

MoJ Accreditor/IA:

- Advise physical and logical audit of assets, and remedial activity.

REQUIREMENT 4 and REQUIREMENT 5

Project Scoping & Supplier Selection

Supplier:

- Ensure that any potential requirements to offshore any elements of service delivery are explicitly communicated with the MoJ as part of the tender response.

MoJ Project Team:

- Ensure that suppliers are explicit about any proposals for offshoring any elements of the delivery when they develop their bids to supply a capability.
- Ensure that the Accreditor, the IA Team, DACU and MoJ Legal advisors are aware of any potential requirements to offshore elements of the delivery.
- Work with the Accreditor and MoJ IT IA to identify and resolve any potential IA issues for work at these offshore locations or involving personnel from these locations.
- Work with DACU to identify and resolve any potential DPA issues for work at these offshore locations or involving personnel from these locations.
- Obtain confirmation from MoJ Legal Advisors that work at these offshore locations or involving personnel from these locations will not cause any potential conflict with UK Law or leave the MoJ exposed to any additional legal liability.
- Reject any proposals that do not meet with Requirement 4 or Requirement 5.

MoJ Accreditor/IA

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

Contract Award

MoJ Project Team:

- Ensure that the supplier contract explicitly prohibits offshoring except where locations and controls are explicitly set out within the contract.
- Ensure that the contract prohibits offshoring to CSSRA and Substantial Security Threat countries, and any other identified problem countries, and that the contract contains flow-down provisions of all offshoring constraints for all subcontracts.
- Ensure that the supplier contract includes a requirement to consult the MoJ before offshoring any elements of the delivery except where explicitly set out in the contract.
- Ensure that the Accreditor and MoJ IT IA are critical reviewers for all supplier contracts with an offshoring requirement.

MoJ Accreditor/IA:

- Advise the MoJ Project team on what countries are currently on the lists, and advise on exceptions on a case-by-case basis.
- Review offshoring elements of supplier contracts.

Development

Supplier:

- Ensure that any potential emerging requirement to offshore any elements of delivery are communicated immediately to the MoJ.

MoJ Project Team:

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

In-Service & Beyond

Supplier:

- Ensure that any potential emerging requirement to offshore any elements of delivery are communicated immediately to the MoJ.

MoJ Service Management:

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

REQUIREMENT 6

Project Scoping & Supplier Selection

Supplier:

- Conduct an initial IS1 Risk Assessment, In line with the MoJ-provided threat assessment, which includes offshoring risks. This must include an HMG GPG6 compliance assessment, highlighting specific low-level risks due to any offshoring proposals, as part of the overall proposal to supply a capability.
- Develop a specific Risk Management Plan to address offshoring threats and risks, detailing how these identified will be mitigated. The Risk Management Plan must provide an estimate of the costs required to implement the proposed mitigations, and any consequent issues that may arise.
- Conduct a Privacy Impact Assessment (PIA) for the proposed solution, including an assessment of the PIA requirements covering the elements of information to be outsourced and documenting how the proposals meet these requirements.

MoJ Project Team:

- Ensure that suppliers are aware of the requirement to include an IS1 Risk Assessment, HMG GPG6 compliance, and supporting low-level risk assessment.
- Reject any proposals that do not contain a PIA, or which contain a PIA that is deemed by DACU, the MoJ Accreditor, or MoJ IT IA to be inadequate.
- Reject any proposals that do not contain a risk assessment, or which contain a risk assessment that is deemed by the MoJ Accreditor and MoJ IT IA to be inadequate.
- Reject any proposals where the mitigations proposed in the Risk Management Plan are deemed by the MoJ Accreditor and MoJ IT IA to be inadequate, or the costs of implementing those mitigations are deemed by the MoJ Security Architecture Team to be unrealistic.

MoJ Accreditor/IA

- Develop bespoke threat assessments and advice for any proposed offshore locations and for use of non-UK personnel for development. Engage with the UK Security Authorities as necessary to support this.
- Review Risk Assessment elements of supplier proposals.

Contract Award

MoJ Project Team:

- Ensure that the supplier contract includes terms requiring the supplier to update the Risk Assessment and Risk Management Plan, including offshoring considerations, immediately following contract award and maintain this as a through-life activity. As a minimum, the supplier should be required to update the risk assessment (and have this approved by the MoJ) for any contract change and as part of the acceptance criteria for each distinct phase of the development.
- Ensure that the Accreditor and MoJ IT IA are critical reviewers for all supplier contracts with an offshoring requirement.
- Ensure that the outcomes of the PIA are folded into the supplier contract.

- Ensure that the project budget includes a suitable level of contingency to accommodate any changes in offshoring costs due to change in Threat Assessment for the offshore environment.

MoJ Accreditor/IA:

- Review offshoring elements of supplier contracts, including the terms and conditions surrounding risk assessment.

Development

Supplier:

- Maintain the risk assessment, including offshoring considerations, in line with contractual requirements.
- Ensure that offshoring arrangements do not break obligations arising from the PIA.
- Maintain the Risk Management Plan, including offshoring considerations, in line with contractual requirements.

MoJ Project Team:

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

MoJ Accreditor/IA

- Provide support for any required review of the supplier risk assessment, including offshoring considerations, in line with contractual requirements.

In-Service & Beyond

Supplier:

- Maintain the risk assessment, including offshoring considerations, in line with contractual requirements.
- Ensure that offshoring arrangements do not break obligations arising from the PIA.
- Maintain the Risk Management Plan, including offshoring considerations, in line with contractual requirements.

MoJ Service Management:

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

MoJ Accreditor/IA

- Provide support for any required review of the supplier risk assessment, including offshoring considerations, in line with contractual requirements.

REQUIREMENT 7
Project Scoping & Supplier Selection

Supplier:

- Identify any potential offshoring requirement as soon as possible in the tender process. Where proposals include an element of offshoring, it must be explicitly stated in the supplier's response to the security requirements. This must explicitly state how security will be maintained in an offshore context (including responses to User Security Requirements, System Security Requirements, etc.)

MoJ Project Team:

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

MoJ Accreditor/IA:

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

Contract Award

MoJ Project Team:

- Ensure that the supplier contract specifically mandates compliance with all offshoring security requirements.

- Ensure that the supplier contract mandates blanket flow-down of all contractual constraints and obligations to all of the suppliers' suppliers, all of the way down the supply chain.
- Ensure that the contract makes provision for routine and no-notice audit of supplier compliance with offshoring requirements, at any-and-all supplier locations and subcontractor locations that are relevant to the work.

MoJ Accreditor/IA

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

Development

Supplier:

- Inform the MoJ upfront if any emerging requirements develop to offshore elements of the solution. Demonstrate how these requirements will be compliant with contractual obligations, and highlight and contractual obligations that would need to be relaxed in order for the proposal to work, balancing this against the potential benefit and considering a range of practicable options (as determined through engagement with the MoJ Project Team, the MoJ Accreditor and MoJ IT IA. Work with MoJ to ensure that this can be managed in a secure way.

MoJ Project Team:

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

MoJ Accreditor/IA:

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

In-Service & Beyond

Supplier:

- Inform the MoJ upfront if any emerging requirements develop to offshore elements of the solution. Demonstrate how these requirements will be compliant with contractual obligations, and highlight and contractual obligations that would need to be relaxed in order for the proposal to work, balancing this against the potential benefit and considering a range of practicable options (as determined through engagement with the MoJ Project Team, the MoJ Accreditor and MoJ IT IA. Work with MoJ to ensure that this can be managed in a secure way.

MoJ Service Management:

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

MoJ Accreditor/IA:

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

REQUIREMENT 8

Project Scoping & Supplier Selection

Supplier:

- Ensure that proposals include an explicit assessment of compliance (including any points of non-compliance) of offshoring elements of proposals with relevant Legislation and Standards. This includes: the DPA and other relevant legislation; the HMG SPF and supporting documentation (specifically, but not exclusively, HMG IS6, HMG GPG6 and the SPF MRs themselves); relevant ISO standards (most notably ISO27001 and ISO25999); Cabinet Office Guidance on IT Offshoring; and local MoJ IA Requirements.
- Ensure that named CLAS Consultant resources are used on the supplier proposal to ensure that this proposal addresses all relevant HMG IA requirements and documentation (including offshoring requirements), and is compliant with these.

MoJ Project Team:

- Ensure that MoJ IA Requirements are made available to suppliers, and that they are aware of their obligations to explicitly demonstrate compliance with offshore elements of their proposals against these.

MoJ Accreditor/IA:

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

Contract Award

MoJ Project Team:

- Ensure explicit supplier compliance with all relevant identified legislation and standards (as per the list set out in the previous column, plus any other relevant standards identified during the tender process) are set out in the contract.
- Ensure IA are engaged in the procurement process, and that IA concerns relating to offshoring elements of the contract are addressed to the satisfaction of the Accreditor prior to awarding the contract.

MoJ Procurement:

- Support the MoJ Project Team in the development of contractual requirements around offshoring. Review contractual clauses relating to offshoring.
- Ensure IA are engaged in the procurement process, and that IA concerns relating to offshoring elements of the contract are addressed to the satisfaction of the Accreditor prior to awarding the contract.

Development

All:

- As per Requirement 7, above.

In-Service & Beyond

All:

- As per Requirement 7, above.

REQUIREMENT 9 and REQUIREMENT 10
Project Scoping & Supplier Selection

Supplier:

- Ensure that the proposal includes provision for through-development testing, including security testing. Demonstrable compliance with the OWASP Testing Guide (downloadable from the OWASP web-site) is encouraged. The level of security testing required must be agreed with the Accreditor, and will need to be directly commensurate with the risk involved.

MoJ Project Team:

- Ensure that suppliers are aware of the requirement for testing, including not only functional testing but also security testing. Reject any proposals that do not make provision for this.
- Ensure that supplier proposals are realistic about the benefits of any offshoring elements of the proposals, and have accommodated realistic project costs and timescales for testing to address offshoring risks. Conduct an internal sanity check of supplier estimates for security and other testing. Reject any proposals where cost or time estimates are unrealistic.

MoJ Accreditor/IA:

- Support assessment of functional and security testing proposals.

Contract Award

MoJ Project Team:

- Ensure that the contract requires the supplier to test the solution against internationally recognised standards at all stages of the development (unit testing, integration testing, acceptance testing, etc). Suppliers must be contractually required to agree test scopes, including security test scopes, with the MoJ before the start of testing.

The MoJ must be contractually entitled to visibility of all test results and progress on remedial activities to the MoJ. Ensure that the scope of testing in the contract includes security testing of the solution, at a level agreed with the Accreditor and the IA Team.

- Ensure that the contract retains executive control over the test process by the MoJ, with the ability to reject substandard delivery, require remediation and enforce contractual penalty clauses.

MoJ Accreditor/IA:

- Review offshoring elements of supplier contracts, including test arrangements. Provide input to the Project Team as required to support contractual terms for test, particularly security elements of testing.

Development

Supplier:

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

MoJ Project Team:

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

MoJ Accreditor/IA:

- Support test review and remedial activities.

In-Service & Beyond

Supplier:

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

MoJ Service Management:

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

MoJ Accreditor/IA:

- Support test review and remedial activities.

REQUIREMENT 11

Project Scoping & Supplier Selection

Supplier:

- Ensure that any proposal to use landed resources is clearly stated. Ensure that any associated costs and risks are identified.
- Where landed resources are to be used, ensure that the proposal clearly sets out what information assets and collateral assets would be made available to those resources, how many landed resources are proposed, from where, what level of clearance would be required, and how clearance information requirements would be satisfied.
- Where clearance is not possible to an equivalent level for a landed resource as for a UK resource, identify what the additional residual risks of this will be, how it is proposed to mitigate these risks. The proposal should identify any practical difficulties with these arrangements and how they will be overcome, as well as setting out the additional costs involved.

MoJ Project Team:

- In liaison with the MoJ Accreditor and MoJ IT IA, ensure that proposals for using Landed Resources are realistic.
- Ensure that the costs associated with the use of landed resources have been fully considered in the proposal.
- Reject any unrealistic or un-costed proposals for use of Landed Resources.

MoJ Accreditor/IA

- Support assessment of security risk and residual risk with supplier proposals to use landed resources.

- Advise on the feasibility of using landed resources from high-threat countries if relevant.

Contract Award

Supplier:

- Ensure that use of landed resources is in line with contractual requirements.

MoJ Project Team:

- Ensure that the supplier contract includes provision to enforce suitable security controls surrounding landed resources, as agreed during supplier selection.
- Ensure that the project budget includes a suitable level of contingency to accommodate any changes in offshoring costs due to change in Threat Assessment for landed resources.

MoJ Accreditor/IA:

- Review offshoring elements of supplier contracts.

Development

Supplier:

- Ensure that all landed resources are vetted to a level commensurate with the value of the information to be handled by that landed resource. Where it is not possible to effectively vet a landed resource to the required level, landed resources must not be used.
- Inform the MoJ immediately if resource requirements change.

MoJ Project Team:

- Ensure that the MoJ Accreditor and MoJ IT IA are kept fully informed of any change in supplier requirements, and that no change in Landed Resource requirements is agreed without the explicit approval of the IA Team.
- Ensure that the supplier is kept fully informed of any change in Threat Assessment relating to landed resources and of the impact on project delivery.

MoJ Accreditor/IA

- Ensure that the MoJ Project Team are made aware of any change in Threat Assessment relating to Landed Resources, and of how this will impact the project.

In-Service & Beyond

Supplier:

- Ensure that all landed resources are vetted to a level commensurate with the value of the information to be handled by that landed resource. Where it is not possible to effectively vet a landed resource to the required level, landed resources must not be used.
- Inform the MoJ immediately if resource requirements change.

MoJ Service Management:

- Ensure that the MoJ Accreditor and MoJ IT IA are kept fully informed of any change in supplier requirements, and that no change in landed resource requirements is agreed without the explicit approval of the IA Team.
- Ensure that the supplier is kept fully informed of any change in Threat Assessment relating to landed resources and of the impact on project delivery.

Further Reading

Title	Version / Issue
CPNI Personnel Security in Offshore Centres	04/2009
CPNI Good Practice Guide: Outsourcing: Security Governance Framework for IT Managed Service Provision	02/08/2006

Title	Version / Issue
CESG Good Practice Guide 16: Taking and Using Cryptographic Items Overseas	Issue 1.0, 08/2009
CESG Good Practice Guide 23: Assessing the Threat of Technical Attack Against IT Systems	Issue 1.0, 04/2010

Notes

http://www.owasp.org

Wherever it is considered that there may be a requirement to use real or anonymised data, rather than synthetic data, the MoJ "Policy on the use of live personal data for the testing of IT systems, processes or procedures" must be complied with. For more information, see this guidance.

