Technical Security Controls Guide: Defensive Layer 2

# Technical Security Controls Guide: Defensive Layer 2

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

## 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](data-security-and-privacy-lifecycle.html) 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](mailto: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.