Security Policy – Security Classification Policy

Chief Security Officer

Department for Work & Pensions

ThinkSecure

This Security Classification Policy is part of a suite of policies designed to promote consistency across the Department for Work and Pensions (DWP) and supplier base with regards to the implementation and management of security controls. For the purposes of this policy, the term DWP and Department are used interchangeably.

Security policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-standards.

Security policies cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

Table of Contents

Table 1 – Terms 2

Policy Title 4

Overview 4

Scope 4

Definitions 5

Policy Statements 6

Accountabilities and Responsibilities 9

Compliance 10

Policy Title

DWP Security Classification Policy

Overview

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).

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.

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)

Scope

This policy applies to:

a) 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).

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

c) 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.

d) 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).

e) 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.

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).

Policy Statements

1.1. 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.

1.2. Each user (as defined in SCOPE) 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.

1.3. 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.

1.4. 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.

1.5. 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**.

1.6. 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.

1.7. Where it is possible, users can apply the appropriate classification label to their work. However, please see 1.11 in relation to communications with customer facing content.

1.8. 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.

1.9. Information received from or exchanged with external partners must be protected in accordance with the relevant legislative or regulatory requirements (as outlined at 2.2) including any international agreements and obligations and the originator's handling instructions.

1.10. 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**.

1.11. 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.

1.12. 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.

2. 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.

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

2.2. A wide range of **personal 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.

2.3. 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.

2.4. 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.

2.5. 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.

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

2.7. 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**.

2.8. 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.

2.9. 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.

2.10. 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.

2.11. 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**.

2.12. 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.

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

Accountabilities and Responsibilities

a) The DWP Chief Security Officer is the accountable owner of the DWP Security Classification Policy and is responsible for its maintenance and review, through the DWP Deputy Director for Security Policy and Data Protection

b) 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.

c) 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.

d) 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.

Compliance

a) All DWP employees, whether permanent or temporary (including DWP's contractors) have security responsibilities and must be aware of, and comply with, DWP's security policies and standards.

b) 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.

c) Security incidents happen where there has been a deliberate attempt, whether successful or not, to compromise DWP assets such as information, people, IT, premises, or any accident resulting in loss of DWP assets.

d) Information security is important, and breeches can, in the most severe circumstances, result in dismissal. All breeches must be reported in accordance with **Accountabilities and Responsibilities**, section d). Not reporting a breach, or suspected breach, may lead to disciplinary procedures being considered.

e) Where systems and/or applications do not allow for an automatic classification to be applied (e.g., non-Microsoft Office 365 systems) the users should assign the correct classification marking themselves manually. If there are technical and/or logistical issues that prevent this from being done, then this should be raised as an exception to the policy (see paragraph h).

f) DWP's Security and Data Protection Team will regularly assess for compliance with this policy and may need to inspect physical locations, technology systems, design and processes and speak to people to facilitate this. All DWP employees, agents, contractors, consultants, business partners and service providers will be required to facilitate, support, and when necessary, participate in any such inspection. DWP Collaboration and

Communication Services will use software filters to block access to some online websites and services. **DWP Employee Privacy Notice**.

g) If for any reason users are unable to comply with this policy or require use of technology which is outside its scope 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.

h) 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.
