Ministry of Justice

Security Guidance

Table of contents

Cyber and Technical Security Guidance

Summary

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

The MoJ Technical Guidance covers technical decisions in the MoJ more widely.

Note: This guidance is dated: 1 June 2022.

Popular links

Popular links for all users:

- Security threat level and emergency procedures
- Overseas travel and accessing MoJ IT systems from overseas
- General app guidance
- Minimum User Clearance Requirements Guide
- Government classification scheme
- Remote Working

Change log

A ‘change log’ is available. It details the most recent changes to this information.

The changes are also available as RSS or Atom feeds.

Offline content

For convenience, offline versions of this guidance are available.

Audience	PDF format	EPUB format
All users. Does not include lots of technical detail.	PDF	EPUB
Group Security. Contains Group Security policy and guidance.	PDF	EPUB

Audience	PDF format	EPUB format
Technical users. Includes lots of technical detail. This document contains all content, including for 'All users' and from Group Security. Download this document if you want the complete set of published MoJ security policy and guidance.	PDF	EPUB

The offline versions of this guidance are time-limited, and are not valid after 1 July 2022.

Security culture

In addition to the obvious security resources such as policies, controls, and software and hardware tools, all organisations need employees, suppliers and other colleagues to behave in a way that helps ensure good security at all times. A simple example is where someone will act in a way that maintains good security, even if they don't know exactly what the formal process is. The extent to which an organisation has good security in indicated by its security culture.

Security culture refers to the set of values, shared by everyone in an organisation, that determines how people are expected to think about and approach security. Getting security culture right helps develop a security conscious workforce, and promotes the desired security behaviours expected from everyone working in or for the organisation.

The MoJ is creating a portfolio of security culture resources to help supplement the formal policy and guidance material. Initial security culture material is available for preview here.