A particular consideration for offshoring is DPA Principle 8: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

For example, an offshore organisation based in Country A, which provides second-line support for an MoJ application from Country A, might rely on teams from its offices in Country B to conduct development and third-line support activities. This would have an impact on the Threat Assessment and hence the risks to the capability.

The Baseline Standard requires at least three years' worth of previous employment history. From experience, it is considered that a commensurate length of time is also required to build up a suitably rich credit history and social footprint to enable reliable checks to be conducted.

http://www.cpni.gov.uk/advice/personnel-security1/overseas-criminal-record-checks/

For example, for personal data transferred outside of the EEA the European Commission approved model clauses as per Directive 95/46/EC of the European Parliament and of the Council, provides a useful template. This can be found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF. The legal framework for managing the export of Protectively Marked information must be no less restrictive than this.

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

The additional costs for offshore proposals will include potentially significant additional costs for IA and Accreditor resources to support bid assessment, solution review, initial Accreditation, re-accreditation and through-life support. An increased requirement for IA engagement and design scrutiny will be inevitable, and would need to be determined by IA. Activities such as audit and remediation are likely to involve an increased time overhead and travel expenses (e.g. for physical site visits to remote sites at overseas locations to conduct audits and follow-up remediation). Other additional project and in-service assurance is almost certain to be necessary.

Logging and monitoring

Accounting

The base principle

Any access, and subsequent activity, to any system or data **must** employ adequate accounting techniques to ensure events can be attributed to the authenticated entity.

Accounting information must be stored in a way that it cannot be readily manipulated, particularly by the authenticated entity.

Log data security & governance

Log data can include Personal Data or inadvertent sensitive data (when an application or system is unexpectedly verbose) and must be adequately protected and governed in a comparable way to the original system's data.

Security-related log data retention

Log data created and processed for information security purposes should be retained for no longer than 2 (two) years by default (this is subject to any legislative or regulative compliance requirements) but for a minimum of 6 months.

These times are generalistic as a guide, and require contextual analysis particularly where Personal Data is involved.

Commercial off-the-shelf applications

We have developed a series of logging requirements for Commercial off-the-shelf (COTS) applications, such as Software-as-a-Service (SaaS) solutions or where applications are not so customised that they can reasonably be considered bespoke/custom for the Ministry of Justice (MoJ).

Baseline Maturity Tier
1. User directory services

Log Collection Principle(s): 1, 2

User directory services, or interactions with them, must create and forward Authentication and Authorisation events.

User directories within application environments can be rich and diverse, such technologies include:

- Active Directory (AD)
- Azure Active Directory
- OpenLDAP
- Amazon Web Services (Accounts and Incognito)
- Okta
- Auth0
- Github.com (acting as an identity provider)
- Google Workspace (acting as an identity provider)
- Oracle identity stores
- Local user stores within operating systems leveraged by tenant applications

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Authenticated user activity events

Log Collection Principle(s): 6

Applications should create viable user activity audit information for authenticated users to reasonably identify which authenticated user took which action.

1. User/group identifier(s)
2. Action/query

3. Response size
4. Response time

Enhanced Maturity Tier
1. Data store events

Log Collection Principle(s): 6

Temporary data stores (such as intermediate queues) and permanent data store (such as databases) are key data locations and all interactions should be highly auditable.

1. Data store identifier(s)
2. Credential identifier(s)
3. Query
4. Query response size
5. Query response time

2. Unauthenticated user activity events

Log Collection Principle(s): 6

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

1. End-client identifier(s)
2. Query metadata:
    a. Destination identifier (such as target hostname, TCP/UDP port and/or full URI)
    b. Query type (for example, `HTTP GET` or `HTTP POST`)
    c. Query size
3. Response size
4. Response time

Custom Applications

We have developed a series of logging requirements for custom applications, such as digital services, applications materially customised that they can reasonably be considered bespoke/custom for the Ministry of Justice (MoJ) and line of business applications at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

Baseline Maturity Tier
1. User directory services

Log Collection Principle(s): 1, 2

User directory services, or interactions with them, must create and forward Authentication and Authorisation events.

User directories within application environments can be rich and diverse, such technologies include:

- Active Directory (AD)
- Azure Active Directory
- OpenLDAP
- Amazon Web Services (Accounts and Incognito)
- Okta
- Auth0
- Github.com (acting as an identity provider)
- Google Workspace (acting as an identity provider)
- Oracle identity stores
- Local user stores within operating systems leveraged by tenant applications

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Authenticated user activity events

Log Collection Principle(s): 6

Applications should create viable user activity audit information for authenticated users so it is reasonably possible to understand retrospectively which actions the user took or attempted.

1. User/group identifier(s)
2. Action/query
3. Response size
4. Response time

3. Unauthenticated user activity events

Log Collection Principle(s): 6

Where unauthenticated users interact with applications (for example, a digital service published and available on the general Internet), associated audit information must be created.

1. End-client identifier(s)
2. Query metadata:
    a. Destination identifier (such as target hostname, TCP/UDP port and/or full URI)
    b. Query type (for example, `HTTP GET` or `HTTP POST`)
    c. Query size
3. Response size
4. Response time

Enhanced Maturity Tier

1. Pipeline events

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

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

1. Source identifier(s)
    a. User(s)
    b. Repository

2. Activity events
    a. Resource creation
    b. Resource destruction
    c. Target environment

2. Data store events

Log Collection Principle(s): 6

Temporary data stores (such as intermediate queues) and permanent data store (such as databases) are key data locations and all interactions should be highly auditable.

1. Data store identifier(s)
2. Credential identifier(s)
3. Query
4. Query response size
5. Query response time

Logging and monitoring

Related information

Security Log Collection on page 71

Overview

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

This is permitted under data protection legislation, to help defend MoJ services against cyber security attacks, and misuse (such as fraud). General Data Protection Regulation (GDPR) Recital 49 notes that the processing of personal data (to the extent that is strictly necessary and proportionate) to ensure the security of a system which forms the underlying lawful basis for why the MoJ processes this type of data for this purpose.

This is why the MoJ can log and monitor external interactions with its services, looking for evidence of cyber security attacks. It also allows the MoJ to act to protect those services. For example, the MoJ can block an IP address associated with known malware, or which is trying to perform a denial of service attack.

At the same time, the MoJ is careful not to “over-retain” log information, or to share it with those who do not need to see it, without lawful justification. The MoJ must always act in a proportionate way with this data.

The MoJ Chief Information Security Office (CISO) is ultimately responsible for all logging and monitoring systems which have been implemented for cyber security purposes. This means that the CISO is also the Information Asset Owner for all logging and monitoring data.

Log retention

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

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

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

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

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

Protecting log files and log data

Default permissions must be set on logging and monitoring systems such that only ops staff for that service, and the MoJ's security operations team (OperationalSecurityTeam@justice.gov.uk), have access to the data in them. All access to the raw logging and monitoring data must also be logged.

Bulk exporting from such logging systems is prohibited by default. Where analysis is required using sensitive logs, it must be performed “in-situ”. Bulk exporting should be prevented by default, using technical or other access controls where possible. If a bulk extract from a logging system is required, for example, into a more complex analytical system or as part of a wider migration, this requires the prior approval of the MoJ CISO.

Contact details

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

Online identifiers in security logging and monitoring
Overview

It can sometimes be counter-intuitive to think of IP addresses, cookies, and log data as personal data. However there are good reasons why it is important fort he Ministry of Justice (MoJ) during design, implementation, and operation of MoJ online services. Put simply, it is easiest for the MoJ to assume that any information captured and processed through public-facing services might contain personal information, and to protect this information accordingly.

What are online identifiers?

Online identifiers are anything that could be used to track someone as they interact with MoJ online services. This can include, for example:

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

Online identifiers could also include metadata captured about a device interacting with MoJ services if this information is sufficiently different to allow devices to be reliably identified.

Why are online identifiers treated as personal data?

If there is any way to tie an online identifier to an individual, then that identifier needs to be treated as though it is personal data.

The way this mapping might be achieved is unimportant.

It could be because the user later provides personal data to the MoJ as part of using a service, and in doing so providesa link between all of the activities that their IP or session cookie has done with their identity.

There might also be a legal route available to the MoJ to determine the identity behind an identifier. For example, by making a lawful request to an ISP to uncover the person associated with a dynamic IP address at a particular time.

For more information on this, see the Information Commissioner's Office (ICO) key definitions, and “Recital 30” from the Article 29 Working Group. There is also an informative article here.

What does this mean for MoJ services?

It is important to think carefully about:

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

MoJ privacy notices on services must be clear about the information captured as part of a user's interaction. This includes “anonymous” interactions, such as simple browsing information about the services. Metadata like this must be included in the scope of privacy impact assessments for MoJ services.

Note: Theoretically, privacy notices are only mandatory for externally-facing services. They are not required for internal services. However, it is undoubtedly good practice - and highly recommended - to apply the same approach, for consistency.

Contact details

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

Protective Monitoring Guide

About this document

Note: This is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon. Please contact us before using this on a new project: itpolicycontent@digital.justice.gov.uk

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

This document is the MoJ IT Security – Protective Monitoring Guide. It is designed to help protect MoJ ICT systems by providing implementation guidance for a protective monitoring solution.

How to use this document

The purpose of this document is to provide guidance on developing a protective monitoring schema for a MoJ ICT system. It must be read in conjunction with CESG Good Practice Guide No.13 - Protective Monitoring for HMG ICT Systems.

Note: This document is a supplement to CESG Good Practice Guide No.13 - Protective Monitoring for HMG ICT Systems, not a replacement.

Overview
Introduction

Protective Monitoring is a set of business processes, with essential support technology, that oversees how ICT systems are used and to assure user accountability for their use of ICT facilities. Protective monitoring places mechanisms for collecting ICT log information to provide an audit trail of defined security relevant events which can be used for reporting and alerting.

HMG Security Policy Framework (SPF) Mandatory Requirement 9 states that:

> Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

In order to meet that requirement, the SPF stipulates that ICT systems must:

> Put in place a proportionate risk based suite of technical policies and controls including: ... IV. Protective Monitoring;

Policy statements on protective monitoring are covered in IT Security – Technical Controls Policy, while this document sets out the MoJ guidance for its implementation.

Scope

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

Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. Protective monitoring is captured as a basic requirement in Level 1 of this model, which the MoJ will need to demonstrate compliance with in their IAMM return to the Cabinet Office.

Basics of protective monitoring
Accounting and Auditing

Protective monitoring as described in CESG Good Practice Guide (GPG) No.13 centres on the concepts of Account and Auditing.

Accounting is defined as 'the process of collecting and recording information about events', whilst Auditing is defined as 'the systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled'.

An organisation can choose to account for almost every transaction that takes place on the system, but then audit almost none of them. When deciding on what approach to take with accounting and auditing it is necessary to first identify what types of information should be recorded then decide what information should be examined and how regularly that examination should be carried out.

Accreditation and protective monitoring

The audit criteria and the decision on what information is collected and alerted upon must be derived from a risk assessment conducted against the ICT system. This decision making process for the selection of protective monitoring controls forms part of the Accreditation process where the resultant protective monitoring solution **must be** documented in the Risk Management and Accreditation Document Set (RMADS). This document provides guidance on the selection of those controls, the key questions to be applied to that selection and a template for documenting it.

Further details on the Accreditation process can be found in the Accreditation Framework.

Note: The Accreditor will assess any protective monitoring solution against CESG GPG No.13, the policy statement in the IT Security – Technical Controls Policy and this guide.

Accounting

The decision on how much information needs to be recorded in an accounting log requires a comprehensive assessment and must be consummate with the risks identified. Recording too much information can be as great a problem as recording too little. If too much information is recorded it can become extremely difficult to review and can cause performance and capacity problems for an ICT system. If too little information is recorded it may be impossible to investigate a security incident effectively.

A good method of analysing this problem is to have a structured approach whereby the different types of information which could be captured are analysed at the different levels of an ICT system (e.g. network, system and application), building a picture of the inter-relationships between the different accounting logs (at those different levels). For example, accounting may take place at the following levels:

- Network accounting (e.g. logs created by network components, such as firewalls or domain controller);
- System accounting (e.g. logs created by individual host systems, such as Windows server security logs);
- Application accounting (e.g. logs created by individual applications).

The network/systems logs can be used to record the following security events:

- All actions taken by the Administrators;
- All actions taken whilst using the database administrators' accounts;
- All updates to operating system files;
- All workstation time-outs;
- Any attempts to copy the password file;
- All updates to the application software;
- Use of the system out of normal hours.

The application logs tend to record almost all the actions that take place whilst an application is being used. These tend include:

- All failed log-on attempts;
- All successful log-ins;
- All log-offs;
- All updates to a record;

- Each time a record is viewed.

Auditing

The types of auditable event mainly fall into two categories.

Firstly, there are events which need to be checked on a regular basis because they could indicate that someone is actively trying to breach the security of the system. An example of this is unauthorised log-on attempts or copying of the password file.

Secondly, when a breach of security is detected (or reported), the work which was being conducted on the system at that time in order to identify:

- How the breach of security occurred;
- Who was responsible for the breach;
- The amount of damage caused by the breach.

To support an investigation into a security incident, it is important to have a range of flexible reporting tools which allow the investigator to sort through the accounting information collected in a variety of different ways, and allows interconnections to be made between data derived from different sources.

Note: When considering what types of information which should be captured and what auditing should be implemented, it is important to ensure that the relevant IT Security Incident Management Plan is factored into the decision making process. This is to ensure that any protective monitoring solution supports the identification, alerting and investigation of security incidents. Further information can be found in the IT Security - Incident Management Plan and Process Guide.

Developing a protective monitoring schema

For the purposes of this guide, a protective monitoring schema sets out all the controls points which will be implemented in an ICT system.

Development stages

The business process for protective monitoring is captured in Figure 1 of CESG GPG No.13. This section covers the stages which should be followed when developing a protective monitoring schema:

- The key questions which must be applied which selecting protective monitoring control items;
- The minimum protective monitoring requirement;
- Selecting minimum control objectives;
- Setting the minimum audit requirement;
- Reporting and service validation.

Key questions

The following key questions cover items which should be thought about when selecting protective monitoring controls:

- What is being audited and monitored? In terms of:
  - Usage scenarios - what users are allowed to do and which actions need to be accounted for;
  - Exceptions and how they will be detected - what users are not allowed to do or what would constitute suspicious activity;
  - The complexity in terms of the different types of connectivity to support these interactions (e.g. air-gapped systems, electronic exchanges, remote access, wireless, Internet services, etc.).
- What information will be collected to support the accounting, audit and monitoring of these activities?
- How the information gathered will be used (including both a list of permitted purposes and a list of prohibited purposes)?
- Who will access the protective monitoring data and their associated responsibilities?
- How the information will be protected, stored, retained and disposed of?
- How notification of monitoring is achieved and how user consent is obtained, or otherwise?

