#Information classification, handling & security guide

All Ministry of Justice (MoJ) employees interact with information, and are responsible for its protection. Information security must be considered during the process of designing, maintaining, and securing the MoJ’s IT systems that are used to process information.

However, not all information warrants the strictest levels of protection. This is why information classification is so important to the MoJ – to ensure that the department can focus its security efforts on its most sensitive information. Information security must be proportionate to the security classification of the information, and must be considered throughout the information lifecycle to maintain its confidentiality, integrity, and availability.

##Classifying information

The three information security classifications the MoJ uses are OFFICIAL, SECRET, and TOP SECRET. This follows the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications).

Each information security classification has a minimum set of security measures associated with it that need to be applied. These security measures might change, depending on the information lifecycle stage.

|  |  |
| --- | --- |
| Classification | Description |
| **OFFICIAL** | All information related to routine business, operations, and services. If this information is lost, stolen, or published, it could have damaging consequences, but is not subject to a heightened threat profile. For regular, unsupervised access to OFFICIAL information, someone would be expected to have achieved [Baseline Personnel Security Standard (BPSS)](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard) assessment. |
| **SECRET** | Very sensitive information that requires protection against highly sophisticated, well-resourced, and determined threat actors. For example, where compromise could seriously damage military capabilities, international relations, or the investigation of a serious crime. For regular, unsupervised access to SECRET information, someone would be expected to have passed [National Security Vetting](https://www.gov.uk/guidance/security-vetting-and-clearance#applicant) Security Check (SC) clearance. In exceptional circumstances, someone with BPSS might be granted occasional supervised access to UK SECRET assets, or be required to work in areas where SECRET or TOP SECRET information might be overheard. |
| **TOP SECRET** | Exceptionally sensitive information that directly supports, or threatens, the national security of the UK or its allies, and requires extremely high assurance of protection from all threats. |

Securing the MoJ’s information must be done with a combination of information security measures:

|  |  |
| --- | --- |
| Type of Measure | Description |
| **PERSONNEL** | Personnel should be aware of their security responsibilities and in turn acquire security clearances and undertake training to support the MoJ’s information security objectives. |
| **PHYSICAL** | Tangible measures that prevent unauthorised access to physical areas, systems, or assets. |
| **TECHNICAL** | Hardware or software mechanisms that protect information and IT assets. |

It is important to understand that security classification is determined by the level of risk in case of loss or unauthorised access, and not by the type of information.

It is the responsibility of the Data Owner to classify the data.

* Most production data is OFFICIAL information. Within this, some production data might be classified as SECRET information.
* Most personal data is OFFICIAL information. Within this, some personal data might be classified as SECRET information if it meets the risk threshold defined.

The table below sets out the definitions for each security classification, as well as whether it is necessary to explicitly mark a piece of information with its classification type.

|  |  |  |
| --- | --- | --- |
| Classification | Definition | Marking |
| **OFFICIAL** | All information related to routine public sector business, operations and services. |  |
|  | Almost all personal information falls within the OFFICIAL classification. |  |
|  | OFFICIAL-SENSITIVE is not a separate security classification. It should be used to reinforce the need to know principle, beyond the baseline for OFFICIAL. | OFFICIAL data does not need to be marked except where SENSITIVE, and must be marked OFFICIAL-SENSITIVE. |
| **SECRET** | Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime. | Must be marked |
| **TOP SECRET** | Exceptionally sensitive information that directly supports (or threatens) the national security of the UK or its allies and requires extremely high assurance of protection from all threats. | Must be marked |

Additional information on how to manage information is described in the [Information Asset Management Policy](/guidance/knowledge-information/managing-information/).

Information security classification may change throughout the information lifecycle. It is important to apply appropriate security classifications and continually evaluate them.

The consequences of not classifying information correctly are outlined below:

* Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.
* Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.
* Incorrect disposal can lead to unauthorised access to information. Disposal of information should be done using approved processes, equipment or service providers.

##OFFICIAL and OFFICIAL-SENSITIVE

All of the MoJ’s information is, at a minimum, OFFICIAL information. It is very likely that the information you create and use in your MoJ day-to-day job is OFFICIAL information.

Examples include:

* Routine emails you send to your colleagues.
* Information posted on the intranet.
* Supplier contracts.
* Information and data you use to build a database, such as database secrets, record types, and field types.
* Most production data.
* Most non-production data.

