Technical Security Controls Guide

# Technical Security Controls Guide

* [**Technical Security Controls Guide: Defensive Layer 1**](technical-security-controls-guide-defensive-layer-1.html)
* [**Technical Security Controls Guide: Defensive Layer 2**](technical-security-controls-guide-defensive-layer-2.html)

## 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](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) and the NCSC [Cyber Assessment Framework (CAF)](https://www.ncsc.gov.uk/collection/caf/cyber-safety-introduction). 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](technical-security-controls-guide-defensive-layer-1.html) 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](technical-security-controls-guide-defensive-layer-2.html) Layer 2 builds a monitoring capability for the network and extends existing security controls to mobile devices.