DWP Security Classification Policy

Policy updated on 12 January 2024

1. Overview

1.1 This DWP Security Classification Policy outlines the principles that DWP will apply to the classification and handling of its data using the baselines set by the wider HMG (His Majesty’s Government) Government Security Classifications Policy (GSCP).

1.2 The GSCP has three tiers of classification – OFFICIAL, SECRET and TOP SECRET. Each of these tiers provides a minimum set of protective controls for each classification level based on the consequences of the information being compromised, lost, or misused.

1.3 The majority of DWP’s information falls into the OFFICIAL tier so this policy focuses on how to handle and protect this information. Any information which, if compromised and likely to cause moderate damage to the work or reputation of DWP, must be marked -SENSITIVE (OFFICIAL-SENSITIVE)

2. Scope

2.1 The DWP Security Classification Policy applies to any information that is created, handled, stored, disposed or moved (sent and received) by DWP and affects all DWP employees, agents, contractors, consultants, suppliers, and business partners (referred to in this policy as ‘users’). This includes all information concerning the department’s business and applies to all formats (verbal, electronic and hard copy).

2.2 Information assets received from third parties outside of DWP must be treated as departmental assets and protected in accordance with this policy.

2.3 All information regardless of classification tier must be protected against a broad range of threats including from individuals, groups, or countries which have the ability or intent to impact the security of an asset.

2.4 Special handling measures apply to information classified as SECRET (highly sensitive information that if compromised could threaten life, or seriously damage the UK's security and/or international relations) and TOP SECRET (exceptionally sensitive information that directly supports or informs the national security of the UK or its allies).

2.5 There may be some areas of DWP that are provided with separate instructions concerning the handling of highly sensitive assets including that classified as SECRET and TOP SECRET. Please visit the Rosa site for more information.

3. Definitions

Additional markings – Additional markings can be added in conjunction with a classification to indicate the nature or source of the information, limit access to specific user groups, and indicate whether additional protective controls are required to protect the information. There are several different types of additional markings, including: handling instructions, descriptors, codewords, prefixes, and national caveats. Information creators should apply additional markings and handling instructions to help users understand information sensitivities and specific restrictions on information sharing.

Handling instructions – Markings which are used within a classification tier to provide additional instructions to users when handling information; they help to protect a range of information with varying sensitivity against a classification's broad threat profile. These do not change the classification but provide more detail around how it can be handled, how widely it can be shared and how it should be protected. Handling instructions are applied after the classification.

Descriptors – These are terms applied by users to easily identify certain categories of information with special sensitivities and highlight additional access restrictions. Descriptors are not additional classifications and do not need to be applied to all documents. They are applied after the classification and after the handling instruction.

Aggregation [of data] – this is a term which relates to combined data assets from multiple sources, or a sole source over time, e.g., multiple pieces of data about an individual, therefore making them identifiable, or multiple records of minimal information in which aggregating the data can make it of higher value. This will not usually affect the classification of the different elements but a new piece, or set, of data formed may need to be classified at a higher level.

Information asset – any item or collection of information which is of value to DWP.

Information creator – The person who has the authority over the creation or distribution of an information asset, and is responsible for the classification, handling, sharing and disposal of that information.

Threat/malicious actor(s) – a person/entity/state that has the capability and intent to impact the security of an asset (including people, property, or information).

4. Policy Statements

4.1 All information that DWP creates, handles, stores, and moves to deliver services and conduct government business is of value and must be protected and handled appropriately.

4.2 Each user (as defined in 2.1) has a duty to maintain confidentiality and must safeguard all DWP and wider government information that they access and/or share, irrespective of the classification marking and whether it is marked or not. Users must be provided with appropriate training as everyone is accountable for their own security decisions when classifying information.

4.3 Information must be handled and distributed based on a genuine need-to-know basis, balanced with the business requirement to share, dependant on the sensitivity of the information.

4.4 Consideration must in particular be given to protecting technically sensitive information such software configuration, patching, and technical vulnerabilities etc., as this may increase the threat to the department and could potentially put DWP assets at risk if disclosed.

4.5 Access to information must be kept to a minimum to conduct official work and limited to those with a legitimate business need who have the appropriate personnel security clearance to access such information, in line with the User Access Control Policy.

4.6 Each individual who creates or shares any information is responsible for determining the classification, handling, distribution, and disposal of that information, considering any source material and its sensitivity, and those people who need to know.

4.7 Where it is possible, users can apply the appropriate classification label to their work. However, please see 4.11 in relation to communications with customer facing content.

4.8 Users must comply with the Information Management Policy principles in the creation, storage, usage, and disposal of information. Only DWP approved devices, systems, and networks, and those of its suppliers, must be used.

4.9 Information received from or exchanged with external partners must be protected in accordance with the relevant legislative or regulatory requirements (as outlined at 5.2) including any international agreements and obligations and the originator’s handling instructions.