Minimum protective monitoring requirement

The minimum level of protective monitoring which need to be implemented is set out in CESG GPG No.13; Table 1 below reproduces part of GPG13 which sets the baseline requirement to achieve a minimum level of protective monitoring.

Protective Monitoring Control	Objective
PMC1: Accurate time in logs.	To provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components.
PMC2: Recording relating to business traffic crossing a boundary.	To provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.
PMC3: Recording relating to suspicious activity at a boundary.	To provide reports, monitoring, recording and analysis of network traffic crossing a boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach an ICT system boundary or other deviation from normal business behaviour.
PMC4: Recording of workstation, server or device status.	To detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of Trojan software or so called "rootkits"). It will also record indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes).
PMC5: Recording relating to suspicious internal network activity.	To monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated the internal network.
PMC6: Recording relating to network connections.	To monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.
PMC7: Recording of session activity by user and workstation.	To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.
PMC8: Recording of data backup status.	To provide a means by which previous known working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised.
PMC9: Alerting critical events.	To allow critical classes of events to be notified in as close to real-time as is achievable.

Protective Monitoring Control	Objective
PMC10: Reporting on the status of the audit system.	To support means by which the integrity status of the collected accounting data can be verified.
PMC11: Production of sanitised and statistical management reports.	To provide management feedback on the performance of the Protective Monitoring system in regard of audit, detection and investigation of information security incidents.
PMC12: Providing a legal framework for Protective Monitoring activities.	To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.

Table 1 - Minimum audit requirements

Additional control objectives

Note: During the risk assessment process, additional control objectives may be identified for inclusion into the set derived from CESG GPG No.13. These additional control objectives must be recorded in the protective marking schema.

Minimum control objectives

The minimum control objectives that are to be applied are in the Protective monitoring schema template. These control objectives are provided as a template for the author of the protective marking schema to fill in, notes are provided and once completed can be used as part of the description of the protective monitoring solution presented to the system Accreditor in the RMADS.

Where a minimum control objective cannot be met (for example, due to an implementation restriction or where the risk does not justify the control) it must be recorded as an exception (a template is provided here).

Note: This is generic set of control objectives and the templates provided in section A.1 and A.2 are designed for the author of the protective marking schema to customising based on the guidance provided in this document, CESG GPG No.13, the ICT system and associated risk assessment.

Control objectives extensibility

It is important to ensure that there is a mechanism in place to review, update or extend the protective monitoring controls once an ICT system is in live operation. This will occur when an ICT system undergoes the re-accreditation process, further details of which can be found in the Accreditation Framework.

Minimum audit requirements

The minimum audit requirement is specified in CESG GPG No.13 where the following provides the audit criteria which **must be** captured in the protective monitoring schema (a template table is provided here):

- The retention period of any protective monitoring data captured;
- Details on when log checks are to be carried;
- Details on when the protective monitoring system is to be manned;
- Details on when the system is to be subject to compliance review;
- Details on the reporting structure (see Reporting Structure), which should be specified in terms of a weekly, monthly or annual report.

Baseline Control Set and implementation of controls objectives

Table 2 defines the minimum controls which **must be** implemented to achieve the baseline controls set out in HMG IA Standard Numbers 1 & 2 – Supplement: Technical Risk Assessment and Risk Treatment.

Control	Baseline Control	Notes
10.10.1 Audit logging	In accordance with SPF Departments must ensure that ICT systems are capable of producing records of user activity to support monitoring, incident response and investigations.	Routine user activity such as log-on and log-off, log-on failures, keyboard inactivity, password change, object permissions change, read/write access to objects, import/export, print, object save and deletion.
10.10.2 Monitoring system use	Departments must develop and implement procedures to monitor use of systems and services by users to support incident response and investigation activities.	Establish baseline activity within the environment and develop auditable events outside this baseline activity.
10.10.3 Protection of log information	Audit logs must be protected in accordance with their sensitivity or protective marking.	The BIL of log information captured must be documented in the ICT system's Business Impact Assesment (BIA).
10.10.4 Administrator and operator logs	ICT systems must be capable of generating audit logs for all system users including system administrators.	Log collection and storage.
10.10.5 Fault logging	Departments must log and review system faults at regular intervals.	System management activity.
10.10.6 Clock synchronisation	Departments must implement a reliable means to keep all server and device clocks of the ICT System in synchronisation.	Establish time server.
13.2.3 Collection of evidence	In accordance with Security Policy Framework MR 9 Departments must have 'a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system, that may be required for legal and management purposes'.	How is the integrity of the collected data assured? How is collected data stored to prevent unauthorised access?
15.3.1 Information system audit controls	Departments must implement plans and controls to ensure that audit and compliance checks do not adversely affect the business operation of an ICT system.	Minimum impact on services is required. Does this mean no degradation of service?
15.3.2 Protection of information system audit tools	System audit tools must be protected to prevent their use for unauthorised purposes.	Installed and controlled in a physically separate environment with protected network connectivity.

Table 2 - Baseline controls to achieve protective monitoring

With Table 2 in mind CESG GPG No.13 outlines a number of options which should be consider when translating the identified control objectives into a protective monitoring solution which can be implemented in an ICT system.

The following provides the typical list of components which can be put together to deliver a protective monitoring solution:

- Security Information and Event Management (SIEM) system, which includes:
  - Log collection;
  - Log analysers;
  - Filtering, query and pattern matching tools;
  - Reporting tools;
  - Computer forensic tools;
  - Network management system;
- Intrusion Detection and Prevention System (IDS/IPS);
- Network Intrusion Detection System (NIDS);
- Host Intrusion Detection System (HIDS);
- Wireless Intrusion Detection System (WIDS).

A template is provided here to capture all the accounting items to be collected and where those items are collected.

Reporting Structure

Protective monitoring is only effective if there is a clear and effective reporting structure is in place to ensure that any alerts generated by the protective monitoring solution are escalated to the relevant people.

Note: The protective monitoring solution must fit into the overall IT Security Incident Management plan; see IT Security - Incident Management Plan and Process Guide for further details.

Service Validation

Once the protective monitoring schema has been generated and approved by the system Accreditor, the next step in delivering an effective protective monitoring solution is ensuring that the service provided is working as planned and that it is effectively gathering the data. This part of the protective monitoring solution must be document and should contain the following:

- Details on the initial operational capability and the start date;
- A defined series of service review points, specifically identifying the review of the control sets and the validation of data gathered;
- A defined criteria for spurious or unnecessary data that should be identified during the validation period and removed from the log reporting/alerting mechanism;
- Details on the full operational capability and the start date. At the point the protective monitoring service is fully operational, no changes may be made to the service without the approval of the system Accreditor.

Protective monitoring schema template
Minimum control objective

This section of the template captures the implementation details and compliance evidence for each protective monitoring control (PMC) specified in CESG GPG No.13. A minimum control object for each PMC is entered and is intended to provide an initial starting position.

Minimum control objective for PMC 1

For PMC 1 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Accurate time in logs.	[Insert additional notes/test as required.]
Control Description	

Provide a means of providing accurate time in logs and synchronisation between system components to facilitate collation of events between those components. The error margin for time accuracy is to be specified.	[Use any of the following: Providing a master clock system component which is synchronised to an approved time source (e.g. GSi time source); Updating device clocks from the master clock using the Network Time Protocol (NTP); Record time in logs in a consistent format (Universal Co-ordinated Time (UTC) is recommended)]		
Objective			
Provide a centralised, single time reference for all components that are subject to monitoring.	Any of the above may be used and an existing clock source within the support environment should be used where possible.		
Risk Level			
VERY LOW/LOW/ MEDIUM	[Insert Risk level]		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 2

For PMC 2 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Recording of business traffic crossing a boundary.	[Insert additional notes/test as required.]
Control Description	
Provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.	[Insert additional notes/test as required.]
Objective	

Ensure only authorised traffic is passed into and out of the PM environment.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	Insert Risk level		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 3

For PMC 3 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording relating to suspicious activity at the boundary.	[Insert additional notes/test as required.]		
Control Description			
Provide reports, monitoring, recording and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour.	[Insert additional notes/test as required.]		
Objective			
Identify potential or actual attempts to access the ICT System environment by an unauthorised individual who is external to the environment	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*[Insert Risk level]*		
Service Description	Report	Alert	Proposed control/ implementation

[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 4

For PMC 4 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording on internal workstation, server or device status.	[Insert additional notes/test as required.]		
Control Description			
Detect changes to device status and configuration.	[Insert additional notes/test as required.]		
Objective			
Identify and report authorised and unauthorised changes to the configuration of devices in the environment.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 5

For PMC 5 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Recording relating to suspicious internal network activity.	[Insert additional notes/test as required.]
Control Description	

Monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated to the internal network.	[Insert additional notes/test as required.]		
Objective			
Identify internal and external attacks on the environment network.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 6

For PMC 6 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording relating to network connections.	[Insert additional notes/test as required.]		
Control Description			
Monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.	[Insert additional notes/test as required.]		
Objective			
Identify, monitor and audit temporary connections to the environment.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation

[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 7

For PMC 7 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording on session activity by user and workstation.	[Insert additional notes/test as required.]		
Control Description			
Monitor user activity and access to ensure they can be made accountable for their actions.	[Insert additional notes/test as required.]		
Objective			
Detect unauthorised activity and access that is either suspicious or is in violation of security policy.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 8

For PMC 8 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Recording on data backup status.	[Insert additional notes/test as required.]		
Control Description			
Provide for a previously known working state of information assets to be identified and recovered.	[Insert additional notes/test as required.]		
Objective			

Implement and audit backup and recovery procedures.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 9

For PMC 9 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Reporting on the status of the audit system.	[Insert additional notes/test as required.]		
Control Description			
Event reporting.	[Insert additional notes/test as required.]		
Objective			
Provide a mechanism for reporting in near real-time.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 10

For PMC 10 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	
Alerting critical events.	[Insert additional notes/test as required.]
Control Description	
Maintain status of the protective monitoring system and its collected accounting data.	[Insert additional notes/test as required.]

Objective			
Ensure the integrity and proper management of the protective monitoring system.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 11

For PMC 11 the following is to be implemented:

Detail	Notes/Statement of Compliance		
Control			
Alerting critical events.	[Insert additional notes/test as required.]		
Control Description			
Maintain status of the protective monitoring system and its collected accounting data.	[Insert additional notes/test as required.]		
Objective			
Ensure the integrity and proper management of the protective monitoring system.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Minimum control objective for PMC 12

For PMC 12 the following is to be implemented:

Detail	Notes/Statement of Compliance
Control	

Providing a legal framework for Protective Monitoring activities.	[Insert additional notes/test as required.]		
Control Description			
Ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.	[Insert additional notes/test as required.]		
Objective			
Maintain legal and statutory obligations.	[Insert additional notes/test as required.]		
Risk Level			
VERY LOW/LOW/ MEDIUM	*Insert Risk level*		
Service Description	Report	Alert	Proposed control/ implementation
[Insert controls to be applied and any additional controls identified as part of analysis.]	[Insert R to denote report]	[Insert A to denote alert]	[Insert additional notes/test as required.]

Exceptions

The exceptions to the minimum baseline requirements must be recorded, a template table is provided below.

Serial	Protective Monitoring Control	Control Detail	Reason for non-compliance
[Insert details of those controls that will not be implemented as a result of reviewing the protective monitoring controls for each of the defined levels to show which controls either cannot be implemented for technical reasons, or as a result of a risk management decision. Delete this row on completion of table.]			

Audit regime

The audit regime which forms part of the protective marking solution must be recorded; a template table is provided below:

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

Accounting items

The table below provides a template to capture all the accounting items to be collected in an ICT system, its source and alerting details.

PMC	#	Cat	Ref	Recorded events	Include in report	Alert on event	Method	Notes in Environment PM policy	Accounting items (defined in GPG13)	Sources and notes	Logging application requirement	Tags	Predicate	Specific Events: Audit	Specific Events: Errors & Warnings	Specific Events: Protocol errors

Contact details

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

Security Log Collection

Security Log Collection

Ministry of Justice (MoJ) systems and services must adequately create and retain event data as part of the DETECT portion of the Cabinet Office's Minimum Cyber Security Standard (MCSS).

Related information

Logging and monitoring on page 54

MoJ Cyber Security Logging Platform

The MoJ Cyber Security team operate a centralised, scalable, multi-tenant, cloud-based log collection and forwarding system for infrastructure (non-application level) log data.

The platform can receive, store, index, filter, search, alert and re-forward log data from any MoJ source (including supplier systems).

Additive technology supply chain

The security log collection principles are designed to be met through technology supply chain as opposed to each system individually.

For example, where the principles require the logging of DNS traffic, this could be achieved within a corporate device ecosystem by logging at the end user device itself, or by configuring the end user device to use a corporate DNS server that logs instead. You may decide to do both, because some DNS queries can go out without the DNS server (for example in the case of a corporate VPN that is not always on).

Where a platform exists, it should provide some assurance to all its consumers that makes clear what logging it collects and what needs to be logged by its tenants.

For example, if a cloud platform allows you to spin up arbitrary virtual machines, but guarantees that all network traffic must pass via a web proxy to go out, which logs, then the cloud platform can tell you that Principle 5: Network Events and Principle 3: Infrastructure Events are logged, but that you need to provide Principle 1. Authentication Events. The platform may even provide you with a base virtual machine which have logging for authentication events built in, meaning that you don't need to provide any logging at that level.

Principles

We have created a series of security log collection principle requirements for the MoJ. If you have any questions or comments, get in touch: security@justice.gov.uk.

To enable ease of referencing, but not to imply priority order, each item is assigned a reference.

1. Authentication events

- a: login successes and failures

- b: multi-factor authentication success and failures
- c: logouts
- d: session creation
- e: session timeout/expiry
- f: session close

2. Authorisation events

- a: group/role creation, modification or deletion
- b: group/role membership changes (addition or subtraction)
- c: group/role elevation (for example, if a user is able to temporarily assume a higher privilege to conduct a finite amount of work)

3. Infrastructure events

Infrastructure is defined as underlying resources, whether a logical switch, server or through to a containerised compute resource in the cloud, upon which end-user or application logic is overlaid.

