DWP Personnel Security Policy

Contents

1. Background

1.1 Personnel security is a system of policies, standards, procedures and technical measures, which combine to mitigate the risk of legitimate access to DWP assets being exploited for unauthorised purposes. In particular, this policy serves to mitigate the “insider threat” and associated risks, the causes of which are inherent vulnerabilities arising from accidental, negligent or deliberate (malicious) actions by people working on the physical or technical DWP estate

2. Purpose and Scope

2.1 The purpose of this policy is to define the Department’s requirement for personnel security controls and how and where they should be applied, and in so doing mitigate the risk of unauthorised access to our data, electronic systems and physical premises.

2.2 This policy applies to all DWP employees, agents, contractors, consultants and business partners (referred to in this document as ‘individuals’) with access to DWP’s information and information systems.

3. Accountabilities

3.1 The Chief Security Officer is the accountable owner of this policy and is responsible for its maintenance and review, through the Deputy Director for Security Policy and Compliance.

3.2 Accountability for the delivery of capabilities to help mitigate the risks relating to this policy lies where the appropriate functional accountability sits for the relevant controls, aligned with wider responsibilities. For example:

i) People and Capability, the Director-General of which is accountable for the design and use of relevant policies and procedures relating to the measurement and monitoring of the movement and behaviours of people working on the DWP estate;

ii) Digital, whose Director-General is accountable for providing services and technology solutions that meet the needs of the wider DWP business, including the means to effectively support the onboarding, movements and off boarding of workforce members, and accompanying requirements; and

iii) Security, sitting within Finance Director-General accountability, and where the Chief Security Officer is responsible for providing assurance relating to this policy, compliance monitoring, and escalation of cross-cutting issues for resolution.

3.3 Accountability for compliance with the behavioural aspects of this policy lies with all individuals in scope, and with line managers, who must monitor compliance with security awareness and personnel vetting requirements, through mechanisms appropriate to the business context and in accordance with available tooling.

4. Policy Statements

4.1 Accountable individuals and functions across DWP must ensure resources and processes are in place to deliver the requirements of this policy, in an integrated fashion where necessary, ensuring that dependencies are mapped and understood.

4.2 All individuals must comply at all times with procedures established under this policy and must also ensure compliance with associated security and P&C policies and standards, including but not limited to:

- Acceptable Use Policy
- Information Security Policy
- Physical Security Policy
- Information Management Policy
- DWP Standards of Behaviour
- The Civil Service Code
- Joiners, Movers & Leavers Policy

4.3 Security awareness

To facilitate awareness and compliance the Department will maintain a Security awareness programme, the key principles of which are:

a) all individuals must undergo security induction upon commencement of their employment.

b) all individuals must complete the annual Security E-Learning modules within the appropriate deadlines.

c) all individuals should be made aware of and able to understand the contents and requirements of regular security awareness campaigns and communications, made available through all appropriate channels.

4.4 Joiners, Movers and Leavers

a) To maintain good practice and support effective risk management, the Department shall ensure that simple procedures and the technical capability is in place to enable all new starters – whether permanent or temporary staff or contracted resource – to have completed mandatory pre-employment checks (Baseline Personnel Security Standard) and to undertake the mandatory security training upon entry to the department and before they have access to any customer-facing systems or other sensitive data;

b) The Department shall ensure that it has technical systems, policies and simple and effective procedures in place to maintain a constant record of the numbers of individuals working on its physical or technology estate at all times, their usual work locations, and their working roles;

c) The Department shall ensure that it has policies, procedures, technical controls and monitoring capability in place and consistently implemented, such as to only allow those with specific access rights to operate on named technology systems and data sets: this is so as to provide assurance that access rights are being explicitly granted, rather than by default;

d) The movement of individuals between roles shall be understood and monitored to the extent that specific system, data and building access rights are granted in relation to a specific role and an individual's access needs relating to it;

e) Simple procedures shall be put in place, and monitored, such that anyone leaving the Department returns their technology equipment upon departure, and that access to departmental systems, applications and data – wherever hosted – shall be removed at the same time;
(see Leaving the DWP: Mandatory Leavers Actions).

f) All individuals and line managers must ensure compliance with the Joiners, Movers & Leavers Procedures and associated policies as defined.

4.5 Security Vetting

a) Line Managers with accountability for roles which are deemed sensitive and appropriate for National Security Vetting must ensure compliance with the DWP Security Vetting Policy. Individuals to whom the policy applies must comply with the requirements of the policy.

4.6 Remote Working

a) Individuals who request permission to work remotely, or from home, including working from abroad, must ensure full discussion with their line managers to comply with the DWP Remote and Home Working Policy and the DWP Acceptable Use Policy.

4.7 Investigation and Disciplinary Measures

a) The Department shall put in place appropriate personnel policies and procedures to enable the timely investigation of any security incidents and/ or allegations of internal fraud, arising as a result of “insider activity” contrary to the intentions of this policy.

b) The Department shall ensure that its personnel policies include effective and proportionate disciplinary measures, appropriately communicated to all individuals, such as to deter inappropriate behaviour under this policy.

5. Policy Compliance

5.1 Individuals are responsible for ensuring that they understand their responsibilities as defined in this policy and continue to meet its requirements. It is a Line Manager’s responsibility to take appropriate action if an individual fails to comply with this policy, ensuring that any security incidents or allegations of internal fraud are reported to the appropriate authority (see below). – Breaching this policy may result in disciplinary procedures (including criminal prosecution) which could lead to dismissal.

i) Security Incidents should be reported (Reporting Incidents) to the Security Incident Response Team (SIRT)

ii) Allegations of internal fraud should be reported to Counter Fraud & Investigations (Counter Fraud and Investigation) directly, or via the Whistleblowers Hotline (Whistle Blowing and raising a concern)

5.2 Members of the DWP Security and Data Protection function will regularly assess for compliance with this policy and may inspect technology systems, design, processes, people and physical locations to facilitate this. This may include technical testing, and testing of physical security controls. Compliance with the testing and inspection regime is expected from all parties.

6. Further information

6.1 Please contact the DWP Security Advice Centre or DWP Think Secure Chatbot for further advice regarding this policy.

Additional Information

Personnel Security Policy frequently asked questions.