4.10 Users are responsible for ensuring that they are aware of their surroundings when working remotely and must take adequate precautions to protect themselves and DWP information when working somewhere other than their usual location as outlined in the Remote Working Security Policy.

4.11 Any communications with customers, either via email or hardcopy are not required to be marked with a classification. However, staff should still take care to protect the data accordingly.

4.12 Users personal information (e.g., payslips) does not require a classification. Users are responsible for the security of their own information after it has left DWP systems.

5. Classification Tiers

Working at OFFICIAL

OFFICIAL – most information that is created, processed, sent, or received which could cause limited, or no damage if compromised. This includes information that has been cleared for publication and routine operational, policy and service information that is not intended for public release but is unlikely to be of interest to threat actors. Multiple records or aggregated pieces of OFFICIAL information may require additional controls.

5.1 All information that is created or processed by DWP is OFFICIAL by default unless it is classified at a higher level.

5.2 A wide range of personal data (including bulk data) can be handled at OFFICIAL, in line with UK (United Kingdom) GDPR (General Data Protection Regulation) and DPA (Data Protection Act) 2018 legal obligations.

Working at OFFICIAL-SENSITIVE

OFFICIAL information marked -SENSITIVE – this marking is for the limited distribution of more sensitive OFFICIAL information on a need-to-know basis. When OFFICIAL information is marked -SENSITIVE this can lead to moderate damage if compromised and will likely be of interest to threat actors due to its sensitivity. This is referred to as OFFICIAL-SENSITIVE throughout this policy.

5.3 OFFICIAL information or material must be marked “OFFICIAL-SENSITIVE" if the compromise of such is likely to:

- Cause damage to the work or reputation of DWP and/or HMG.
- Cause moderate damage to the UK’s international reputation, economy, or relations with an international partner.
- Cause moderate harm or distress to a group of people.

- Be of interest to threat actors due to its sensitivity or topical significance.

If using the “OFFICIAL-SENSITIVE” marking, it should be included in the header and footer of a document and in the subject line of an email where possible.

5.4 Information with the OFFICIAL-SENSITIVE marking may be subject to additional controls to protect need-to-know sensitive data and consideration must be given to distribute only where necessary.

5.5 Individual business areas may have separate instructions concerning the handling of especially sensitive information assets. In determining whether a -SENSITIVE marking should be applied, consideration should be given to Special Category Data and Criminal Offence Data as defined by UK GDPR, children’s data, and large aggregated data sets. The risks around aggregating data increase where more information is added, this must therefore be carefully managed to prevent data loss.

Working at SECRET

The SECRET classification tier is used for sensitive information that requires enhanced protective controls, the use of appropriately assured IT (Information Technology) (such as the Rosa capability) and heightened user discretion to guard against compromise. A compromise of SECRET information has severe implications, and it could threaten the lives of individuals or groups and seriously damage the UK’s security resilience and/or international relations, its financial security and/or impede the investigation of serious and organised crime.

5.6 Before gaining access to SECRET and TOP SECRET material, users must seek the appropriate level, and approval, of National Security Vetting.

5.7 Users who handle SECRET information must exercise the appropriate discretion to ensure that they are not overlooked or overheard as per the baseline behaviour expectations.

5.8 The Information Creator is responsible for assessing the potential impact of a compromise of information and the expected threat profile to determine whether information is SECRET. They are responsible for marking the information, as well as monitoring and assessing whether any situational factors surrounding the information warrants updating the classification. Everyone who processes SECRET information assets on behalf of HMG (employees, delivery partners and third-party suppliers) is personally accountable for handling, distributing, and disposing of the information responsibly in line with HMG policy.

5.9 If the context around an information asset has changed, it is the information creator’s responsibility to re-classify and re-mark the material by assessing the impact of compromise and the expected threat. It also is the responsibility of the Information Creator to inform recipients if classified information they have provided has been downgraded to OFFICIAL. They should also consider applying an additional marking to the downgraded information such as -SENSITIVE and provide details in writing.

5.10 Information handling and security requirements of SECRET data must be clearly communicated to recipients, who must have a defined need-to-know reason to have the information.

Working at TOP SECRET

The TOP SECRET classification tier is reserved for the most sensitive information assets that directly support or inform the national security of the UK or allies AND require extremely high assurance of protection from the most serious threats with the use of Secure Isolated Networks and highly secure physical infrastructure. A compromise could cause exceptionally grave damage; it could cause widespread loss of life or threaten the security or economic wellbeing of the country or friendly nations.

TOP SECRET information justifies the most stringent behavioural, procedural, and technical controls to protect against the highest capability of threat actors and reduce the chances of an intentional or unintentional compromise. The exceptionally grave damage that would occur if compromised, combined with the enhanced capabilities expected from the most capable and well-resourced threat actors, is what distinguishes TOP SECRET classified information.

5.11 Users who handle TOP SECRET information must exercise the appropriate discretion to ensure that they are not overlooked or overheard as per the baseline behaviour expectations.

