DWP Security Classification Policy

Contents

Introduction

Individuals who undertake work of the Department for Work and Pensions (DWP), have a personal responsibility to handle the DWP’s information in accordance with DWP’s Standards of Behaviour Policy. Employees must make sure that they are familiar with that policy and the general guidance on handling information assets. If individuals fail to follow the rules, not only do they risk disciplinary action in some cases, they may cause distress to claimants, colleagues, DWP’s suppliers, or break the law, as well as damage DWP’s reputation, and incur unnecessary costs for the taxpayer.

Government departments follow agreed principles for the classification of information. These principles describe the way that different types of information are to be handled, and whether any must be marked to indicate special handling arrangements.

The Government Security Classifications is simple with only 3 tiers of information classification – OFFICIAL, SECRET and TOP SECRET. This means that the majority of DWP’s information falls into the OFFICIAL tier.

Scope

This policy applies to all DWP employees and suppliers who handle DWP’s information assets, whether those relate to the administration, internal policies or personal data, and regardless of whether these relate to employees, suppliers or claimants.

This policy describes the way that DWP has decided to protect its information, and when to apply markings if required.

Principles

The Government Security Classification scheme came into force on the 2 April 2014 and from this point forward the former markings must not be used for any new or amended information. The current scheme does not need to be applied retrospectively to information marked under the old scheme unless that information is modified.

The policy covers the storage, processing, transmission and transport (electronic and hard copy) of information assets.

The term ‘information assets’ includes any information concerning the DWP’s business, whether it relates to individual claimants, employees or suppliers, or other information and applies irrespective of the format in which it is held.

Decisions on the handling and classification of particular information assets are to be taken by individuals where they are responsible for the creation or authorship of such information.

Only use the DWP’s IT equipment and related supplier systems to store and process information.

All employees and suppliers have a duty of confidentiality and responsibility to safeguard all DWP information and data, irrespective of whether it is securely marked or not.

No markings other than OFFICIAL-SENSITIVE may be used for information within the OFFICIAL tier.

Handling of Information Assets

All information has value, regardless of whether it has a visible protective marking or not and must be treated with appropriate care.

The requirements for the secure handling of any of DWP’s information assets is as follows:

- DWP’s information must only be accessed, obtained or transferred where the employee or supplier has a legitimate business reason for doing so. Employees and suppliers are personally accountable for demonstrating that they are entitled to access any information where they have done so,
- Information must only be sent, shared with or copied to others where they are entitled to be given access to that information.
- Where an information asset cannot be physically marked, it must still be treated in accordance with the handling requirements of this policy, depending upon its sensitivity or value.
- Where information assets have to be sent outside DWP the most secure method must always be used. E-mail over the internet may be used in circumstances where this is allowed for in-line with DWP policy.
- Hard copy sensitive or valuable information assets must be securely locked away when not in use. Apart from documents already in the public domain none of DWP’s information must be left on unoccupied desks in offices overnight, in accordance with the clear desk standard.

- Information assets received from third parties outside DWP must be treated as if they were DWP assets, and protected in accordance with the relevant sections of this policy.

These are only general rules; some areas of DWP may be provided with separate instructions concerning the handling of especially sensitive assets.

Marking of Sensitive Assets

Although most information within the OFFICIAL tier will not be marked, the handling caveat OFFICIAL-SENSITIVE must be used for information of particular sensitivity and value to DWP, where the attendant risks make it necessary to expend effort on a broader range of controls to protect or keep it secure. Email communicated within DWP, or to other government Departments and Agencies, must include OFFICIAL-SENSITIVE as a handling marking when applicable. This must be written in the subject line of the email. Physical information must be physically marked with this caveat.

Although providers are not required to use protective markings where these are not stipulated in contracts, nevertheless the contracts do emphasise the requirement to securely protect DWP data. It is for DWP to determine and instruct suppliers on these requirements where applicable.

Handling information which is ‘OFFICIAL’ (unmarked)

This includes the majority of information in DWP and must be the default position.

Handling Information which is ‘OFFICIAL-SENSITIVE’ and marked

This is the minority of DWP’s information, it has particular sensitivity and value, it requires special handling measures above and beyond those given to unmarked OFFICIAL information, to protect the confidentiality and integrity of the information.

Further Information

If there are any questions regarding this guidance, please contact your line manager or where appropriate, the Authority.