Ministry of Justice

Information Classification and Handling

Security Policy

Contents

Information Classification and Handling Policy

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 email) 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

The Government Security Classification (GSC) system has three levels: `OFFICIAL`, `SECRET`, and `TOP SECRET`.

The GSC was issued by the Cabinet Office in 2018: https://www.gov.uk/government/publications/government-security-classifications

OFFICIAL

This is the majority of information that is created or processed by the public sector.

> Includes routine business operations and services, some of which could have damaging consequences if lost, stolen, or published in the media, but which are not subject to a heightened threat profile.

This classification applies to the vast majority of government information including general administration, public safety, criminal justice, and law enforcement, and reflects the fact that reasonable measures need to be taken to look after it and to comply with relevant legislation such as the Data Protection Act, Freedom of Information Act, and Public Records Acts.

OFFICIAL-SENSITIVE

A limited amount of information is particularly sensitive, but still comes within `OFFICIAL` if it is not subject to the threat sources for which `SECRET` is designed, even if its loss or compromise could have severely damaging consequences. The need to know principle **SHALL** be rigorously enforced for this information, particularly where it might be shared outside of a routine or well understood business process. There are very few activities where all related information or cases require the `OFFICIAL-SENSITIVE` marking, though this might apply to assets previously marked as `CONFIDENTIAL`. Across a range of information assets which were previously normally marked as `PROTECT` or `RESTRICTED`, there might be individual cases/instances which are more sensitive (some of which might be marked `CONFIDENTIAL` on an individual basis). This more sensitive information is identified by adding '`SENSITIVE`', and must therefore be marked '`OFFICIAL-SENSITIVE`'. This marking alerts users to the enhanced level of risk and that additional controls are required.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined or highly capability threats.

> Where compromise might seriously damage military capabilities, international relations or the investigation of serious organised crime.

Use of `SECRET` **SHALL** only be used where there is a high impact and a sophisticated or determined threat (elements of serious and organised crime, and some state actors):

- Classified material received from Other Government Departments (OGDs) or agencies relating to national security and counter-terrorism.
- Intelligence and investigations relating to individuals of interests to security agencies.
- Information that might seriously damage security and intelligence operations.
- Information affecting the ability to investigate or prosecute serious or organised crime.
- Personal/case details where there is a specific threat to the life or liberty of an individual such as protected witness scheme records.

The concept of sophisticated or heightened threat doesn't only apply to those with a high technical (IT) attack capability, but might apply to criminals who have a developed capability to intimidate or coerce individuals. If disclosure of information might result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information **SHALL** be tightly controlled. `SECRET` **SHALL NOT** become the default status for material just because of the type of case or potentially severe consequences such as murder trials, or where there is a threat to life. The threat capability **SHALL** also be present.

TOP SECRET

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

> Where compromise might cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level. Any business area holding or expecting to hold information at this level **SHALL** contact the Departmental Security Officer to agree controls.

Applying the classification system

The following considerations apply:

- Staff and delivery partners are responsible for ensuring that all information is looked after with care, to enable the business to function as well as meeting privacy needs.
- The majority of MoJ and wider government information will fall into the OFFICIAL tier; there is a significant step up to SECRET and TOP SECRET which are essential for national security and the very highest threat areas.
- OFFICIAL provides for a general and sufficient level of control of information (including for systems holding such information) which is not subject to heightened threat sources. Within this, there is flexibility to apply additional operational controls to reflect sensitivity.
- In most areas of MoJ activity at OFFICIAL, staff should continue to follow existing business instructions and procedures for handling information that apply to those activities. Such instructions should include provisions for identifying and dealing with more sensitive cases.
- The 'Working with Official information' desk aid and handling rules should be referred to when receiving, handling or creating information in any format, which is not routine or covered by general processes or instructions.
- Material at OFFICIAL does not require a marking to be applied, but must be protected in accordance with the handling rules and any local instructions. However, information assessed to be particularly sensitive must be marked OFFICIAL-SENSITIVE, giving a clear warning that strict control of access and special handling apply (see below).
- Staff are expected to comply with local instructions and minimum controls, but need to exercise common sense in situations where applying a control is not possible or would seriously hinder effective business or safety. In all but the most urgent cases, seek approval from your manager or the Information Asset Owner before adopting lesser controls. Decisions must be risk based, and the assessment must be recorded at the earliest convenient opportunity.
- Existing material with former protective markings including UNCLASSIFIED, PROTECT, and RESTRICTED does not need to be retrospectively reclassified. See the transition note in this guidance.
- Descriptors, such as PERSONAL or COMMERCIAL are no longer used. In exceptional circumstances or where the recipient might not recognise the sensitivity of the information being sent, authors may include 'handling instructions' in a document or email to draw attention to particular requirements.
- The security officer for your part of the MoJ should be consulted to agree controls if you receive,handle or otherwise process any information at SECRET or TOP SECRET.

Controls

At OFFICIAL, any local instructions or operating procedures should continue to be followed. These should assist staff in identifying any cases that require the OFFICIAL-SENSITIVE marking.

This guidance note and the desk aid entitled "Working with Official information" provide some general rules. You might also need to refer to local intranet pages or the handling rules if creating or processing any non-routine material.

