Ministry of Justice

Information Classification and Handling

Security Policy

Contents

Information Classification and Handling Policy

Introduction

This document provides the core set of IT security principles and expectations on the handling and classification of information on Ministry of Justice (MoJ) IT systems.

The MoJ stores and processes a wide variety of information, some of which attracts an HMG protective marking or contains personal information. The MoJ has a duty to protect all the information stored and processed on its IT systems.

This policy outlines the Information Classification and Handling Policy for all information held on MoJ IT systems.

Scope

This policy covers all staff (including contractors and agency staff) who use MoJ IT systems.

The overarching policy on information classification and handling is maintained by MoJ Security. This document only contains IT specific policies which are in addition to the overarching policy.

The overarching policy can be found here.

All Users **must be** made aware of the Information Classification and Handling Policy, and provided with security awareness training which covers this policy.

All Users **must be** provided with refresher security awareness training which covers this policy every 12 months.

Inventory of assets

All information assets need be identified and have a nominated asset owner, to help ensure that the appropriate protection of these assets is maintained.

Examples of what an information asset constitutes are:

- Databases and data files.
- System documentation.
- User manuals, training material, operational or support procedures.
- Security documentation such as RMADS or disaster recovery plans.
- Archived backup data.

The list of information assets and associated Information Assets Owners is coordinated and maintained by individual MoJ business groups, where the responsibility resides with the business group SIRO.

All MoJ business groups **must maintain** a list of information assets, their associated named Information Asset Owner (IAO), and which IT systems they reside on.

Note: Some information assets might not be held on IT systems.

Deriving a classification

At the MoJ, all information assets are assessed against HMG guidance on business impact, and HMG guidance on the protection of personal data. This assessment is used to select the appropriate classification from the Government Security Classification scheme.

All information assets stored or processed on MoJ IT systems **must be** assessed for a Business Impact Level, where an impact level for the Confidentiality, Integrity and Availability for each asset is derived.

The Asset Owner is responsible for determining the classification that applies to an asset.

All users are responsible for applying the appropriate classification to information assets created or handled on an IT system, where a pre-existing classification does not exist.

Note: As outlined in the MoJ IT Security Policy, all MoJ data and assets must have IT security controls designed and implemented to protect Confidentiality, Integrity, and Availability.

Further information on the criteria and derivation for classification can be found at: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/.

Reclassifying information

The asset owner has responsibility for reclassifying an asset. If another user has reason to believe that an asset is incorrectly classified or has an incorrect handling caveat, they should normally discuss this with the asset owner. The other user cannot unilaterally reclassify the asset.

The exception is where the asset might need a higher classification than that assigned by the asset owner. The reclassification must still be communicated to the asset owner, for consistency. If it is agreed that the classification should be increased, check with the Operational Security Team (OperationalSecurityTeam@justice.gov.uk) whether additional actions are required to protect the material.

Application of Government classification

The Government classification scheme defines how information should be labelled and handled. Output from IT systems containing information that is classified must carry classification labels where it is `OFFICIAL` or higher. This includes, but is not limited to, printed reports, removable media, electronic messages (such as e-mail) and file transfers.

All IT hardware and removable media assets **must** be labelled with the highest classification from among each of the individual information assets stored or processed on it.

Note: This classification might be reduced if sufficient security controls are applied, for example whole disk encryption, and if there is agreement with the system assurer or Chief Information Security Officer (CISO).

All output from an IT system **must** be given the classification of the highest of each of the individual information assets contained within that output.

Where applying a classification label is not feasible, an alternative method **must be** agreed with the system assurer or CISO.

Further information on the criteria and derivation for classification can be found at: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/.

Information handling on MoJ IT systems

The MoJ policy for handling classified material applies to all MoJ IT assets and all outputs from an IT system.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.

Government Classification Scheme

These summary guidelines are based on the Government Security Classification (GSC) as issued by the Cabinet Office in 2018. The link below provides full handling guidance for information classifications including OFFICIAL, SECRET and TOP SECRET:

https://www.gov.uk/government/publications/government-security-classifications

In summary, the majority of information that is created or processed by the public sector is now classified as OFFICIAL. The other two classifications are SECRET and TOP SECRET.

SECRET classification should be used on very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors.

TOP SECRET is HMG's most sensitive information requiring the highest levels of protection from the most serious threats.

Classifications can have additional indicators, providing extra information about looking after the information with that classification. A frequently-seen example is OFFICIAL-SENSITIVE. This is still classified as OFFICIAL, but there is an additional indicator that tells you the information is of a more sensitive nature, and so should be handled and looked after accordingly.

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for security advice, contact the Cyber Assistance Team CyberConsultancy@digital.justice.gov.uk.