- a: power/service on / off
- b: creation/registration and deletion/de-registration, including suspension/hibernation if applicable
- c: software update events/status
- e: IP address allocation/deallocation
- f: Firewall/routing rule creation, modification or deletion
- g: Network change events (for example addition or removal of virtual networks or interfaces)

4. Domain name service queries

- a: successful and unsuccessful queries
- b: recursive lookup status
- c: infrastructure node / end-user device registration / de-registration (if applicable)

5. Network traffic events

- a: successful and unsuccessful inbound service daemon connections
- b: unsuccessful outbound connections where the network traffic is *not* associated to an inbound request

6. Contextual security related events

In context and where present, technology may generate events pertinent to security and these must be captured.

For example, operating system patch state information from end-point protection detections through to encryption states within storage arrays.

7. Log transmission to the MoJ Cyber Security Logging Platform

- a: All log data must be sent to the MoJ Cyber Security owned log platform unless all principles have already been met through the deployment of a holistic locally deployed and monitored Security Information and Event Management (SIEM) solution.

Where 7(a) above is true, the MoJ Cyber Security team will advise in context what information must be sent from the in-place SIEM to the MoJ Cyber Security Logging Platform.

Enterprise IT - Infrastructure

We have developed a series of logging requirements for Enterprise IT infrastructure, such as underlying networks, network services and directory services at different maturity tiers in order to support defensive cyber security, such as detecting breaches.

Baseline Maturity Tier

1. User directory services

Log Collection Principle(s): 1, 2

User directory services (such as Active Directory (AD), Azure Active Directory or OpenLDAP must create and forward Authentication and Authorisation events from the directory service itself. (Normal authentication and authorisation events for the underlying operating system and server should be forwarded as appropriate.)

For example:

- An administrator logging onto the AD server using the local end-user device's administrator account should result in an authentication event for the machine being sent.
- A directory admin logging on to the AD service from their end-user device without logging into the local machine should generate an authentication event for the directory.

These event types must be logged and forward:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (changes to ACL's, granting of new roles in RBAC models)
10. Privilege escalation events (use of sudo, UAC)
11. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Productivity Suite security logs

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

Productivity suites (such as Google Workspace or Microsoft Office 365) must create and forward all security-related log data (as defined by the vendor), including unsuccessful Authentication and Authorisation events.

For example, within an Office 365 tenancy with Conditional Access enabled and set to require multi-factor authentication when a user device is perceived to be outside of the corporate network and such prompt is made and the outcome of that challenge.

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded.

1. Client IP address
2. Query
3. Query response content including:
    a. Returned record(s) or NXDOMAIN
    b. Authoritative nameserver
4. Query response code
5. Zone and/or view identifier (if local zone response and/or multiview)

This remains true for where nodes (for example, servers) may bypass internal DNS services.

4. Web proxy access logs

Log Collection Principle(s): 5

Where web traffic proxies exist, access logs must be created and forward and must, include the following variables:

1. Authenticated user name
2. Client IP address
3. HTTP method (for example, `CONNECT GET`)
4. Full destination/target URL
5. Connection return status code (for example, 200 or 403)
6. Size of response

5. File server authentication, authorisation and access logs

Log Collection Principle(s): 6

Where file service exist, sufficient log data must be created and forwarded, including sufficient data to satisfy the following:

1. Detect permission changes and the user who changed such
2. Detect all file/folder changes and the user who changed such
3. Detect all file/folder read/open and the user who did such

6. Security-related event logs for all server operating systems

Log Collection Principle(s): 6

Security-related event logs from all servers (whether virtualised or physical) operating in a 'server' role:

- [additional information pending]

7. Allocation of IP address leases from DHCP services

Log Collection Principle(s): 3, 5

DHCP services must be configured to create and forward the following:

1. Successful client DHCP requests, including:
    a. Requesting client MAC address
    b. DHCP scope identifier
    c. IP address leased
    d. IP address lease duration
2. Unsuccessful client DHCP requests, including:
    a. Requesting client MAC address
    b. DHCP scope identifier (if applicable for unsuccessful request)

8. VPN concentrator activity data

Log Collection Principle(s): 3, 5

Where a end-user device VPN concentrator is in use, connection-related log data must be created and forwarded:

1. Success or unsuccess status
2. User/certificate identifier
3. Client IP address
4. Concentrator identifier

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded:

1. Client IP address
2. Firewall/router identifier
3. Request response code

4. Request content, including:
    a. IP protocol (for example, ICMP)
    b. Destination/target port
    c. Destination/target IP address
    d. Destination/target hostname address (if reverse lookup performed)

2. Internal DNS namespace zone content

Log Collection Principle(s): 4

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

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

Log Collection Principle(s): 5

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

4. Endpoint protection security logs

Log Collection Principle(s): 6

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

5. Mobile device enrollment activity

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

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

1. Enrolment or un-enrolment event type
2. End-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
3. End-user account name (if applicable)

Enterprise IT - Mobile Devices

We have developed a series of logging requirements for Mobile Devices (also known as End-user Devices), such as thin-clients, desktops, laptops, tablets and mobile smart phones at different maturity tiers in order to support defenisve cyber security, such as detecting breaches.

Baseline Maturity Tier

1. Device power events

Log Collection Principle(s): 1

Devices must create and forward local power events.

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

2. User identification activity

Log Collection Principle(s): 1, 2

Devices must create and forward local Authentication and Authorisation events.

These event types must be logged and forward:

- a: account creation
- b: account lockout
- c: account unlock
- d: account authentication failures

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

3. Domain name service query logs

Log Collection Principle(s): 4

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

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

4. Security-related operating system event data

Log Collection Principle(s): 6

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

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

5. Security-related software event logs

Log Collection Principle(s): 6

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

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

6. Network information

Log Collection Principle(s): 5

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

- a: IP address of DHCP server
- b: IP address leased
- c: IP address subnet leased
- d: IP address lease duration

- e: Network interface identifier
- f: DHCP response instructions, for example:
  - 1: DNS servers
  - 2: Proxy servers

7. VPN dial-up activity

Log Collection Principle(s): 5

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

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

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded.

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

2. Command/executable runtime information

Log Collection Principle(s): 6

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

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

3. Configuration information

Log Collection Principle(s): 6

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

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

Hosting Platforms

We have developed a series of logging requirements for hosting platforms, such as virtualised and/or containered compute with associated supporting services such as database and queuing services at different maturity tiers in order to support defenisve cyber security, such as detecting breaches.

Baseline Maturity Tier

1. User directory services

Log Collection Principle(s): 1, 2

User directory services must create and forward Authentication and Authorisation events from the directory service itself.

User directories within hosting environments can be rich and diverse, such technologies include:

- Active Directory (AD)
- Azure Active Directory
- OpenLDAP
- Amazon Web Services (Accounts and Incognito)
- Okta
- Auth0
- Github.com (acting as an identity provider)
- Google Workspace (acting as an identity provider)
- Local user stores within operating systems

These event types must be logged and forwarded:

1. Account creation
2. Account lockout
3. Account reinstatement
4. Account authentication failures
5. Account authentication successes after 1 or more failures
6. Account password changes
7. Group membership addition / deletion (in particular, any group that gives admin access)
8. Group creation
9. Privilege modification for users (for example, role delegation through AWS IAM)
10. Multi-factor authentication state, such as:
    a. Enabled
    b. Disabled
    c. Reset/rotation
    d. Recovery method used

2. Bastion/Jump/Action-proxy services

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

Bastion/jump boxes that act as a management consolidation route and should be highly auditable therefore must create and forward security-related event data:

1. SSH keypair generation/revocation, including:
    a. Public key
    b. Keypair 'friendly name' / identifier
2. Account login attempts:
    a. Public key
    b. Username

3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded:

1. Client IP address
2. Query
3. Query response content including:
    a. Returned record(s) or NXDOMAIN
    b. Authoritative nameserver

4. Query response code
5. Zone and/or view identifier (if local zone response and/or multiview)

This remains true for where nodes (for example, servers) may bypass internal DNS services.

4. Web proxy access logs

Log Collection Principle(s): 5

Where web traffic proxies exist, access logs should be created and forward and must, include the following variables:

1. Authenticated user name (if applicable)
2. Client identifiers:
    a. IP address
    b. Reverse lookup client name (if applicable)
3. HTTP method (for example, CONNECT GET)
4. Where available, full destination/target URL or SNI value
5. Connection return status code (for example, 200 or 403)
6. Size of response

5. Hypervisor events

Log Collection Principle(s): 3, 6

Hypervisors manage virtualised compute resources and are entrusted to segregate the same. All instructions to hypervisors should be highly auditable.

1. Virtual machine creation (including templates)
    a. Identifier(s)
    b. Operating system image information
2. Virtual machine 'power' events:
    a. Identifier(s)
    b. 'Power' on
    c. 'Power' off (including restart flag)
3. Virtual machine deletion
    - Identifier(s)
4. Virtual machine resource modification events:
    a. CPU addition/removal
    b. RAM addition/removal
    c. Networking additional/removal
    d. Storage mount/dismount/resize

6. Orchestrator events

Log Collection Principle(s): 3, 6

Orchestrators such as Cloud Foundry and Kubernetes create and manage a variety of technology resources to facilitate an application environment.

1. Resource creation (including templates)
    a. Identifier(s)
    b. Resource type
    c. Operating system image information (if applicable)

2. Container 'power' events
    a. Identifier(s)
    b. 'Power' on
    c. 'Power' off (including restart flag)
3. Resource deletion
    - Identifier(s)
4. Resource modification events:
    - Identifier(s)

7. Allocation of IP address leases from DHCP services

Log Collection Principle(s): 3, 5

DHCP services must be configured to create and forward the following:

1. Successful client DHCP requests, including:
    a. Requesting client MAC address
    b. DHCP scope identifier
    c. IP address leased
    d. IP address lease duration
2. Unsuccessful client DHCP requests, including:
    a. Requesting client MAC address
    b. DHCP scope identifier (if applicable for unsuccessful request)

Enhanced Maturity Tier

1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall `DENY` log data must be forwarded.

1. Client IP address
2. Firewall/router identifier
3. Request response code
4. Request content, including:
    a. IP protocol (for example, ICMP)
    b. Destination/target port
    c. Destination/target IP address
    d. Destination/target hostname address (if reverse lookup performed)

2. Internal DNS namespace zone content

Log Collection Principle(s): 4

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

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

Log Collection Principle(s): 5

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

4. Endpoint protection security logs

Log Collection Principle(s): 6

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

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

Log Collection Principle(s): 6

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

6. Mobile device enrollment activity

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

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

1. Enrolment or un-enrolment event type
2. End-user device identifier(s), such as client IP address and/or MAC address and/or assigned DHCP name
3. End-user account name (if applicable)

7. VPN concentrator activity data

Log Collection Principle(s): 3, 5

Where VPN services are in use, connection-related log data must be created and forwarded.

1. Success or unsuccess status
2. User/certificate identifier
3. Client IP address
4. Concentrator identifier

8. Pipeline events

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

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

1. Source identifier(s)
    a. User(s)
    b. Repository
2. Activity events
    a. Resource creation
    b. Resource destruction

Log entry metadata

Any security log data collected must comply with these metadata standards to ensure we are able to consistently interpret log data using other systems.

Time/date

- a: all log events must be time stamped in the common log timestamping format as defined by ISO8601 `[dd/MM/yyyy:hh:mm:ss +-hhmm]` where the fields are defined as follows:
    - 1: dd is the day of the month
    - 2: MMM is the month
    - 3: yyyy is the year
    - 4: :hh is the hour
    - 5: :mm is the minute
    - 6: :ss is the seconds
    - 7: +-hhmm is the time zone

- b: systems must use an automated time syncing protocol (such as NTP) with an external time source to ensure it is not subject to 'time drift' that may impact the accuracy of time stamping.

Formats

Only the following log file formats should be used:

- a: Apache Common Log Format
- b: NCSA (Common or Access, Combined, and Separate or 3-Log)
- c: Windows Event Log
- d: W3C Extended Log File Format
- e: W3C Extended (used by Microsoft IIS 4.0 and 5.0)
- f: SunTM ONE Web Server (iPlanet)
- g: IBM Tivoli Access Manager WebSEAL
- h: WebSphere Application Server Logs

Security Log Collection Maturity Tiers

Ministry of Justice (MoJ) systems and services must adequately create and retain event data as part of the DETECT portion of the Cabinet Office's Minimum Cyber Security Standard (MCSS).

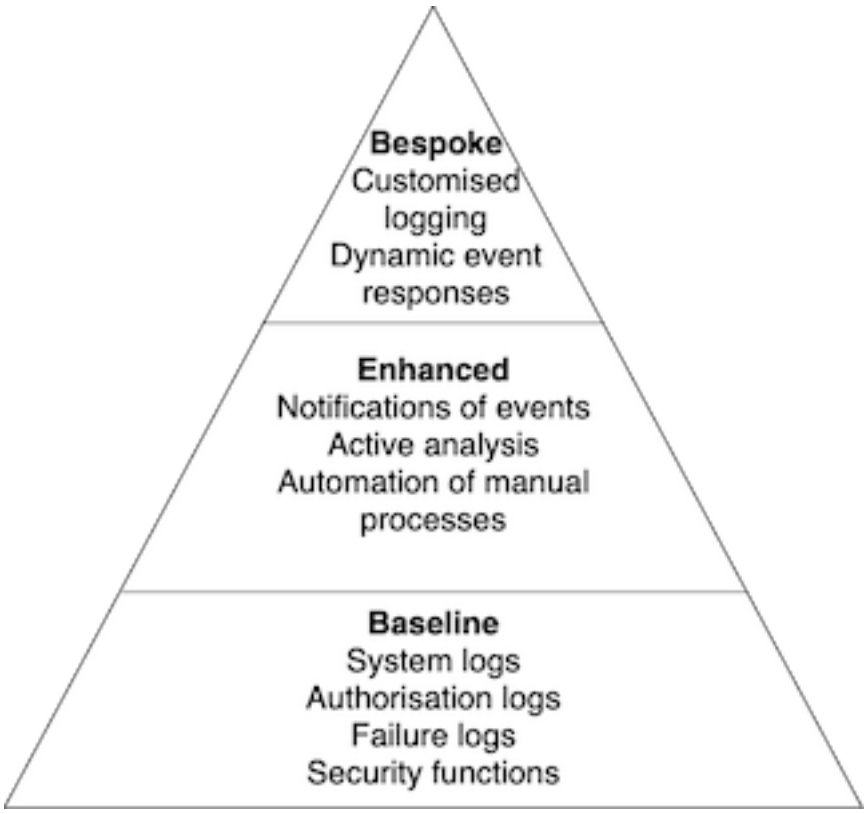
Three tiers have been developed to reflect the breadth and complexity of collecting and forwarding log data.

These three tiers represent different levels of risk profile, and concern about a system. All systems should be capable of meeting the baseline standard.