Controls should be consistent with the minimum controls set out in the Handling Rules. These must be applied to all information within OFFICIAL and are adequate for most information, providing defence against the sort of threats

faced by a major company. These threats include, but are not limited to, 'hacktivists', single issue pressure groups, investigative journalists, competent individual hackers, potentially aggrieved participants or users of the justice system, and the majority of criminal individuals and groups.

Business areas or Information Asset Owners (IAOs) should review risks to their information, and ensure local procedures are in place, adopting additional controls where needed.

The Handling Rules document identifies additional considerations for some aspects of control. Business areas or IAOs might decide to adopt more robust controls in these areas, particularly for material marked OFFICIAL-SENSITIVE or where information is moved, transmitted or otherwise communicated outside of the secure office environment.

Controls should be applied proportionately for information which would previously have been 'unclassified'. Such information still needs looking after if it is required for the job, but might not require controls designed to provide confidentiality.

If IAOs or staff are considering classifying any new assets or reclassifying any existing assets as SECRET or TOP SECRET, they should consult their IA lead and security adviser, or with MoJ security in relation to technical threats, to determine whether a heightened threat might be present, and to agree necessary controls.

Marking of information

Marking is only needed for information which is OFFICIAL-SENSITIVE, SECRET or TOP SECRET. Classifications can be added to information in many different ways but the most important thing is that the marking is clearly visible to anyone using or receiving the information.

This could mean:

- Marking the top and bottom of documents, clearly, in CAPITALS, and CENTRED in the header and footer.
- Showing the marking in the subject line of emails:
  - Type OFFICIAL-SENSITIVE at the start of the subject line, in CAPITALS.
  - Remember to consider whether material that is sensitive needs to be sent, and whether it is safe or appropriate to send if the recipient is outside a secure government network.
  - You must not email anything at SECRET or above.
- Marking the front of folders or binders:
  - Apply clearly in a prominent position in CAPITALS.
  - Apply the highest classification of any of the contents.

Material that needs marking must be transmitted securely. The classification of contents must not be visible on an external envelope sent by post or courier.

Transition to the classification system

For information bearing the 'old' markings, the following guidance should be followed to ensure appropriate handling. Unless there are specific instructions to the contrary, staff are expected to maintain current levels of control and use existing IT systems on which information is currently held or processed.

The old protective markings do not automatically read across, particularly at CONFIDENTIAL.

- All material up to and including RESTRICTED becomes OFFICIAL.
- Much material at CONFIDENTIAL becomes OFFICIAL, but some might become SECRET.
- Only a limited amount of material at RESTRICTED needs marking as OFFICIAL-SENSITIVE.
- CONFIDENTIAL material moving into OFFICIAL is likely to require marking as OFFICIAL-SENSITIVE.

Old marking	New classification	Examples
UNCLASSIFIED or not protectively marked.	Treat as OFFICIAL (unmarked). Where controls prevent otherwise safe sharing of non-sensitive information, IAOs have some discretion to relax controls, provided any relaxations are specific to their assets and have no wider risk consequences, such as for the security of IT assets and government network code of connection.	Public notices and leaflets, published information, information that doesn't contain personal data or other sensitive content, and training materials.
PROTECT.	If information relates to general administration, treat as OFFICIAL (unmarked). Where used for personal data, maintain existing controls. Individual case records containing particularly sensitive content need to be marked OFFICIAL–SENSITIVE, though these instances may already be marked RESTRICTED or CONFIDENTIAL.	Documents containing personal data such as personnel records, citizen or offender case records, and general administration not intended for publication.
RESTRICTED.	If it relates to general administration, there should be a presumption that it can be treated as OFFICIAL (unmarked).	General administration, policy documents, commercial documents, or case records.
	You need to consider whether the subject matter is particularly sensitive and there is a need to rigorously enforce access controls, in which case material may additionally require handling or marking as OFFICIAL–SENSITIVE. Anything with this level of sensitivity might already have agreed handling constraints. If in doubt, discuss with the Information Asset Owner.	Particularly sensitive case records, contentious policy drafts and advice, and sensitive negotiations.
CONFIDENTIAL hard copy previously received from another Department.	Check with the author or originating Department. The presumption should be to treat as OFFICIAL–SENSITIVE and continue with current handling controls, unless there is a clear national security aspect or it relates to protected witnesses, in which case treat as SECRET. If you want to reproduce content in an electronic document, check the classification with the author or originating Department. See the note after the table.	
CONFIDENTIAL electronic copy received by secure government network or held on stand-alone system used for CONFIDENTIAL.	Continue to observe the operating instructions for the system you are using. Continue to use the secure government network for any reply, and use the marking applied by the original author. Otherwise, adopt controls for OFFICIAL–SENSITIVE. See the note after the table.	
SECRET.	Continue to treat as SECRET, subject to any formal review of the classification of the information assets involved in the particular area of activity. If hard copy, treat as SECRET and log, store, move and dispose of accordingly. If held on a stand-alone system currently rated at SECRET, treat as SECRET and observe the operating controls for the system.	Material relating to national security or counter-terrorism, and some protected witnesses.

Note: Electronic records marked CONFIDENTIAL should not be processed or saved on the MoJ existing standard networks such as DOM1 or Quantum, or on electronic document management systems unless or until the originator

or Information Asset Owner has issued revised guidance allowing the information to be handled at `OFFICIAL`, including `OFFICIAL-SENSITIVE`, and the system has been rated to hold material at `OFFICIAL`, with any additional access controls, or the system reclassified as `SECRET`.

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.