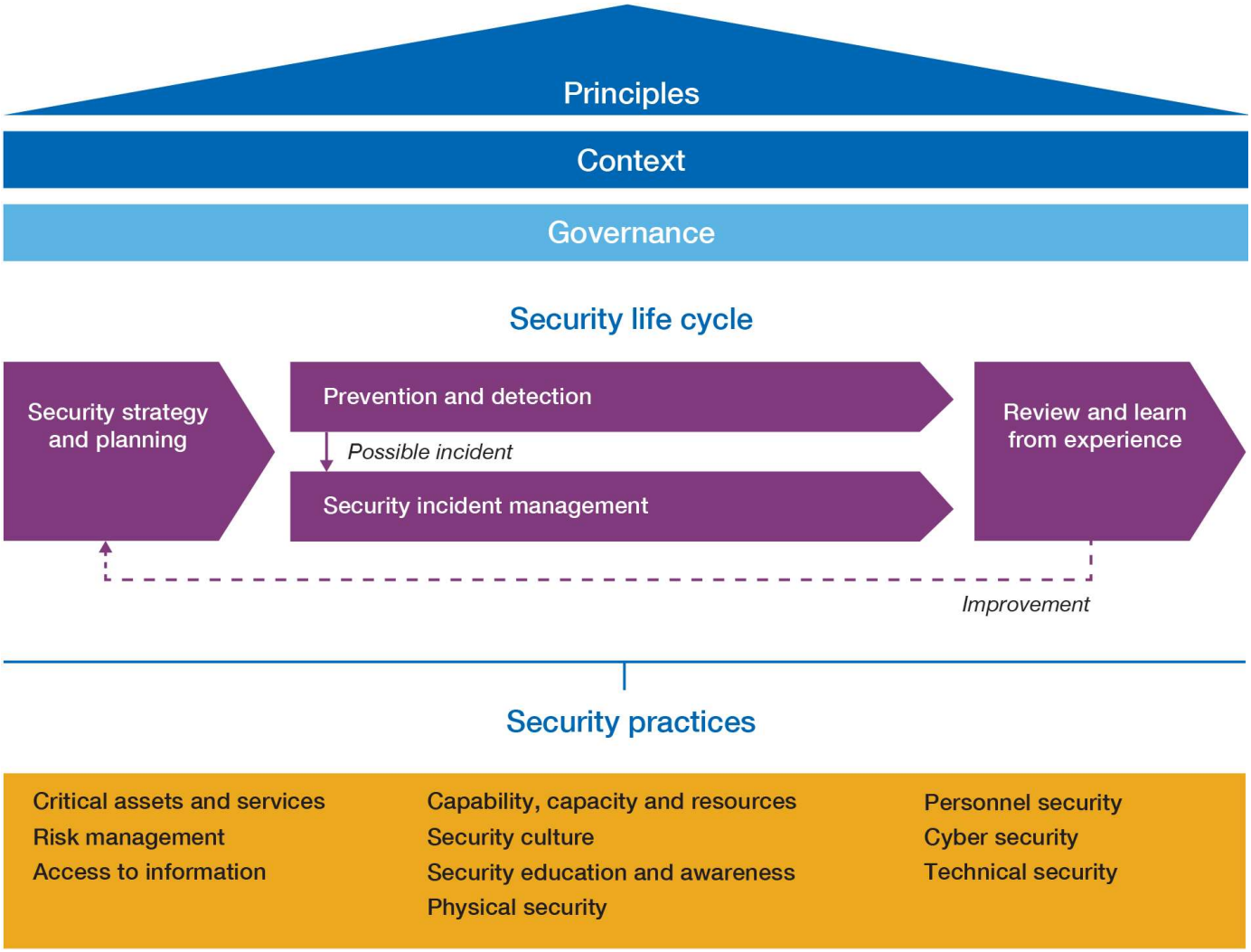
Getting in touch

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

Background

Government Functional Standard - GovS 007: Security replaces the HMG Security Policy Framework (SPF). The policies which sit within that framework remain in

effect, but are now in support of this standard.



Sections 6.3 Cyber security and 6.4 Technical security of the standard state:

- > The purpose of cyber security is to ensure the security of data and information. To operate effectively, the UK government needs to maintain the confidentiality, integrity and availability of its information, systems and infrastructure, and the services it provides.

- > The purpose of technical security measures is to holistically protect sensitive information and technology from close access acquisition or exploitation by hostile actors, as well as any other form of technical manipulation. Technical security also relates to the protection of security systems from compromise and/or external interference.

Information structure

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

Level 1	Level 2
Information security policies	Management direction for information security
Mobile devices and teleworking	Mobile device policy
	Teleworking
Human resource security	Prior to employment
	During employment
Asset management	Responsibility for assets
	Information classification
	Media handling
Access control	Business requirements of access control
	User access management
	User responsibilities
	System and application access control
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas
	Equipment
Operations security	Operational procedures and responsibilities
	Protection from malware
	Backup
	Logging and monitoring
	Control of operational software
	Technical vulnerability management
Communications security	Network security management
	Information transfer

Level 1	Level 2
System acquisition, development and maintenance	Security requirements of information systems
	Security in development and support processes
	Test data
Supplier relationships	Information security in supplier relationships
	Supplier service delivery management
Information security incident management	Management of information security incidents and lost devices
Information security aspects of business continuity management	Information security continuity
Compliance	Compliance with legal and contractual requirements
	Information security reviews
Risk Assessment	Risk Assessment Process

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

Information security policies

Management direction for information security

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

	Software Developer
Technical Controls Policy	Technical Architect, DevOps, IT Service Manager, Software Developer

Mobile devices and teleworking

Mobile device policy

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

Teleworking

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

Human resource security

Prior to employment

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

During employment

Ongoing Personnel Security	All users
Personnel risk assessment	All users

Reporting personal circumstance changes	All users
Training and Education	All users
Voluntary drug testing policy	All users
Voluntary drug testing policy procedures	All users