Some systems are at greater likelihood of compromise. This is due to factors such as age or public threats. Other systems would have a higher impact if compromised. This is due to the systems being sensitive or having distinctive perceived value. Such systems should be monitored to a higher standard.

The extent to which a security log collection process implements the monitoring requirement indicates the logging maturity.

Each level of monitoring - or 'tier' - has characteristics that are 'in addition' to lower level tiers. For example, a system operating at the Enhanced tier should also meet the requirements of the Baseline tier.



Baseline

The baseline tier is the generally minimum expected for event types. It includes data that should be generated, recorded, and forwarded for onward analysis. It applies to all of the MoJ systems. In most cases, this requirement may be met through the underlying platform(s) on which the systems are built.

This tier covers the broad spectrum of events that can reasonably be used to detect compromise. It allows the defensive cyber team to respond appropriately before significant impact.

Enhanced

The enhanced tier, in conjunction with the baseline event types, provides earlier notification of attempted compromise. It enables gathering of more information to detect stealthier or more capable attackers.

Bespoke

The bespoke tier concerns systems that are critical to the security, stability and statutory function of the MoJ, or that contain highly sensitive data. In this tier, systems must generate additional bespoke (customised) event types. These event types are typically agreed in context between the MoJ Cyber Security team and the associated product or service team. The objective is produce logging that reliably identifies and captures key nuance and contextual security monitoring data, based on applicable threats and risks.

Contact details

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

System acquisition, development and maintenance

Security requirements of information systems

Technical Security Controls Guide

Introduction

This guide explains the technical security controls that should be implemented on information systems developed, procured or operated by the Ministry of Justice (MoJ) or on its behalf. This guide aligns with NIST 800-53 and the NCSC Cyber Assessment Framework (CAF). The guidance provides the MoJ with 3 phases or layers of defence. These controls must be implemented to ensure the MoJ's network infrastructure is secure.

Who is this guide for?

This guide has two audiences:

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

What is an MoJ 'system'?

Within this guide, a system includes:

- Hardware - laptops, desktop PCs, servers, mobile devices, network devices, and any other IT equipment.
- Software - such as operating system (OS) and applications (both web-based and locally installed).
- Services - such as remote databases or cloud-based tools like Slack.

Related guides

Defensive Layer 1: Creating a baseline security environment Layer 1 sets out the technical controls required to build strong network foundations, including secure configuration and software development.

Defensive Layer 2: Implementing monitoring capabilities Layer 2 builds a monitoring capability for the network and extends existing security controls to mobile devices.

Technical Security Controls Guide: Defensive Layer 1
Defensive layer 1: Creating a baseline security environment

DO

The following security controls should be implemented to create a baseline security environment.

✓ Enforce access control through using Multi-Factor Authentication (MFA), security attributes and enforcing the 'need to know' principle. Dual authorisation must also be used to conduct sensitive system changes. For more information, see the Access Control guide.

✓ Implement host-based protection such as host firewalls and host based intrusion detection.

✓ Restrict the use of remote access connections, using the following controls:

- The monitoring and control of remote access methods.
- Ensuring all remote access methods are encrypted.
- Enabling the capability to rapidly disconnect a user from accessing an information system, and/or revoking further remote access.

✓ Implement the following access control and security measures to protect Ministry of Justice (MoJ) wired and wireless networks:

- Restrict a user's ability to change wired and wireless configurations.
- Use strong encryption and authentication on both wired and wireless networks.
- Carry out regular audits of routers and wireless access points looking for unauthorised units.

✓ Synchronise timestamps with a primary and secondary authoritative time sources.

✓ Classify system connections, and apply restrictions to external systems and public networks.

✓ Test backup solutions at least every three months, to ensure data reliability and integrity.

✓ Use deny-listing/allow-listing tools for current and newly developed software.

✓ Enforce session lock controls with pattern-hiding displays.

✓ Use encryption to protect information. Encryption mechanisms should include:

- Secure key management and storage.
- PKI certificates and hardware tokens.

✓ Ensure that system component inventories:

- Are updated as part of installation or removal tasks.
- Have automated location tracking where possible.
- Have clear and unambiguous assignment of components to systems.
- Do not have component duplication.

✓ To protect the network against malicious actors and code, implement the following security controls:

- Vulnerability scanning tools.
- Intrusion detection systems.
- Signature and non-signature based detection of malicious code or behaviour.
- Software patching and updates.
- Detection of unauthorised commands.
- Tools for real-time analysis of logs.
- Detection of indicators of compromise.

✓ When connecting to external networks and systems, ensure those network and systems provide secure connection, processing, storage, service controls and physical locations.

✓ Make provision for exceptional (excess) capacity or bandwidth demands, above what is required for 'typical' business as usual operations, and implement monitoring and detection tools for denial of service attempts.

✓ Where possible, ensure a redundant secondary system or other resilience controls are in place, using alternative security mechanisms and communication protocols.

DO NOT

The following list identifies what should not be done, and what activities should be limited, to improve baseline security controls.

✖ Allow systems to release information from secure environments unless all the following security controls are implemented on the destination system:

- Boundary security filters.
- Domain authentication.
- Logical separation of information flows.
- Security attribute binding.
- Detection of unsanctioned information.
- Restriction of suspicious inbound and outbound traffic.

✖ Allow general users to make unauthorised configuration changes to the security settings of software, firmware or hardware. Any exceptions, such as software updates, must be risk assessed and approved by IT and the Risk Advisory Team.

✖ Allow users to install software. Instead, software installations should be approved first, and only users with privileged access should be permitted to conduct the installation.

✖ Allow split tunnelling without careful consideration of how traffic will remain protected.

✖ Allow inbound traffic from unauthenticated or unauthorised networks.

✖ Allow discovery of system components or devices on the network.

✖ Enable boundary protection settings that permit different security domains to connect through the same subnet.

Defensive layer 1: Creating a baseline security software development and system configuration

DO

The following list describes what should be in place to create secure software development and configuration environments within the MoJ.

✓ If you are developing or maintaining systems or applications, use a development lifecycle and associated tooling which enforces security by design. Examples include:

- Code analysis and testing.
- Mapping integrity for version control.
- Trust distribution.
- Software, firmware, and hardware integrity verification.

✓ Use baseline configuration templates for critical and non-critical assets. These need to include:

- Automation support for accuracy and currency, such as hardware and software inventory tools and network management tools.
- Retention of previous configurations.
- Separate development and test environments.
- Cryptography management.
- Unauthorised change detection

✓ Enforce binary or machine executable code are provided under warranty or with source code, and implement time limits for process execution.

✓ Verify the boot process, and ensure the protection of boot hardware.

✓ Implement low module coupling for software engineering.

✓ Enforce application partitioning.

✓ Take a 'deny by default' approach to boundary protection for both outbound as well as inbound. Example controls include:

- Automated enforcement of protocol formats.
- Separate subnets for connecting to different security domains.

✓ Enforce protocol formats.

DO NOT

The following list outlines the actions that should not be undertaken in relation to software development and secure configuration.

✖ Allow access privileges for library or production/operation environments for unauthorised users.

✖ Configuration changes or applications to go live without testing them in a non-live environment.

✖ Use live data, including personal data, in system or application testing. Exceptions must be approved by the relevant SIRO and, if the live data contains personal data, the Data Protection Officer.

✖ Install or execute off-the-shelf software without ensuring appropriate support and security arrangements and agreements are in place.

Technical Security Controls Guide: Defensive Layer 2
Defensive layer 2: Implementing monitoring capabilities

DO

The following list identifies the security controls that should be implemented to mature existing Layer 1 controls and enable active monitoring of the Ministry of Justice (MoJ) network.

✓ Monitor login attempts and block access after 10 unsuccessful attempts.

✓ Implement session timeouts and block accounts after a defined period of inactivity, for example, 5 minutes.

✓ Implement a mobile device management solution to enable the wiping of mobile devices where access to the device has been lost or unauthorised access identified, for example, in the event of:

- An identified data breach.
- An identified policy breach such as jailbreaking a device.
- A lost device.
- The end of an employment contract, for example, for an employee or contractor.

✓ Use tools such as Elastic for easy storage, search and retrieval of information from logs, such as security, system or application logs collected from end points. Where artificial intelligence tools for searching these logs are available implement their use, an example might be AWS' Macie.

✓ Terminate network connections associated with communication sessions. For example the de-allocation of:

- Associated TCP/IP address pairs at the operating system level.
- Network assignments at the application level if multiple application sessions are using a single, operating system level network connection.

✓ Implement maintenance tools. For example:

- Hardware/software diagnostic test equipment.
- Hardware/software packet sniffers.
- Software tools to discover improper or unauthorised tool modification.

✓ Use monitoring systems to generate alerts and discuss options with the Operational Security Team (OST).

✓ Have the capability to respond to alerts generated by the monitoring system or by users and discuss options with OST.

✓ Control the development and use of mobile code, whether developed in-house, third party or obtained through acquisitions, by following a formalised development and onboarding process, see the Data Security & Privacy Lifecycle guide.

✓ Implement concurrent session control which is defined by:

- Account type, for example privileged and non-privileged users, domains, or applications.
- Account role, for example system admins, or critical domains or applications.
- A combination of both the above.

✓ Implement spam protection tools, which have the capability to:

- Monitor system entry and exit points such as mail servers, web servers, proxy servers, workstations and mobile devices.
- Incorporate signature-based detection.
- Implement filters for continuous learning.

✓ Use error handling techniques, such as pop-up messages, which provide information necessary for corrective actions without revealing data that can be exploited by threat actors.

DO NOT

The following list describes what actions should **not** be undertaken when implementing Layer 2 security controls.

✖ Allow connections between internal and external systems without carrying out security checks.

✖ Allow the use of unauthorised software. Software must be approved by the MoJ. Contact the Cyber Assistance Team (CAT) for advice at CyberConsultancy@digital.justice.gov.uk.

✖ Allow general users to execute code on their mobile devices. Your devices should be able to:

- Identify malicious code.
- Prevent downloading and execution.
- Prevent automatic execution.
- Allow execution only in secured and segregated environments.

✖ Display internal error messages such as stack traces, database dumps, and error codes to users outside of the MoJ-defined personnel and roles.

✖ Allow unauthorised removal of maintenance equipment, for example, backup disks and power supplies.

✖ Decommission maintenance equipment without appropriate security controls, for example:

- Verifying that there is no organisational information contained on the equipment.
- Sanitising the equipment.
- Retaining the equipment within the facility.

Security in development and support processes

Maintained by Default

We believe that technology should be Maintained by Default, particularly in relation to security.

h/t https://www.ncsc.gov.uk/articles/secure-default

Good technical maintenance is security maintenance

Technical maintaince isn't just about patching or upgrades (but they often play a large and important part of maintenance) but more of refreshing designs, methods and approaches to leverage new technologies to increase quality, speed and performance and reducing costs.

Good technical maintenance (including patching and upgrades) includes security benefits whether that is patching a known security issue through to implementating newer cryptography methods that both benefit security but also reduce computational effort or enhance user privacy.

Good technical maintenance (just like other release or change paths) should include an appropriate amount of testing (outside of production) to understand any negative consequences of changes.

Commodity technical maintenance

The Ministry of Justice (MoJ) expect technology systems to be maintained to ensure the commodity functional elements do not become end of life, or cease function as a result.

Examples include:

- [automated] certificate renewals
- upgrading of hashing methods to implement new standards once they become commoly accepted best practices
- upgrading from SSLv3 to TLS, and from TLS1.[0/1] to TLS1.2, ultimately into TLS1.3 (and beyond)

Secure by Default

We believe that technology should be Secure by Default. This means embedding security from inception, so that it is intrinsic and as transparent as possible.

h/t https://www.ncsc.gov.uk/articles/secure-default

Good technical design is security design

Secure by Default takes a holistic approach to solving security problems. Security is treated as a core fundamental rather than a followup activity.

Embedding security within a design is directly comparable to good modern technical designs and fundementally ensuring the 'thing' actually works.

Secure by Default

The National Cyber Security Centre (NCSC) describe the Secure by Default principles as:

- security should be built into products from the beginning, it can't be added in later;
- security should be added to treat the root cause of a problem, not its symptoms;
- security is never a goal in and of itself, it is a process - and it must continue throughout the lifetime of the product;
- security should never compromise usability - products need to be secure enough, then maximise usability;
- security should not require extensive configuration to work, and should just work reliably where implemented;
- security should constantly evolve to meet and defeat the latest threats - new security features should take longer to defeat than they take to build;
- security through obscurity should be avoided;
- security should not require specific technical understanding or non-obvious behaviour from the user.

Context is important

The principles above can generally be applied in most scenarios however interpretation and applicability in context can vary - the Ministry of Justice (MoJ) Cybersecurity team are here to help and advise.

NCSC also have a set of whitepapers which help explain some approaches to building products which align with these principles (and they add to them over time):

- Building a secure feature-rich computing platform, such as a smartphone.
- Storing sensitive data on consumer platforms

Source code publishing

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ). In particular, it applies to product owners, technical architects, security architects, and developers.

MoJ policy about making source code developed by the MoJ available complies with UK Government guidance.

By default, MoJ developers **MUST** develop source code in a way that means it can be stored and published in the open. There are exceptions, for example sensitive material such as encryption keys.

This document is not about the use of existing open source materials.

Reasons for working in the open and sharing source code by default

Point 8 of the “Digital by Default” Service Standard states that you should:

> Make all new source code open and reusable, and publish it under appropriate licences (or provide a convincing explanation as to why this cannot be done for specific subsets of the source code).

This includes “Making source code open and reusable”.

When you should not publish materials in the open

There are some circumstances when materials should not be public.

Obvious examples include security or encryption keys or credentials, and configuration details. Other examples include:

- Algorithms used to detect fraud.
- Materials that relate to unreleased policy.
- API keys for cloud-hosted applications or environments, for example AWS.

An important exception is for materials developed by third parties. They might have retained ownership of the Intellectual Property (IP).

More guidance to help you decide when to publish materials in the open or not is available here.

Contact details

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

System Test Standard

Legacy information

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

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

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

About this document

This document is the Ministry of Justice (MoJ) System Test Standard. It is designed to help protect MoJ IT systems by providing a common standard for system security testing.

How to use this document

The purpose of this standard is to provide a process around the security testing of MoJ IT systems and outline what security issues should be considered at each stage of the process.

Note: This document focuses on the security aspects of system testing. It is not intended to provide comprehensive information on general system testing.

Overview
Introduction

The purpose of system testing is to ensure all the functional and non-functional requirements of the system are verified to be operating within specified bounds.

