Ministry of Justice

IT Security

Policy

Contents

IT Security Policy (Overview)..... 3

Introduction..... 3
Audience..... 3
Associated documentation..... 3
Principles..... 3
Technical users..... 4
Service Providers..... 4
Enforcement..... 4
Incidents..... 4
Contacts..... 4

IT Security All Users Policy..... 4

Introduction..... 4
Audience..... 4
Approach..... 5
Assets..... 5
Security classification..... 5
Physical and personnel security..... 5
Identity and access control..... 6
Password management..... 6
Email security..... 6
Remote working and portable devices..... 6
Malware protection..... 7
Roles and responsibilities..... 7
Incidents..... 8
Contacts..... 9

IT Security Technical Users Policy..... 9

Introduction..... 9
Audience..... 9
Vulnerability scanning and patch management..... 9
Technical controls..... 9
Cryptography..... 10
Software development..... 10
Security incident management..... 10
Suppliers and procurement..... 10
IT Security..... 10
Physical and personnel Security..... 11
Privileged users..... 11
Risk management..... 11
Technical risk assessment and information assurance..... 11
Audit..... 11
Incidents..... 12
Contacts..... 12

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.

Audience

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 **SHALL**:

- 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 **SHALL** 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 **SHALL** 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`

Contacts

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

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.

Audience

This policy is aimed at three audiences:

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

	Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the MoJ.
General users	All other staff working for the MoJ.

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

Approach

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

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

Assets

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

Security classification

All MoJ Staff are responsible for ensuring data is:

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

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

Physical and personnel security

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

- All MoJ IT systems and services must be assessed against environmental risks, for example flood or fire, to maintain the asset's confidentiality, integrity, and availability.
- The MoJ's IT Teams are not directly responsible for the physical security and environment of the MoJ sites.

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

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

Identity and access control

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

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

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

Password management

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

Email security

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

The more detailed 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 that **SHALL** be used to protect all systems against malware. Malware might enter the MoJ by employee email, through the internet, mobile computers, or 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 **SHALL** 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 **SHALL** 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 that the policy and guidance material continues to provide appropriate risk appetite and a suitable risk framework.	Implementing and managing information risk management in their respective business groups.
		Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.
		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.

Role	Responsibility	Which includes...
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.
		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`

Contacts

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

IT Security Technical Users Policy

Introduction

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

Audience

This policy is aimed at:

Technical users	These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including 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 the 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 **SHALL** use cryptographic technologies to provide secure connections to third party systems or to protect information "at rest" on user devices, including laptops and mobile devices.

However, where staff have procured key material or hardware through the United Kingdom Key Production Authority (UKKPA) or any other cryptographic items where National Cyber Security Centre (NCSC) dictate that national cryptographic policy applies, the NCSC dictate the policy. In this case, the 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 **SHALL** 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 **SHALL** 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 **SHALL** 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 **SHALL** be regularly monitored, reviewed, and audited.
- When the MoJ buys IT goods, services, systems, or equipment, IT security implications **SHALL** be considered.

- All MoJ IT suppliers who handle and store information on behalf of the MoJ **SHALL** 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 **SHALL** be put in place for any supplier not meeting compliance requirements, and the relevant MoJ teams **SHALL** be notified and consulted.
- All MoJ suppliers and contractors **SHALL** 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 **SHALL** 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 **SHALL** 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 **SHALL** be reviewed.

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

Incidents

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

Operational Security Team

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

Contacts

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