IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

# DWP Information Security Policy

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

## Version Control Table

| Version | Date | Major Change |
|---|---|---|
| 1 | 27/06/2018 | |
| | | |
| | | |
| | | |
| | | |

## Updating policy

This policy will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

# Contents

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

## What is the DWP Information Security Policy?

The Information Security Policy sets out how DWP and its delivery partners/suppliers manage and protect our information. It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity (accuracy) and availability of information within our organisation.

## Why does DWP need an information security policy?

Having an information security policy is government and industry best practice. It helps to prevent theft, loss and unauthorised access or disclosure of electronic files, paper documents and online services.

## Who does the Information Security Policy apply to?

Anyone who has a business need to handle DWP information or equipment, including all DWP employees, agents, contractors, consultants and business partners.

## 1. Background

1.1. DWP is committed to ensuring that effective security arrangements are implemented and regularly reviewed to reduce the threats and manage risks to:

- The information that DWP collects, creates, uses and stores,
- DWP employees, claimants and citizens,
- DWP's physical assets and resources,
- DWP's digital, IT and communication systems, and
- Premises that DWP uses to accommodate its operations, people, and visitors

## 2. Scope

2.1. This overarching policy provides direction for all DWP information security policy and the standards and controls which underpin it.

2.2. This policy aligns with and is based on the ISO 27000 series and in particular ISO27001 techniques and principles and ISO27002 requirements and will be used to inform DWP future consideration of an Information Security Management System. Standards drawn from the ISO 27000 series will be applied and communicated as needed.

2.3. This policy applies to all aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store, process, transmit or receive information.

2.4. This policy applies to all DWP data, and any data that DWP is processing for other data controllers.

2.5. This policy applies to:

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

- All DWP employees - who should understand their responsibilities in using the Department's information assets including its systems. DWP Employee non-compliance with this policy may result in disciplinary consequences.
- DWP staff engaged in designing and implementing new technology solutions, who must reflect the policy requirements into design and build.
- DWP Contracted suppliers that handle/access/process Authority Data. Contracted suppliers must provide the security measures and safeguards appropriate to the nature and use of the information. All Contracted suppliers of services to the DWP must comply, and be able to demonstrate compliance, with the Department's relevant policies and standards.

## 3. Accountabilities

3.1. The Chief Security Officer is the accountable owner of the DWP Information Security Policy and is responsible for its maintenance and review, through the Head of Security Policy, Governance & Resilience.

3.2. Any exception to the Information Security Policy must be risk assessed and agreed by the Chief Security Officer.

## 4. Policy Statements

4.1. DWP recognises all information has value and sets out in this Information Security Policy how it safeguards DWP information through security standards, and protects the systems, equipment and processes that support its use through applying controls and a control environment.

4.2. This Information Security Policy defines how we achieve information security through implementing supporting standards and controls to protect information;

- Confidentiality: by restricting access to authorised users;
- Integrity: by making sure that the information is always accurate and complete;
- Availability: by making sure that the information is available to authorised users when required.

4.3. DWP protects its systems and processes through standards that are applied proportionately, based on formal risk assessments, continually reviewed, and align with the following:

- The Data Protection Act (1998) and the HMG Security Policy Framework.
- Related HMG standards and Good Practice Guidance for protecting personal data and managing information risk including those of CESG.
- The ISO27001 techniques standard, the ISO27002 code of practice, and other ISO 27000 standards and security best practice.
- Contractual obligations.
- Relevant Codes of Connection.
- Other applicable legislation.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

4.4. DWP requires Contracted Suppliers that generate, access and process Authority Data to take a similar proportionate, risk based approach to information security in accordance with the relevant DWP Security Policies and Standards which adopt and apply ISO 27001 Standards and the Cyber Essentials.

4.5. DWP applies the Baseline Personnel Security Standard (BPSS) in employee recruitment and requires Contracted Suppliers to apply similar or identical controls where applicable. DWP applies Human Resources policies in the protection of its information and requires Contracted Suppliers apply similar personnel security policies.

4.6. DWP will ensure that DWP and its suppliers implement and operate information security in accordance with the organisational standards and procedures to mitigate against breaches of legal, statutory, and embed contractual obligations related to information security.

4.7. DWP systematically monitors and measures information security performance against its own and cross government metrics. DWP develops and improves information security policies and standards to provide sufficient protection for information by addressing identified risks, and consistent with central HMG standards and guidance. New information security standards and procedures will be communicated to employees and others on a regular basis.

## 5. Responsibilities

5.1. DWP's Information Security Policies and Standards provide appropriate protection for personal and sensitive personal data as a result of effective implementation of the following responsibilities:

5.1.1. Governance and Compliance Functions

5.1.1.1. Enable management of information security through developing governance structures in an organisation that directs and manages information security,

5.1.1.2. Provide control of information security risks within DWP to acceptable levels by risk management and the use of protective marking and other controls,

5.1.1.3. Support DWP employees to comply with these requirements, as expressed through the HR Standards of Behaviours and Security Code of Conduct, and ensure employees are aware of the consequences of non-compliance,

5.1.1.4. Ensure that suppliers are aware that failure to comply with this policy and other requirements (which will be communicated through the contractual process) will result in corrective action and escalation following agreed processes.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

5.1.2. Line Managers and Contracted Suppliers

5.1.2.1. Ensure all employees fully understand and fulfil their agreed responsibilities for information security under the Security Code of Conduct and the Acceptable Use Policy,

5.1.2.2. Require Contracted Suppliers to be aware of and fulfil their information responsibilities including personnel information security responsibilities,

5.1.3. Information Asset responsibility

5.1.3.1. Identify DWP information assets and define responsibilities to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation and to the citizen, and its hosting location,

5.1.3.2. Ensure DWP has appropriate structures and processes to enable the Department to understand the use of and monitor its information assets.

5.1.4. Employees and Contracted Suppliers - access to information assets and systems

5.1.4.1. Ensure there are documented information asset access controls and procedures, and that security responsibilities have been allocated and accepted, and log system and service user activity to determine individual accountability.

5.1.4.2. Ensure the effective use of cryptography, especially where interconnections between systems or services exist.

5.1.4.3. Ensure users are accountable for safeguarding their authentication information,

5.1.4.4. Ensure correct and secure operations of information processing facilities by regulating, monitoring and reviewing the implementation of protective measures,

5.1.4.5. Ensure the protection of information in networks and any supporting information processing facilities, and maintain the security of information transferred within an organisation and with any external entity,

5.1.4.6. Ensure personal data is not saved or processed in any spread-sheet or system other than those approved by DWP Security for that purpose. Personal data must only be placed in document frameworks such as MS Word, Excel and PowerPoint when following approved local business processes which apply DWP security policy,

5.1.4.7. Ensure that information security is integral to information systems across the entire lifecycle of acquisition, development, maintenance and decommissioning,

5.1.4.8. Define security responsibilities through contract terms and requirements for all suppliers to ensure protection of the organisation's assets that are accessible by suppliers,

5.1.5. Security incident management function

5.1.5.1. Define formal procedures for the management of information security incidents, including improvements and changes to those procedures,

5.1.6. Continuity and Resilience function

5.1.6.1. Require business units to develop, implement and embed appropriate information security business continuity management, including business continuity plans for critical systems and services to minimise disruption against identified threats and risks,

5.1.7. Technology function (through Infrastructure Operations)

5.1.7.1. Require disaster recovery functionality for security systems based on a business impact analysis, risk assessment and cost calculation and in compliance with ISO27001 to re-establish access to and protection of our information.