HMG Security Policy Framework mandatory requirements 9 states that:

> Departments and Agencies must put in place an appropriate range of technical controls for all IT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

Policy statements on system testing are covered in the IT Security Technical Users Policy. This document sets out the MoJ standard for system test implementation from a security perspective.

Scope

This standard is concerned with the security testing of all MoJ IT systems including IT systems hosted by third party suppliers on behalf of the MoJ.

Definitions

For the purposes of this standard, the following definitions apply:

System testing	Tests conducted against an application or IT system to ascertain whether that application or IT system has implemented the desired functional and non-functional requirements.
Security testing	The subset of system tests which concentrate on testing an application's or IT system's functional and non-functional security requirements.

Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. System testing is captured as a basic requirement in Level 1, which the MoJ will need to demonstrate compliance with in the MoJ IAMM return to Cabinet Office.

Testing approach

This standard outlines at a high level the security testing which must be applied to all MoJ IT systems to ensure that security vulnerabilities are identified and risk managed appropriately. The aim is for this standard to feed into the overall test requirements and test plan for an IT system.

System testing, in particular system security testing, must be performed in support of the system assurance process to provide confidence that:

- The implementation delivers the agreed security controls.
- There are no unacceptable security vulnerabilities within the delivered solution.

The following three principles must be applied when putting together a test plan for an IT system:

1. The rigour of the tests must be commensurate with the impact of a security failure.
2. The tests may need to be repeated to provide assurance that subsequent changes to the system or service have not introduced new vulnerabilities.
3. The testing services (automated or otherwise) used must generate security compliance/assurance evidence against known threats and current IT security policies. For example, penetration testing (or ITHC), ad-hoc scanning, secure code review, and software configuration assurance.

Note: It is MoJ policy that system testing **MUST NOT** be conducted in a live environment. System testing should combine tests conducted in a non-live system test environment with tests conducted in a live environment (e.g. an IT Health Check).

The rest of this document is split into four sections:

1. Guidelines: Sets out the basic security requirements for IT system testing and provides guidance on system test data.
2. Risk assessment and management: Outlines the link between system assurance and security testing.
3. Types of security tests: Provides an overview of the common types of security testing.
4. Pre-live security testing: Outlines how security testing links in with the standard set of testing activities which are conducted during the development and deployment phases of an IT system.

Guidelines

HMG IS 1 and 2 require that assurance evidence is provided covering an IT system's business systems design, implementation, and operation.

Security testing of an IT system to obtain the assurance evidence required can occur at various points throughout the system development and deployment lifecycle (see Table 1). For example:

Commercial off the Shelf (COTS) product assurance	Test assurance obtained through the use of a security evaluated, either by CESG or via the Common Criteria scheme COTS product. This assurance can be obtained during the system design phase.
System configuration tests	Test assurance obtained before deployment and maintained thereafter in line with the system re-accreditation process. Further details on the Accreditation process can be found in the Accreditation Framework.

System test data

Data used for system testing usually involves test data which have similar characteristics as close as possible to operational data.

Data used for system testing **must not** contain any live data. The use of live data, and in particular live data containing personal information, is prohibited. However, as test data will tend to simulate live operations data, it is important that test data is protected to ensure details of the system design and operation are not compromised.

To protect system test data, the following principles should be followed:

- The test manager must authorise the use of test data.
- Test data should be erased from a testing environment immediately after the testing is complete or when no longer required.
- The copying and use of test data should be logged to provide an audit trail.

In exceptional circumstances, the use of live system data might be permitted. Permission to use live data is by exception only. A valid business case must be approved by the MoJ IT Security Officer (ITSO), system assurer, and Information Asset Owner (IAO). Further information can be obtained from the MoJ Data Access and Compliance Unit (DACU) who maintain the policy on the use of live personal data.

Note: The risk associated with the use of live personal data for testing might require Senior Information Risk Owner (SIRO) approval. See this information for further details.

Risk assessment and management

As expressed at the start of this section, the rigour of any security tests must be commensurate with the impact of a security failure. This means that a risk based approach must be taken when considering what types of security tests to execute.

The decision on what security tests to include in the overall system test plan must be based on the system IS1 risk assessment, and agreed with the system assurer. The section below (Types of security tests) provides an overview of the types of security tests which must be considered. Further details on the assurance process can be found in the Accreditation Framework.

When a security test has been conducted, it is likely to highlight several risks and issues which need to be remediated and managed appropriately. This remediation is usually captured in a Risk Treatment Plan (RTP) which outlines what

the issue or vulnerability identified is, the risk associated with it, and the planned risk mitigation. The RTP needs to be agreed with the system Accreditor prior to being implemented. Further details on this process can be found in the Accreditation Framework.

Types of security tests

Security testing is discussed as part of the NCSC guidance on Building a secure digital service.

This section provides an overview of the three most common types:

- System configuration tests.
- Vulnerability scanning.
- Compliance scanning.

System configuration tests

System configuration tests are first conducted prior to deployment and repeated periodically thereafter with the objective being to ensure that the system or system component does not contain any unacceptable vulnerabilities.

These tests may include:

- Internally conducted tests (e.g. by the system developer) to provide informal assurance that there are no unacceptable vulnerabilities.
- External and perhaps more rigorous tests to provide formal assurance, for example, a penetration test or social engineering test.

There any many different types of penetration test. For most MoJ IT systems, the most common conducted is an annual IT Health Check (ITHC).

Internal tests may be performed more regularly to provide informal assurance that on-going changes have not introduced any new vulnerabilities to an IT system, and that existing security controls are operating correctly.

IT Health Check

An IT Health Check (ITHC) is the penetration test conducted as part of the NCSC specified and managed CHECK scheme. It is intended to provide external assurance that an IT system's setup and configuration meets the desired HMG assurance level.

Note: Most systems connected to MoJ or other government networks or systems mandate an ITHC every 12 months.

Vulnerability scanning

A vulnerability scan is intended to scan a network (and connected IT systems), cataloguing the patch status of all software and system services, and alerting on those identified which are not up-to-date, based on databases of patches and vulnerabilities. These alerts provide an operational view of the technical vulnerabilities an IT system is exposed to, and the information required to assist an IT system manager in applying up-to-date patches.

This type of scanning is intended to provide regular internal assurance to the ITSO and assurer that operational security risks are being managed effectively.

Compliance scanning

Besides simply testing for the absence of correctly patched software, some vulnerability scanners can also test when an IT system's settings correspond to an established benchmark, for example, to the MoJ password requirements, or a commercial security standard such as PCI DSS. The scanner operates by examining the security configuration settings of each IT system client (through a client installed agent) against one or more benchmarks (e.g. PCI DSS or ISO 27001), producing a compliance report as an output which can be supplied as assurance evidence.

Pre-live security testing

During the development and deployment phases of an IT system, there are a number of standard testing activities which are conducted. Security testing is not a separate stream of activity. It must be integrated within the overall set of testing activities.

The Secure code review activity highlights the issues associated with secure code reviews, while the Security consideration activity provides an overview of the security testing consideration which should be applied against each standard testing activity.

Secure code review

In principle, good software development practices and the application of a comprehensive code quality assurance regime should cover the basics of what is required to deliver a secure system. The NCSC provides guidance on Building a secure digital service. It is recommended that those responsible for software development and system testing review the guidance, and ensure any development practices and system testing reflects the guidance provided.

Note: It is essential that the secure coding guidance provided to application developers and the secure code review regime is documented, and made available to the system assurer for review and approval.

Security consideration

Table 1 below provides a high level overview of the security testing which should be considered against each of the main testing activities typically conducted during the development and deployment phases of an IT system.

Table 3: Table 1 – Security consideration

Testing activity	Description	Security testing consideration
Unit, Module, or Package Testing	This is aimed at verifying that individual modules/packages comply with their design.	See Secure code review.
Component Testing	Units or Modules combined into components then tested. This is aimed at verifying that the individual components meet their design and specification requirements. Third party software may also be introduced at this point and tested.	See Secure code review. Functional testing and enhanced secure code review of security enforcing components.
Integration Testing	Involves combining system components together into a complete system release, then testing as a whole.	Functional testing of security enforcing components. Functional testing of the integration of components with security enforcing functions.
Acceptance Testing (FAT and SAT)	The set of tests to be run to demonstrate the suitability of the system to the client. These will typically be a subset of the tests used for system testing in the integration phase.	Testing of both functional and non-functional security requirements. Penetration test or ITHC (see System Configuration Tests). Vulnerability scan (see Vulnerability Scanning). Compliance scan (see Compliance Scanning).

Testing failure

Should a failure occur in any of the security testing activities undertaken, an assessment must be made on what caused the failure and how serious it is. There may need to be discussions with the system assurer to inform them of any serious issues which might affect the assurance of the IT system.

Acceptance testing

As described in the last row of Table 1, some form of security testing must form part of the acceptance criteria for an IT System.

Contact details

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

Test data

Using Live Data for Testing purposes

Summary

This document describes the use of live data during testing of Ministry of Justice (MoJ) systems. In general, using live data for testing purposes is considered bad practice. By default, the MoJ does not permit testing using live data. It is highly likely that simply using live data for testing purposes would not be compliant with GDPR.

Following this guidance will help you avoid problems, but cannot guarantee that you have addressed all the concerns. You must carry out a full Data Protection Impact Assessment.

Who is this for?

This guide is aimed at two audiences:

1. The in-house MoJ Digital and Technology staff who are responsible for testing systems as part of technical design, development, system integration and operation.
2. Any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the MoJ.

Do you really need to use live data?

According to Information Commissioners Office, you may use either live or dummy data to test your products so long as they are compliant with data protection law. However, using dummy data may be preferable as it does not carry any risk to data subjects.

If you are processing live data, you will need to complete a Data Protection Impact Assessment beforehand if there is a possibility of risk to the data subject. The ICO has helpful information about using a Sandbox to help utilise personal data safely.

Data used for testing purposes must have characteristics that are as close as possible to operational data. But that is not the same thing as needing to use live data.

Check whether you really need to use live data, by considering the following questions:

1. **Speed:** What are your time requirements for test data provisioning?
2. **Cost:** What is an acceptable cost to create, manage and archive test data?
3. **Quality:** What are the important factors to consider related to test data quality?
4. **Security:** What are the privacy implications of these two sources of test data?
5. **Simplicity:** Is it easy for testers to get the data they need for their tests?
6. **Versatility:** Can the test data be used by any testing tool or technology?

The best test data simulates live operations data.

Note: It is important that test data is protected to the same standard as the live data. This is to ensure that details of the system design and operation are not compromised.

To protect test data, the following principles should be followed:

- The test manager must authorise the use of test data.
- Test data should be erased from a testing environment immediately after the testing is complete or when no longer required.
- The copying and use of test data should be logged to provide an audit trail.

Note: In the absence of an allocated test manager for a project, refer to the system owner.

By default:

- Data used for testing must not contain any live data.
- Using live data containing personal information is prohibited.

In exceptional circumstances, the use of live system data may be permitted. Permission to use live data is by exception only. A valid business case must be approved by the MoJ CISO, system assurer and the Information Asset Owner (IAO).

The Information Asset Owner must ensure that live data will be used lawfully, fairly and in a transparent manner in the interest of the data subject.

A thorough risk assessment, and a Data Protection Impact Assessment, should be carried out to ensure where interdependent applications, systems, services, APIs, BACS, XML, or processes, may be required, these are appropriately reviewed and security controls put in place.

Anonymising data

It might be acceptable to 'anonymise' the live data such that it can be used more safely for testing purposes. Consider:

- Is it possible to do this?
- What processes can you follow to generate acceptable data?
- Is randomisation sufficient?
- What about obfuscation?
- When is production-like data acceptable (or not) for testing purposes?
- How do you ensure that production-like data is sufficient for testing purposes?
- What are the expectations regarding suppliers - for code, and for services?

If you are considering the anonymisation option, pay particular attention to specific types of data that are often sensitive. Examples of data that must be anonymised include:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where it can be used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation
- data concerning criminal offences
- email addresses
- bank details
- telephone numbers
- postal or residential addresses

This list is not exhaustive.

In general, recommendations for anonymising data include:

- Replace with synthetic data.
- Suppress (remove) or obfuscate.
- A useful link for anonymising telephone numbers is here.

Data Privacy considerations

The use of live data for testing, where the data contains personal information, is almost certainly incompatible with the initial specified, explicit and legitimate purpose(s) known to data subjects. In effect, the data subject didn't know that their data would be used for test purposes.

There are sometimes valid reasons when you do need to use live data for test purposes but they are normally the exception rather than the norm and typically looked at on a case by case basis where appropriate risk management calls can be taken.

Looking at datasets being pulled out of databases are a prime example of where you may need to use live data to make sure that a software application is functioning correctly. For some things it is not always possible to use synthetic data.

Where a project is considering the use of live data for test purposes, it is essential to understand the data first, to be clear about what GDPR related factors apply.

You might need to look at fair processing notices and take these into account around the context of the tests being performed.

Note: It may actually be illegal to perform planned tests if fair processing notices do not allow using the data for test purposes.

Where the data involves personal information, help must be obtained from the MoJ Data Privacy team. At the very least, you must revisit or update an existing Data Protection Impact Assessment.

If there is no option apart from using live data, some of the things that should be considered will include the following:

- How will the data be extracted or obtained, and who will perform or oversee the extraction? What clearance do they have?
- What controls are in place to extract the data?
- Where is the data going to be extracted to? In other words, what media or mechanism will be used? For example, is the data extracted using electronic means such as SFTP, or is the data extracted to removable media, or does it remain 'in situ'?
- How is this data going to be protected at rest and during transit?
- What systems will the data be copied to, and in what environments?
- What systems will the data be processed by?
- How will access to this information be controlled both at rest and during transit for all systems that are involved in processing it?
- What access controls are in place end to end?
- Once testing is complete how will the data be removed/destroyed? What assurances do you have over this?

If live data is being used for test purposes within the Production environment, then backups are key and the testing to make sure that backups can be quickly restored is a must. There needs to be a good rollback plan in place. There also has to be an appetite for risk acceptance.

Ensuring test data is GDPR compliant

If you are intending to seek a special exception for using live data, or if you have anonymised the data but still want to have a satisfactory level of Data Privacy consideration, the follow points will help. Ensure that your test model has:

- Well-defined documentation of personal data information in all test environments.
- Effective data discovery to understand and unearth sensitive data information.
- Implemented a test data management process for the entire data life cycle that includes profiling, sub setting, masking, provisioning and archiving data in test environments.
- An irreversible 'on-the-fly' data masking process for production data within a repository.
- Permission and alerts in place for data exports and access outside the region, as this is restricted.
- Controls to prevent access to personal data from unauthorised access points, devices, or locations.