OFFICIAL means that the MoJ’s typical security measures are regarded as sufficient.

OFFICIAL-SENSITIVE whilst not a formal classification, should be used sparingly, so that its effectiveness is not weakened. This is especially important when you consider that OFFICIAL is already well-protected.

Use OFFICIAL-SENSITIVE when you want to remind users to be careful when handling information. This asks them to use extra care, beyond what is expected for the baseline OFFICIAL classification.

##SECRET

The threshold for classifying information as SECRET information is very high. It is unlikely that you will encounter SECRET information in your day-to-day job.

SECRET information should not usually be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is SECRET, contact the Cyber Assistance Team (CAT) immediately: [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

To help decide whether some information should be classified as SECRET, ask yourself a simple question:

If a hacker gained unauthorised access to the information, could it compromise the security or prosperity of the country?

The answer is most likely No. In that case, you should consider using the OFFICIAL classification.

##TOP SECRET

If the threshold for classifying information as SECRET is very high, the threshold for classifying information as TOP SECRET is extremely high. It is very unlikely that you will encounter TOP SECRET information in your day-to-day job.

TOP SECRET information should not be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is TOP SECRET, contact the Cyber Assistance Team (CAT) immediately: [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

To help decide whether some information should be classified as TOP SECRET, ask yourself a simple question:

If a hacker gained unauthorised access to the information, would it directly and immediately threaten the national security of the country?

The answer is most likely No. In that case, you should consider using the OFFICIAL or SECRET classification, as appropriate.

##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](mailto:OperationalSecurityTeam@justice.gov.uk)) whether additional actions are required to protect the material.

##Reclassification examples

When deciding whether it is appropriate or desirable to reclassify information, a useful model is to consider what audience might get value from accessing the information. For example, if a hostile country might want the information, then the information might well be best classified as SECRET. Alternatively, a reclassification decision might be required as a result of changing threat advice from intelligence agencies.

##Example 1

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as OFFICIAL, with the SENSITIVE handling caveat.

A user wishes to share a copy of the report as-is with their team. They cannot remove the handling caveat without prior discussion and agreement from the asset owner.

##Example 2

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as OFFICIAL, with the SENSITIVE handling caveat.

A user wishes to share a subset of the report with their team. In particular, the report is substantially re-worked to remove all the private information. The user becomes the owner of this new asset. They are responsible for this new asset. They can decide that the SENSITIVE handling caveat is not required.

The original report retains its OFFICIAL classification and SENSITIVE handling caveat.

##Example 3

An asset owner creates a report. The report contains information about plans to handle a pandemic. The asset owner decides that the report should be classified as OFFICIAL, with the SENSITIVE handling caveat.

A user reviews the report. They realise that the information could potentially compromise the security or prosperity of the country. They decide to increase the classification of the report, and treat it as SECRET. They discuss this decision with the asset owner, so that the original report is correctly reclassified.

##Handling and securing information

The [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) is the most comprehensive guide on the security measures necessary for each of the three security classifications, including measures related to the following:

* Personnel (administrative) security.
* Physical security.
* Technical (information security).

The following sections set out the minimum measures you need to consider when handling and securing information within the different levels of classification.

##Handling and securing OFFICIAL and OFFICIAL-SENSITIVE information

|  |  |  |
| --- | --- | --- |
| Type | Measure | Example |
| **PERSONNEL** | Make sure all MoJ staff including contractors undergo baseline security clearance checks. | A contractor working with the MoJ Security Team must undergo a baseline background check (i.e. BPSS check) at minimum. Refer to [Security Vetting Guidance](/guidance/hr/recruitment/security-vetting/). |
| **PHYSICAL** | Make sure that you lock your screen before you leave your desk. |  |
|  | When working in an unsecured area, for example when working remotely, think about whether unauthorised people might be able to eavesdrop on your conversations, or look over your shoulder at your screen. |  |
|  | The MoJ has additional requirements when moving assets which can be found in the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications). | A software developer working from a flatshare should take calls in private, and use headphones and a privacy screen. |
|  | Transferring information from one location to another requires planning and preparation, including a risk assessment. More information on this is available in the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications), and from your manager. | A technical architect working on the requirements for a new MoJ platform should lock their laptop before leaving their desk. |
| **TECHNICAL** | Protect information at rest by using appropriate encryption. | In the development of a new cloud-hosted solution, the following criteria should be considered: remote access connections and sessions are encrypted using an appropriate VPN; information stored at rest on end user devices and the cloud is encrypted; information in transit between the end user and the cloud service, such as payment services, is encrypted; and the cloud service used is a [Digital Marketplace (GCloud)](https://www.digitalmarketplace.service.gov.uk/g-cloud) service. |
|  | Appropriate encryption is also necessary when protecting information in transit. | When using any services over the PSN, make sure you fully read the agreements that you make with the service provider for details and definitions about the data you use or transfer using the service, to ensure you understand the risks to compliance, confidentiality, integrity, and availability. |
|  | [Digital Marketplace (GCloud)](https://www.digitalmarketplace.service.gov.uk/g-cloud) services can be used for OFFICIAL information. |  |
|  | You must not use removable media such as an USB memory stick unless it is unavoidable. When you have to use one, it must be MoJ issued, encrypted so that the effects of losing it are minimised, and the data erased securely after use. |  |