Termination and change of employment

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

Asset management

Responsibility for assets

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

Information classification

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

Media handling

Removable media	All users
Secure disposal of IT equipment	All users

Secure disposal of IT - physical and on-premise	All users
Secure disposal of IT - public and private cloud	Technical Architect, DevOps, IT Service Manager, Software Developer
Working securely with paper documents and files	All users

Access control

Business requirements of access control

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

User access management

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

Monitoring Guide	Manager, Software Developer

User responsibilities

Protecting Social Media Accounts	All users

System and application access control

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

Cryptography

Cryptographic controls

Automated certificate renewal	Technical Architect, DevOps, IT Service Manager, Software Developer
Cryptography	Technical Architect, DevOps, IT Service

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

Physical and environmental security

Secure areas

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

Equipment

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

Operations security

Operational procedures and responsibilities

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

Protection from malware

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

Backup

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

Logging and monitoring

Accounting	Technical Architect, DevOps, IT Service Manager, Software Developer
Commercial off-the-shelf applications	Technical Architect, DevOps, IT Service Manager,

	Software Developer
Custom Applications	Technical Architect, DevOps, IT Service Manager, Software Developer
Logging and monitoring	Technical Architect, DevOps, IT Service Manager, Software Developer
Online identifiers in security logging and monitoring	Technical Architect, DevOps, IT Service Manager, Software Developer
Protective Monitoring	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Enterprise IT - Infrastructure	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Enterprise IT - Mobile Devices	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Hosting Platforms	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Log entry metadata	Technical Architect, DevOps, IT Service Manager, Software Developer
Security Log Collection: Maturity Tiers	Technical Architect, DevOps, IT Service Manager, Software Developer

Control of operational software

Guidance for using Open Internet Tools	All users

Technical vulnerability management

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

Vulnerability scanning guide	Technical Architect, DevOps, IT Service Manager, Software Developer

Communications security

Network security management

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

Information transfer

Bluetooth	All users
Criminal Justice Secure Mail (CJSM)	Technical Architect, DevOps, IT Service Manager, Software Developer
Data Sovereignty	Technical Architect, DevOps, IT Service Manager, Software Developer
Email	All users
Email Authentication Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Email Blocklist Policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Email Blocklist Process	Technical Architect, DevOps, IT Service Manager, Software Developer
Email Security Guide	Technical Architect, DevOps, IT Service Manager, Software

	Developer
General Apps Guidance	All users
Phishing Guide	All users
Secure Data Transfer Guide	All users
Secure Email Transfer Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Sending information securely	All users
Spam and Phishing Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Web browsing security policy profiles	All users (Policy)
Wifi security policy	All users (Policy)

System acquisition, development and maintenance

Security requirements of information systems

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

Security in development and support processes

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

Test data

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

Supplier relationships

Information security in supplier relationships

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

Supplier service delivery management

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

Information security incident management

Management of information security incidents and lost devices

Forensic Principles	Technical Architect, DevOps, IT Service Manager, Software Developer
Forensic Readiness Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
Forensic Readiness Policy	Technical Architect, DevOps, IT Service Manager, Software Developer
Incident Management Plan and Process Guide	Technical Architect, DevOps, IT Service Manager, Software Developer
IT Incident Management Policy	Technical Architect, DevOps, IT Service Manager, Software Developer

Lost devices or other IT security incidents	All users
Reporting an incident	All users

Information security aspects of business continuity management

Information security continuity

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

Compliance

Compliance with legal and contractual requirements

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

Information security reviews

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

Risk Assessment

Risk Management

Infrastructure and system accreditation	Technical Architect, DevOps, IT Service Manager, Software Developer
IT Health Checks	Technical Architect, DevOps, IT Service Manager, Software Developer
IT Health Check - Test cancellations and delays	Technical Architect, DevOps, IT Service Manager, Software Developer

Risk Assessment Process

Risk reviews	All users

Other Guidance

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

Glossary

A glossary of some terms used in this guidance is available here.

Acronyms

A more extensive list of acronyms is available here.

Technical Guidance

The MoJ Technical Guidance should be read together with this security-focused guidance.

Feedback

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