If testing is to go ahead
Developer access

In a normal working environment, developers working on an application, platform or service would be segregated away from access to live/production data. They would never be able to see or manipulate this data. The use of live data for test purposes would potentially negate or bypass these controls.

Also, developer roles are often specified as not requiring SC clearance or above. This applies also to external (3rd party) software suppliers generating bespoke applications or services. The expectation is that the developers do not ever have access to live data.

The use of live data for testing may mean that the clearance levels for developers on a given project would need to be reviewed.

Preparing for tests

Any code or tests involving live data should ensure the following:

- Code performs input validation.
- Output is correctly encoded.
- Full authentication and authorisation is in place.
- Session management is in place to ensure that code and data is not continually available outside the testing activities.
- Strong cryptography is used to protect data 'at rest', 'in transit' and 'in use'.
- All errors and warnings generated by applications, services, or recorded in logs are monitored, captured and actioned.
- A Data Protection Impact Assessment has been performed.
- Any backup processes will correctly filter out or otherwise protect the live data within the test environment.

Supplier relationships

Information security in supplier relationships

Assessing suppliers

The Ministry of Justice (MoJ) assesses suppliers as a responsible public body managing public funds and data. These assessments range from commercial and legal for the purposes of contract through to risk assessments for the purposes of information security.

The MoJ utilises a range of risk management techniques including information risk assessments.

Suppliers are expected to create, maintain and demonstrate a mature and considered approach to risk management when engaged with the MoJ.

Accreditation

The MoJ no longer accredits new systems or suppliers (as defined by CESG Information Assurance Standard 1&2).

The MoJ maintains accreditations where committed to by existing contract.

Commodity digital technology

MoJ assesses commodity digital technology supply chain such as Software-as-a-Service (SaaS) tools such as Google Workspace, Microsoft Office 365, Trello and AtlassianCloud based on the Cloud Security Principles, information risk assessment techniques and shared data within HMG.

Contractual promises

The Ministry of Justice (MoJ) embeds data governance and security-related clauses and schedules with contracts.

The MoJ is in the process of standardising and commoditising comprehensive clauses and schedules and will implement them over time.

Security Aspects Letters

Purpose

The Ministry of Justice (MoJ) will issue a Security Aspect Letter (SAL) where appropriate.

SALs are generally not required at OFFICIAL but MoJ may issue a SAL where it is optimal to do so or to supersede existing SALs from the previous classification scheme.

This page was last updated on 2018-12-21

Template

Dear <NAME OR ROLE OF SECURITY DIRECTOR>,

Subject: Security Aspects Letter

This Security Aspects Letter ('SAL') establishes the security principles which <ORGANISATION LONG LEGAL NAME, should be highest entity position such as the Group Plc> and/or its affiliates (together "<ORGANISATION SHORTNAME>") shall comply with in producing, handling or storing materials, information or data pertaining to the Ministry of Justice ('Authority').

This letter applies to <ORGANISATION SHORTNAME> and any relevant subcontractor within <ORGANISATION SHORTNAME>'s supply chain as required.

The following sections have been identified as the main areas where guidance is required. If there are any queries, please ask for clarification.

Purpose

This SAL issued by the Authority intends to convey the security principles required of <ORGANISATION SHORTNAME> to appropriately and proportionately ensure adequate confidentiality, integrity and availability of Authority data.

The SAL is not a complete and exhaustive list of requirements and conveys the spirit of information security and risk management requirements.

<ORGANISATION SHORTNAME> is required to ensure a comprehensive approach to information risk management through procedural, policy, personnel, physical and technical controls while in possession of Authority information.

Markings

This SAL has been developed under the premise that all information assets will be classified OFFICIAL under the UK Government Security Classifications Policy (GSCP) and that some may carry additional descriptors (for example, COMMERCIAL) to re-enforce handling requirements (such as 'need to know' principles) through the use of the SENSITIVE handling caveat.

All information must be considered OFFICIAL whether it bears a marking or not.

Handling Instructions

It should be noted that assigning an appropriate classification to information remains the responsibility of the creator or owner of the asset. Information marked with the SENSITIVE handling caveat may state, or otherwise be accompanied by, additional handling requirements (for example to limit distribution or define additional access controls) which all recipients including the <ORGANISATION SHORTNAME> must comply with.

In general, the Authority expects <ORGANISATION SHORTNAME> to apply the need-to-know principle to information related to Authority systems, and restrict access to such material to those within <ORGANISATION

SHORTNAME> (and its supply chain) who genuinely need it to perform their duties. General system information such as system names, IP addresses, high-level designs, etc does not require special handling protections.

Legacy Material

Information marked under the previous classification scheme(s) (such as UNCLASSIFIED, PROTECT, RESTRICTED or CONFIDENTIAL) should be effectively considered OFFICIAL unless otherwise stated.

Information marked under previous classification schemes should be reviewed as to whether the information within requires handling caveat markings and/or particular handling guidance before being re-marked as OFFICIAL.

Data Aggregation

In aggregation, the impact of a breach of any of these Security Aspects may be higher than the individual records or documents. <ORGANISATION SHORTNAME> should ensure that aggregated or accumulated collections of information assets are protected appropriately.

Data Offshoring

<ORGANISATION SHORTNAME> is permitted to Process Authority data (including Personal Data) outside of the United Kingdom subject to the maintenance of adequate information controls and governance, including (not not limited to), the continuation of the protection of rights and freedoms of Data Subjects in relation to their Personal Data, adequate contractual controls and adequate consideration under the <ORGANISATION SHORTNAME> Information Security Management System (ISMS).

<ORGANISATION SHORTNAME> must not routinely transfer or otherwise Process Authority data within an incompatible legal framework to the United Kingdom - more information on this is available on suitable request from the Authority.

Definitions are as per the Data Protection Act (2018)

Policy Compliance

Effective and appropriately scoped policy controls must be in place to underpin effective information management.

While related information security management certifications recognised by the British Standards Institution (BSI) such as ISO27001:2013, ISO27002:2013 and Cyber Essentials Plus are preferred, they are not required subject to comparable controls, policies and practices being in place.

A robust ISMS must be in place that ensures information assets are appropriately protected.

A holistic approach to information security must include staff awareness and training through to robust technical and enforced access controls.

Physical Security

Physical locations (such as offices and data-centres) must have appropriate physical security characteristics to safeguard information from informational risks.

Personnel Security

All personnel with direct or indirect access to, or influence over, information assets must achieve security clearance to at least the HMG Baseline Personnel Security Standard (BPSS).

Some roles and sites may require additional levels of clearance. These will be advised by the Authority to <ORGANISATION SHORTNAME> on a case-by-case basis.

All required security clearances must be achieved, and warranted to the Authority, prior to commencement of work by the individual unless otherwise agreed in writing by the Authority.

Full details of Security Clearance requirements are available with the Authority Vetting policy.

IT Controls

Systems

IT systems must be assessed under <ORGANISATION SHORTNAME> ISMS to ensure an appropriate level of informational risk understanding and where applicable corresponding controls or risk mitigation strategies.

IT technical controls should make all efforts to align to current recognised good practices and be periodically reviewed (no less than 12 month intervals) to understand and re-align controls where appropriate. Best practices include, but are not limited to, encryption methods, multi-factor authentication and software life cycles.

<ORGANISATION SHORTNAME> must ensure system suitability as per the output of the <ORGANISATION SHORTNAME> ISMS prior to the introduction of non-test data.

<ORGANISATION SHORTNAME> must provide information risk management information to the Authority on request so that the Authority may determine whether the assessment made and controls in place are sufficient and robust.

Any remedial activity that may be required by the Authority will be considered under contractual and commercial arrangements however <ORGANISATION SHORTNAME> must acknowledge that systems must be fundamentally fit for purpose and capable of protecting information assets in proportion to their content and value as defined by <ORGANISATION SHORTNAME> and/or the Authority.

Data transfer protections (data-in-transit)

All Authority, or Authority related data (such as professional work product pertaining to or on behalf of the Authority), must be protected against negative events (such as interception, misdirection, manipulation or otherwise unintended outcome) while in transit.

The Authority considers application or transport level encryption to be sufficient at OFFICIAL subject to configuration guidance from the UK National Cyber Security Centre (NCSC) having been met.

Some examples of satisfactory approaches include, but are not limited to:

- Email systems meeting the 'Securing government email' guidance
- Transport Level Encryption (TLS) version 1.2 and above aligned to NCSC recommended configuration(s)
- Internet Protocol Security (IPSec) aligned to NCSC recommendation configuration(s)
- NCSC-approved products or services for data transfer
- Authority-approved products or services for data transfer

<ORGANISATION SHORTNAME> should discuss with the Authority where deviations from NCSC recommendations may be required due to technological limitations.

SAL revisions

The Authority reserves the right to issue a revised SAL at any time.

You are requested to acknowledge receipt of this letter and your acceptance of its terms as incorporated into your contract and binding within 14 days.

You are requested to confirm that the details of this SAL have been brought to the attention of the personnel directly responsible for the security of the services provided to, or in support of, the Authority, that they are fully understood, and that the security and information assurance requirements set out in the contract schedules can and will be taken to safeguard the material concerned within 28 days.

You agree to provide a SAL in similar form to all subcontractors, obtain their acknowledgement and provide a copy to the Authority within 28 days.

Yours sincerely,

Chief Information Security Officer Ministry of Justice (UK)

Declaration

<ORGANISATION SHORTNAME> will be required to return a declaration.

Please sign the declaration below and return this letter to the Authority, keeping a copy for your own records. Should you have any queries, please contact the Authority via your point of contact and/or the contact details located within the SAL.

Supplier Declaration

The <ORGANISATION SHORTNAME> hereby confirms that the associated with the requirements described in this Security Aspects Letter have been brought to the attention of the individuals and organisations directly responsible for the provision of the various services. Additionally, that they are fully understood, and that the required security controls can and will be taken to safeguard the material and assets concerned.

For and on behalf of <ORGANISATION SHORTNAME>

…….. (name)

…….. (position) [Should be at least Director level]

……(date)

Distribution

Internal within Authority:

Action:

- Authority Security & Privacy

Information:

- Director of Authority Service Delivery
- Head of Service Delivery
- Authority Commercial

External:

Action:

- <ORGANISATION SHORTNAME>

Supplier corporate IT

The Ministry of Justice (MoJ) does **not** by default prohibit the use of supplier organisation corporate IT for the processing of MoJ data on the basis that the corporate IT environment is well designed, maintained, governed and defended in line with large scale commercial threat models.

Subject to the suitability described, the MoJ does **not** require suppliers to create or maintain dedicated or segregated IT solutions for the processing of MoJ data classified at OFFICIAL.

Technical security

Supplier corporate IT systems are expected to maintain appropriate levels of technical security defences to proportionally defend all types of data within whether the supplier's own corporate data through to MoJ data being processed.

This will range (but not be limited to) the use of modern Transport Layer Security or IPSec for in-transit encryption through to modern hashing and cryptography mechanisms for data stored at-rest, whether a data entry in a database or the entire storage drive in a laptop.

Supplier systems are expected to be proportionally resilient to malware, ensuring segregation between systems, users and data and employ adequate commodity measures (such as email attachment scanning/filtering).

Email security

Supplier corporate email systems processing MoJ data are expected to align to the UK government secure email policy which summarily requires widely accepted best practices.

Supplier corporate email systems are *not* required to technically integrate to the Public Services Network (PSN).

Data Governance
Data offshoring

Supplier's may process MoJ data (including Personal Data for which the MoJ is responsible) outside of the United Kingdom, subject to the maintenance of adequate information controls and governance.

MoJ data must not routinely be processed within an incompatible legal framework to the United Kingdom.

Working overseas

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

When working overseas, this may include limiting access to information while the user travels or using secondary temporary accounts to avoid primary account compromise.

Data backups

Supplier corporate IT systems may backup data for extended retention times (for example, keeping archived or deleted emails for an additional few months). Backup systems may also exist in such a way that individual backup items cannot be individually deleted, and are subject to a system-wide backup rotation/retention schedule.

Subject to appropriate data governance, the MoJ acknowleges these cases.

Local end-user device data

The MoJ acknowleges that corporate users typically 'download' files (from local email client caching to file downloads via a web browser) that can remain within 'Downloads' folders until explicitly deleted by the user.

MoJ expects suppliers to consider these types of data locations in data governance regimes, however it is appreciated that data destruction may be guidance based from the supplier organisation to supplier staff.

Supplier service delivery management

Baseline for Amazon Web Services accounts

The Ministry of Justice (MoJ) has a 'lowest common denominator' for security-related promises, capabilities and configurations of MoJ Amazon Web Services (AWS) accounts.

The baseline is not a holistic list of dos and don'ts, but a *minimum* line in the sand for what 'at least' **must** be done.

The base principle

All MoJ AWS accounts **must** utilise a series of agreed configurations to enable and support good tenancy within AWS and a suitable cyber security posture.

Anti-solutionising

This baseline discusses outcomes not *how* the baseline will be achieved/implemented.

The MoJ Cyber Security team strongly encourage the use of the highest abstraction level of services available from AWS to achieve these goals, and minimising the amount of custom code and configuration which needs to be developed (and thereafter, maintained) to satisfy each baseline.

Security incidents

The CyberSecurity team should be added as a security contact for all Information security incidents generated by AWS. The contact details for an AWS Account can be updated using the reference here.

- Full Name: `Operational Security Team`
- Title: `Mx`
- Email Address: OperationalSecurityTeam@justice.gov.uk

Baseline
IAM Access Analyzer

Utilise IAM Access Analyzer to audit and identify resources that are shared with an external entity.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
IAM Access Analyzer is enabled on all accounts, in all used regions, all of the time.	Alerts fire for new findings.	Findings are archived (if intended) or resolved (if unintended) within 7 days.

GuardDuty

Leverage AWS' commodity IDS solution to detect/protect from malicious or unauthorised behavior.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
GuardDuty is enabled on all accounts, in all regions, all of the time.	Alerts fire when GuardDuty is not enabled in a MoJ AWS account. Alerts fire for at least `HIGH` and above (or some version of) GuardDuty matches.	GuardDuty is automatically re-enabled.

CloudTrail

Leverage AWS' native activity audit platform (with adequate non-repudiation) to capture what AWS user (IAM etc) activity and changes are made within our AWS accounts

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
CloudTrail is enabled within all accounts, all of the time. CloudTrail logs are carbon copied to an AWS account controlled by Cyber Security.	Alerts fire when CloudTrail is not enabled in an MoJ AWS account.	CloudTrail is automatically re-enabled.

Config

Leverage AWS' native AWS configuration activity audit platform to capture what changes are being made to AWS configurations.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
Config is enabled within all accounts, all of the time. Config logs are carbon copied to an AWS account controlled by CyberSecurity via CloudTrail.	Alerts fire when Config is not enabled in an MoJ AWS account.	Config is automatically re-enabled.

