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.

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

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

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

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

Minimum User Clearance Requirements Guide

Introduction

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

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

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

Multi-Factor Authentication (MFA) Guide

Introduction

This Multi-Factor Authentication (MFA) guide explains how MFA can be used to ensure that users are only granted access to 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)
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)

Preference	Type
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

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

Privileged Account Management Guide

Introduction

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

How to manage privileged accounts

Holders of privileged accounts, such as system administrators, have privileges to perform most or all of the functions within an IT operating system. Staff should have privileged accounts only when there is a business need, in order to prevent malicious actors gaining privileged access to 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

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

Operations security

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.

Security Log Collection

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).

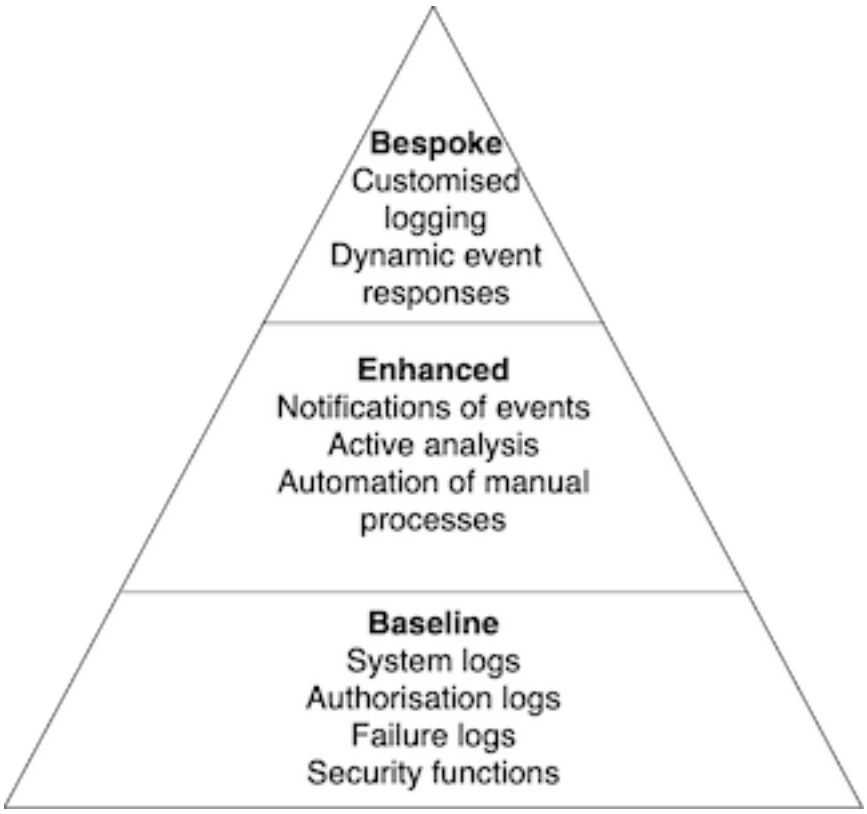
Three tiers have been developed to reflect the breadth and complexity of collecting and forwarding log data.

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.

Last updated: April 20th, 2020.

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

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 abroad

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

When working abroad, this may include limiting access to information while the user travels or using secondary temporary accounts to avoid primary account compromise.

Data backups

Supplier corporate IT systems may backup data for extended retention times (for example, keeping archived or deleted emails for an additional few months). Backup systems may also exist in such a way that individual backup items cannot be individually deleted, and are subject to a system-wide backup rotation/retention schedule.

Subject to appropriate data governance, the MoJ acknowleges these cases.

Local end-user device data

The MoJ acknowleges that corporate users typically 'download' files (from local email client caching to file downloads via a web browser) that can remain within 'Downloads' folders until explicitly deleted by the user.

MoJ expects suppliers to consider these types of data locations in data governance regimes, however it is appreciated that data destruction may be guidance based from the supplier organisation to supplier staff.

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
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.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
Compute (for example, EC2 or ECS) instances should not be directly accessible from public networks unless through specific intentional design and should be behind CloudFront and/or applicable load balancing (preferring AWS LB technology). It must be truly exceptional for common service ports (for example, TCP80 or TCP443) to be served directly from compute resources.	Compute instances are programmatically reviewed to ensure they are not internet-accessible unless explicitly designed and documented to be so. If there is a mismatch the resource creator and AWS account owner notified.	After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. After 7 days, the relevant security groups are forcefully and automatically changed to remove 'world' access.

SecurityHub

SecurityHub enabled where possible.

Over time we will be able to leverage this more, but in the immediate future this will enable us to do CIS-based scans.

What must be in place	Monitoring	Resolution/Escalation if baseline is broken/violated
SecurityHub is enabled on all accounts, in all regions, all of the time.	Alerts fire when SecurityHub is not enabled in a MoJ AWS account.	SecurityHub is automatically re-enabled.

Implementation

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

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.