5.12 The Information Creator must assess the potential impact of a compromise of information and the expected threat profile to determine whether information is TOP SECRET. They are responsible for marking TOP SECRET information which must only be used for the most sensitive assets. Before users can access TOP SECRET material for the first time, they must be briefed by their security teams on how to handle the information and equipment in a careful and secure manner. It is the responsibility of the security team to ensure their users have routine refresher training thereafter.

5.13 At TOP SECRET, information handling and security requirements must be clearly communicated to recipients and shared on a strict need-to-know basis.

6. Responsibilities

6.1 Line managers must demonstrate and promote good security behaviours as they are responsible for ensuring their employees understand and apply security classifications and handling instructions correctly.

6.2 Line managers must ensure that their employees are aware of their responsibilities for information classification, undertake the necessary training, understand security requirements and how legislation relates to their role, including the potential sanctions (criminal or disciplinary) that may result from inappropriate use or behaviours.

6.3 Employees must immediately report any suspected or actual compromise of OFFICIAL, OFFICIAL-SENSITIVE, SECRET and TOP SECRET information via the DWP Place portal. This includes any loss, theft, uncleared access or tampering of information or assets.

7. Compliance

7.1 All users have a responsibility towards protecting departmental information and must be aware of, and comply, with DWP's security policies and standards.

7.2 Many of DWP's employees and contractors handle sensitive information daily and so need to be enacting minimum baseline behaviours appropriate to the sensitivity of the information-see annex C for further details.

7.3 Information security is important, and breaches may, in the most severe circumstances, result in dismissal. All breaches must be reported in accordance with section 6.3 and the consequences of not reporting a breach, or suspected breach, may lead to disciplinary procedures being considered.

7.4 If for any reason users are unable to comply with this policy, they must discuss this with their line manager in the first instance for resolution. If unsuccessful, then consult the Security Advice Centre who provide advice on escalation/exception routes.

7.5 If there are technical or logistical issues which means the policy cannot be complied with, An exception to policy may be considered in certain instances. This helps to control the risk of non-compliant activity and reduce potential security incidents. If an individual is aware of an activity that falls into this category, they should notify the security policy team immediately.

Other Useful Documents

- Email Policy
- DWP Standards of Behaviour Policy
- Remote Working Policy
- Information Management Policy
- Examples of OFFICIAL and OFFICIAL-SENSITIVE information

Annex A: Additional Markings- Handling Instructions and Descriptors

Handling Instructions	**Description**
DWP Use Only	Information that should only be shared within the named organisation(s). Users should seek permission from the creator before sharing outside the named organisation(s).
HMG Use Only	Information that should only be shared with other HMG departments [*/ with organisations using gov.uk domains / with wider public sector organisations*], and not with external partners. *Not for use with TOP SECRET
Non-visible	Information that is still managed and protected according to its classification (e.g., OFFICIAL) but no visual marking displayed. This is to be applied to any documentation that is sent out to customers.

These handling instructions are the ones most commonly used within DWP. A list of additional markings and descriptors as defined by central government can be found on page 15 of the Government Security Classification Policy.

Annex B - Examples of OFFICIAL and OFFICIAL-SENSITIVE

OFFICIAL

- Routine, non-personal information exchanges related to delivering the Department’s business,
- Non-contentious policy discussions, proposals and draft speeches
- Internal management information, such as planned procedures, training opportunities or operational and financial management of the department,
- General communications with our providers, such as data processors.
- Freedom of Information casework (as well as final published replies)
- Routine information exchanges and discussions with foreign (non-UK) governments.
- General policy and operations data that has no significant impact on the Department and its operations.
- General information on employers, providers, employment, education, and training opportunities.

OFFICIAL-SENSITIVE

- Sensitive ministerial submissions and advice,
- Discussions about proposed estate changes or office closures.
- Sensitive internal policies awaiting consultation with trade unions.
- Operational data relating to pay negotiations, major security or business continuity issues.
- Sensitive assets, such as issues concerning national security, cryptography, architecture, software and security artefacts.
- Special Customer Records and issues relating to the policy and application and processing of such records.
- Policy formulation or proposals on sensitive issues,
- Aggregated personal information about multiple identifiable (for example they can be identified readily from that data) individuals, including claimants, employees and customers, the disclosure of which could cause harm or distress to those persons. Thus, a list of names and NINOs if disclosed would not cause harm, but a list of individuals with benefit details, and addresses, and dates of birth, and so on, would be OFFICIAL-SENSITIVE.
- Correspondence relating to the award of state honours.
- Investigations and civil or criminal proceedings against employees of the department, and investigations or proceedings against a departmental supplier or provider.
- Information where its handling is subject to statutory or other obligations, for example under Payment Card Industry standards, certain (security) exemptions under the FoI (Freedom of Information) Act.

Annex C - Baseline controls and behaviours to support protecting data

Detailed guidance on baseline actions individuals should take can be found on GOV.UK at working with OFFICIAL.