ICT security policy framework

This content is a version of the MOJ ICT Security Framework, January 2015.
This is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon.
Please contact us before using this on a new project: itpolicycontent@digital.justice.gov.uk.

This guidance applies to all staff and contractors who work for the MOJ.

MOJ's ICT security policy forms part of MOJ's corporate security policy.

Corporate security policy
IT systems are crucial in delivering the Department's core business activities effectively and all staff are required to understand their obligations in how to safeguard MOJ data and how to use IT appropriately.

The ICT security policy framework is designed to:

inform you on the acceptable use of MOJ ICT
let you know how to safeguard information assets from unauthorised access and modification
describes how you should use, access and disclose information in accordance with protective marking policies, regulations and applicable legislation
allows the department to detect, manage and recover from security incidents with the least disruption to the organisation
ensure MOJ IT suppliers and service providers comply with the minimum requirements set out in this policy and within the wider security policy framework
ensure that MOJ information and IT assets are utilised for MOJ business use only
enable MOJ to make best use of its investment in IT
ICT security policies – tier 1
ICT security policy
ICT security policy – information assurance strategy statement
Staff guidance
The ICT security guide gives you advice and guidance on the main security issues that are likely to affect you as a computer user within MOJ, including its agencies and associated offices. It also sets out your individual responsibilities for ICT security.

IT security guide
Security guidance for contractors
Remote working & mobile guide
Manager, developer and responsible owner guidance
There are further detailed ICT security policies which **must** be taken into consideration if you are developing, procuring or configuring MOJ ICT.

ICT security policies – tier 2

These polices form the core set of detailed security policies covering both IT usage and technical security controls:

Forensics readiness policy
IT incident management policy
Technical controls policy
Use of HMG Cryptography policy

IT security policies – tier 3

Tier 3 documents are available online and provide: benchmark standards, implementation guidance on specific security controls, and procedures for a particular policy (or policy statement/s).

Online documents

Access control standard
Code of connection standard
Data handling and information sharing guide
Forensics readiness guide
HMG cryptography business continuity standard
ICT asset disposal guide
Incident management plan and process guide
IT disaster recovery plan and process guide
Malware protection guide
Offshoring guide
Password standard
Patch management standard
Protective monitoring guide
System backup standard
System lockdown and hardening standard
System test standard

Contacts

Email Operational Security Team:
operationalsecurityteam@justice.gov.uk

or call:
0161 234 2046

This guidance is dated May 2018.

To provide feedback on this document, please contact us: itpolicycontent@digital.justice.gov.uk, or click one of the following icons.

Very unhelpful. Unhelpful. Helpful. Very helpful.

Last reviewed: 14 September 2021

Content tagged as: CICA, HMCTS, HQ, LAA, OPG, PB,