Tagging

Tag all of our AWS objects, so we know they have a purpose and are intentional with defined ownership.

We have our own infrastructure ownership/tagging standards.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All relevant AWS objects are tagged as per MoJ requirements.	Creating AWS user is notified automatically in increasing urgency when object is untagged. AWS account owner (and increasing escalation) is automatically notified when objects remained untagged.	Untagged objects are forcefully and automatically shutdown/disabled or isolated after 7 consecutive days of not being tagged.

Regions

Do not use non-EU AWS regions for strategic compliance and performance reasons.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
No AWS account can create resources outside of AWS EU regions.	Alerts fire when non-EU resources are created to both the infrastructure teams and resource creator.	Non-EU resources are automatically and forcefully shut down after 12 hours.

Identity and Access Management

Enforce Identity and Access Management and Joiners, Movers and Leavers (JML) within AWS. We also need to ensure accounts that legitimately exist are well protected.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
AWS user accounts have a defined and peer reviewed method for request/creation. Viable, authoritative and 'single source of truth' documentation exists to describe each AWS account and who should and should not have access (in terms of roles). Idle AWS user accounts are suspended. MFA is required, always, enforced by policy. Root user account usage is considered abnormal. Passphrase and/or MFA seed cycled on every AWS root account use.	AWS group account owners are alerted when new AWS accounts are created. Idle (30 or more consecutive days of non-activity) AWS user accounts issue suspension notices to AWS group account owners and target users. Where an account does not have MFA, the user and AWS group account owners are notified after 7 consecutive days. Any login or use of an AWS root account issues login alerts to the AWS group account owners.	Idle AWS user accounts are automatically suspended past threshold. Non-MFA AWS user accounts are automatically suspended past threshold. Alerts fire when an AWS root user account is used but the credentials are not updated within 7 days of utilisation.

For more information on MFA, see the Multi-Factor Authentication guidance.

Encryption

Leverage native AWS configuration options to make reasonable efforts to protect data.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All AWS objects supporting encryption must have it enabled.	S3 buckets without suitable SSE-* encryption enabled are alerted to resource creator and account owner.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security.

'World' Access

Ensure that public access to AWS data storage and compute is intentional, to avoid the 'leaky bucket' problem, and to aid attack surface minimisation.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
All AWS S3 objects should be not world (public) readable unless specifically intended to do so.	S3 objects are programmatically reviewed (including 'open' ones) against the source infrastructure-as-code, if there is a mismatch the resource creator and AWS account owner notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. After 7 days, the S3 object permissions are forcefully and automatically changed to remove 'world' access.
Compute (for example, EC2 or ECS) instances should not be directly accessible from public networks unless through specific intentional design and should be behind CloudFront and/or applicable load balancing (preferring AWS LB technology). It must be truly exceptional for common service ports (for example, TCP80 or TCP443) to be served directly from compute resources.	Compute instances are programmatically reviewed to ensure they are not internet-accessible unless explicitly designed and documented to be so. If there is a mismatch the resource creator and AWS account owner notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. After 7 days, the relevant security groups are forcefully and automatically changed to remove 'world' access.

Security Hub

Security Hub enabled where possible.

Over time we will be able to leverage this more, but in the immediate future this will enable us to do CIS-based scans.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
Security Hub is enabled on all accounts, in all regions, all of the time.	Alerts fire when Security Hub is not enabled in a MoJ AWS account.	Security Hub is automatically re-enabled.

Implementation

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

Compliance

Compliance with legal and contractual requirements

Data destruction

Data Destruction

'Data destruction' is the process of erasing or otherwise destroying data stored on virtual/electronic or physical mediums such as, but not limited to, printed copies, tapes and hard disks in order to completely render data irretrievable and inaccessible and otherwise void.

The base principle

For legislative, regulative, privacy and security purposes, it **must** be possible to decommission and delete (irreversibly 'erase' or 'destroy') data and confirm to a degree of relative confidence it has been completed.

Data should be erased from all related systems, such as disaster recovery, backup and archival, subject to reasonable data lifecycle caveats.

Destruction standards

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning
- NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation
- Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): https://www.pcisecuritystandards.org
- DIN: http://www.din-66399.com/index.php/en/securitylevels

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific Ministry of Justice (MoJ) guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific MoJ guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

Data lifecycle caveats

Automated systems involved in data management and associated lifecycles may not be capable of immediate destroying data on demand.

Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

There is generally no need to attempt to manually delete such data prior to the automated retention lapse as long as it is ensured that if the data is restored prior to data destruction it is not processed.

It is important that the final expected data where all data lifecycles will have completed to be readily identifiable with high confidence.

Definitions

The current draft of the definitions that are required by the current draft short and long format data destruction clauses.

Definitions to be added into definition contract schedule

Data Destruction - Data destruction is the process of erasing or otherwise destroying data or information whether in physical form (such as printed paper) or stored on virtual/electronic or physical mediums such as, but not limited to, tapes and hard disks; the purpose is to render data completely irretrievable and inaccessible, and therefore void.

Supplier - ?

Authority - ?

Buyer - ?

Data Process/Processing - means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Long format clause

The current draft of the Ministry of Justice (MoJ) commodity long format data destruction clause.

`Highlighted` words indicate potential requirement for contextual change, requirement of definition and so on.

Clause

1. Data Destruction
    a. The `Authority` requires the `Supplier` to ensure that `Data Destruction` has been adequately completed at the natural end and/or termination of contract as per `Schedule XX`.
    b. The `Supplier` shall take all reasonable commercial measures to ensure Data Destruction is an irrevocable action to prevent the reconstitution of data, in alignment with methods described in `Appendix XX`.
    c. The `Supplier` shall notify the `Authority` when data destruction has taken place, including the final date by which such destruction shall be complete in the case of scheduled data destruction or natural data management lifecycles such as through automated backup or disaster recovery systems.
    d. Where data cannot be immediately destroyed, access control methods must be put in place to limit the ability the ability for `Data Processing` until data destruction can be completed.
    e. The `Supplier` shall provide evidence of data destruction on request from the `Authority`, including but not limited to, copies of third-party data destruction certificates, copies of internal policy and process documents in relation to data management and data destruction.
    f. The `Supplier` shall notify the `Authority` within `24 (twenty-four) hours` of identification of unsuccessful or incomplete data destruction.

Long format appendix

The current draft of the Ministry of Justice (MoJ) commodity long format data destruction appendix. The appendix is a dependancy of the long format clause itself.

`Highlighted` words indicate potential requirement for contextual change, requirement of definition and so on.

Appendix

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning

- NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation
- Payment Card Industry Data Security Standard (Data Destruction): https://www.pcisecuritystandards.org
- DIN: http://www.din-66399.com/index.php/en/securitylevels

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific `Authority` guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific `Authority` guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

The required outcome is to ensure that `Authority` data is inaccessible by any reasonable commercial and resourced means (such as commercially available data recovery services).

Short format clause

The current draft of the Ministry of Justice (MoJ) commodity short format data destruction clause.

`Highlighted` words indicate potential requirement for contextual change, requirement of definition and so on.

Clause

The `Supplier` shall return all `Authority` Data in a machine-readable non-proprietary format defined by the `Authority` within `30 (thirty)` calendar days of the end of the contract.

The `Supplier` must also state, ensure and warrant the final calendar date by which any associated data management lifecycle system(s) will be complete, including the manual or automated data destruction at the end of such period. Such data management lifecycle(s) may include, but are not limited to, the `Supplier`'s supply chain and/or Data Processors, backup system(s) and/or disaster recovery and business continuity system(s). The `Authority` retains all applicable rights to instruct the `Supplier` to destroy all `Authority` Data according to the terms of this `[G-Cloud]` contract.

The `Supplier` is required to ensure adequate and complete Data Destruction of `Authority` Data, including any relevant and associated non-proprietary `Supplier` Data or work product stemming from the `Buyer` Data that the `Supplier` has not been otherwise permitted to retain or use.

Data Destruction must follow applicable guidance from the UK National Cyber Security Centre (NCSC) and/or the Payment Card Industry Data Security Standard (PCI-DSS) and/or DIN 66399.

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific `Authority` guidance: the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific `Authority` guidance: paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters.

Instruction & Confirmation Letter

The current draft of a templated Ministry of Justice (MoJ) data destruction letter, that may be issued by the MoJ to a supplier. The letter describes required actions and information, followed by a responsive declaration from the supplier.

Letter issued by MoJ

Background

For legislative, regulative, privacy and security purposes, it must be possible for Suppliers to decommission and delete (irreversibly 'erase' or 'destroy') data and warrant the same. Similarly, any storage media holding such data must be securely and comprehensively erased before reuse or disposal (such as at end-of-life).

An example of a data destruction obligation is where a Supplier (acting as a 'Data Processor', as defined by Data Protection legislation) working on behalf of, or supplying services to, the Ministry of Justice (the 'Data Controller', as also defined by Data Protection legislation). The Data Processor, including any sub-processor instructed or otherwise involved in Data Processing on the Data Processor's behalf, must comply with instructions from the Data Controller regarding data irrespective of any commercial contract or promise such as a Data Subject exercising the 'right to be forgotten'.

This document provides an acceptable data destruction baseline from the Ministry of Justice, and associated declaration. When followed completely, this baseline for data destruction is considered sufficient to comply with data decommissioning and disposable tasks (and corresponding supplier assurances) for material classified as OFFICIAL under the UK HMG Government Security Classifications Policy (including sensitive personal data or sensitive commercial data within the same).

Data Lifecycle

The Ministry of Justice informally acknowledge that automated systems involved in data management and associated lifecycles may not be capable of immediate decommissioning data on demand. Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

The Ministry of Justice require positive confirmation of the final date by which these systems will have completed their data lifecycle tasks and data destruction will have been completed by.

Where data cannot be erased immediately, there must be methods in place to limit and constrain access to the data until the data lifecycle is complete or manual intervention can be made and subsequent data destruction assured.

The Ministry of Justice reserves all rights regarding instructions relating to data. This includes any need for immediate data destruction.

Standards

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

- National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning
- NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation
- Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): https://www.pcisecuritystandards.org
- DIN: http://www.din-66399.com/index.php/en/securitylevels

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific MoJ guidance:

- the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
- data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific MoJ guidance:

- paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

The required outcome is to ensure that Ministry of Justice data is inaccessible by any reasonable commercial and resourced means (such as commercially available data recovery services).

Supplier declaration

Please sign the declaration below and return this letter to the Ministry of Justice, keeping a copy for your own records. Should you have any queries, please contact the Ministry of Justice CISO via security@digital.justice.gov.uk

Return electronically. Electronic signatures or otherwise positive confirmation are accepted.

Chief Information Security Officer Ministry of Justice 102 Petty France Westminster, London SW1H 9AJ
security@digital.justice.gov.uk

Date: _____

We hereby confirm that all Ministry of Justice data, including non-proprietary data generated through the provision of Service, has been suitably, appropriately, and irreversibly destroyed in its entirety and rendered permanently inaccessible and void.

`Data backup, including disaster recovery systems, will automatically conduct appropriate data destruction as part of an automated data life cycle on or before the _____ (Strike as applicable)`

`Anonymised and/or non-Personal Data has been retained for statistical analytical purposes only. We warrant compliance with all applicable data protection and privacy legislation in this regard. (Strike as applicable)`

Contract/project reference: _____

For and on behalf of organisation: _____

Name: _____

Position: _____

Date: _____

Data security and privacy

Data Security and Privacy

We believe that our technology must keep data safe and protect user privacy.

Our digital projects contain important information. Serious data breaches might result if we fail to:

- protect information
- handle it correctly at all times
- dispose of it safely when it is no longer required

Breaches might cause:

- harm to individuals
- financial loss to the Ministry of Justice (MoJ)
- a loss of confidence in us as an organisation

For personal data, the EU General Data Protection Regulation (GDPR) and UK Data Protection Act (2018) apply. These make the consequences of data breaches very clear.

To follow the data regulation/legislation, we **must** ensure that:

- we protect data to the best of our organisation's capabilities
- we collect data only for described, lawful purposes
- we use data only for the described, lawful purposes

Why are security and privacy important?

Breaches can have an adverse effect the relationship between citizen and government.

Not only do we have a duty to protect citizens data, but the penalties for violations are also severe. Under the GDPR, serious infringements can result in fines of up to €20M.

We must apply appropriate security and privacy protection to all the information we hold and process, at all times.

We should treat all data as sensitive unless proven otherwise.

All our work must follow this ethos.

When this applies

This principle applies to **all** MoJ technology projects and business actitivies.

While GDPR applies only to personal information, all MoJ projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow MoJ guidelines unless exceptional and approved circumstances apply.

The Information Commissioner's Office (ICO) - the UK's independent regulatory office for data protection - has published guidance on how to determine what is personal data.

A Data Protection Impact Assessment (DPIA, formerly commonly known as a Privacy Impact Assessment or PIA) is required for all projects. There are some exceptions described by the ICO.

Data Security & Privacy Lifecycle Expectations

Below are a series of data security and privacy expectations of Ministry of Justice (MoJ) projects at various stages in their lifecycle.

These measures can help simplify and ease the burden of embedding data security and privacy at the heart of projects.

Pre-Discovery and Discovery

Assess the data security and privacy implications of the project requirements thoroughly. Do this as part of the broader work addressing the project's strategic imperatives.

In particular:

- From the start of the project, and throughout its duration, think about how data security and privacy might affect the functionality and delivery of the project.
- Consult with technical architects to help inform and enhance the ways of delivering the work, whilst continuing to ensure compliance.
- Discuss any problems or ramifications that arise with legal or business experts. Identify areas where the required data security and privacy compliance might cause issues for functionality.

Alpha

During this stage of the project lifecycle, internal and external (Cabinet Office / Government Digital Service) teams will perform service assessments. These will specifically check for aspects of GDPR/DPA18 compliance.

In particular:

- >That the majority of compliance considerations have been addressed at this stage.
- That the development team can say how their work ensures compliance.
- That the technical architecture choices can be tested against data security and privacy requirements. As an example, blockchain technologies might not be acceptable as they can prevent automated removal of information when it is no longer required.

Beta (Private and Public)

These are assessments performed as the service transitions from Private to Public availability. The assessments are again performed by internal and GDS teams. Use live systems for the assessments.

In particular:

- All manually actionable data security and privacy requirements must be met.
- Manual testing is expected.

- Automatic deletion is not required yet, because the service is unlikely to have enough data at this stage. However, plans and mechanisms for automatic deletion should 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.