Technical Security Controls Guide: Defensive Layer 1

# Technical Security Controls Guide: Defensive Layer 1

**Parent topic:** [Technical Security Controls Guide](technical-security-controls-guide.html)

## 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)](multi-factor-authentication-mfa-guide.html), 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](access-control-guide.html) 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](using-live-data-for-testing-purposes.html), 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.