**Note:** Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) for further guidance.

##Handling and securing SECRET information

|  |  |  |
| --- | --- | --- |
| Type | Measure | Example |
| **PERSONNEL** | Make sure employees and contractors undergo Security Check (SC). | A contractor working with the MoJ Security Team must have at least SC before being allowed to access SECRET information. |
| **PHYSICAL** | Consider using multiple layers of security to protect SECRET information. SECRET information should be held on a secure computer network which is physically isolated from unsecured networks and the internet. | Imagine you are moving locations for a server used to host SECRET information. The encrypted server is secured in a locked and monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after relevant parties, including the data owner, line manager, and the system owner, have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two SC-cleared individuals, for example, employees of a specialised commercial courier company. |
|  | Transferring SECRET information from one location to another requires planning and preparation, including the completion of a Risk Assessment and the use of SC-cleared personnel. More information on this is available in the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) and from your manager. |  |
| **TECHNICAL** | SECRET information at rest should be protected with very strong encryption. Contact the MoJ Security Team for more information: [security@justice.gov.uk](mailto:security@justice.gov.uk). |  |
|  | Care should be taken to ensure that SECRET information in transit is only shared with defined recipient users through assured shared infrastructure or using very strong encryption. |  |
|  | SECRET information should be processed on IT systems which have been approved for the SECRET threat model. Advice on what commercial IT systems meet this requirement is available from the MoJ Security Team: [security@justice.gov.uk](mailto:security@justice.gov.uk) |  |

**Note:** Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) for further guidance.

##Handling and securing TOP SECRET information

|  |  |  |
| --- | --- | --- |
| Type | Measure | Example |
| **PERSONNEL** | Ensure employees and contractors undergo Developed Vetting (DV) security clearance checks. | A contractor working with the MoJ Security Team should have at least DV clearance before being allowed to access TOP SECRET information. |
| **PHYSICAL** | Handling and storing TOP SECRET information requires exceptional planning, monitoring, and record-keeping. | Imagine you are moving locations for a server used to host TOP SECRET information. The encrypted server is secured in a locked and continuously monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after you, your manager, and senior managers have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two DV-cleared individuals, for example, employees of a specialised commercial courier company. When it happens, local police may need to be informed and involved in providing an additional layer of security. |
|  | Working remotely with TOP SECRET is not permitted due to the extreme sensitivity of the information. |  |
|  | Transferring TOP SECRET information from one location to another requires even greater planning and preparation than for SECRET information, including the completion of a Risk Assessment by senior management and the use of DV-cleared personnel. More information on this is available in the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) and from your manager. |  |
| **TECHNICAL** | When physical security measures cannot be used, TOP SECRET information at rest should be protected with extremely strong encryption. Contact the MoJ Security Team in these circumstances: [security@justice.gov.uk](mailto:security@justice.gov.uk). |  |
|  | Care should be taken to ensure that TOP SECRET information in transit is only shared with defined recipient users through accredited shared infrastructure or using extremely strong encryption. |  |
|  | TOP SECRET information should be processed on IT systems which have been approved the TOP SECRET threat model. Advice on what commercial IT systems meet this requirement is available from the MoJ Security Team: [security@justice.gov.uk](mailto:security@justice.gov.uk). |  |

**Note:** Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) for further guidance.

**Note:** For further information on statutory disclosures and transfer to national archives, please refer to the [HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications).

##Contacts

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

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).