DWP Physical Security Policy

Chief Security Officer

Date: 21/01/2025

Department for Work & Pensions

ThinkSecure

This DWP Physical Security 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: Gov.uk

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.

Contents

Policy Title

DWP Physical Security Policy

Overview

This DWP Physical Security Policy provides our employees, contractors, partners, and other interested parties with clear policy direction that requires them to ensure that all necessary physical protective security controls are in place. This will prevent unauthorised access, damage, interference, or harm (malicious or otherwise) to DWP's assets and personnel, enabling continuous delivery of DWP business priorities.

Purpose

This policy sets out a framework to follow a 'layered' approach to physical security. Its effective application will provide secure environments, commensurate with assessed risks, from which DWP can operate to achieve its strategic aims and objectives and appropriately protect personnel and DWP assets.

This policy provides a high-level organisational objective for DWP for its Physical Security, supported by MANDATORY behavioural **Physical Security Standards** and **Physical Technical Standards**, which MUST be followed to ensure compliance.

Scope

This policy applies to:

a) This DWP Physical Security Policy applies to all DWP employees, contractors, partners, and service providers. This will include employees of other organisations when on the DWP Estate.
b) This DWP Physical Security applies to all DWP premises and all locations in which DWP business is conducted (including floorplates on co-located premises). Operational delivery is also undertaken on premises which are not part of DWP Estate; external landlords or providers are responsible for the implementation of the relevant security services and equipment.

c) This policy does not replace any legal, statutory, or regulatory requirements.

Policy Statements

1. All DWP employees, contractors, partners, and service providers must follow the required behavioural standards, defined physical security processes, and where relevant, any supporting procedures. All staff must ensure they remain observant, report suspicious behaviour, and highlight non-compliance. This vigilance will help prevent unauthorised access to, or attacks against, the DWP and reduce the impact should they occur.
2. Staff must familiarise themselves with the correct reporting procedures, outlined within the **Security Portal**. Security Incidents must be reported following DWP's defined processes.
3. Each DWP premises presents unique physical security challenges, and each must implement MANDATORY **Physical Security Standards** and **Physical Technical Standards** as a minimum, with further enhanced controls introduced based upon a risk informed assessment and categorisation appropriate to the individual site.
4. All sites must undertake an annual review of asset holdings as defined within the annual assurance assessment.
5. Existing and emerging physical security threats should be recorded and reviewed on an annual basis, or as the threat changes, and evaluated against His Majesty's Government's **Physical Security Standard - UK Government Security - Beta.**
6. All sites must maintain an annual assessment of physical security controls and associated risks, following the defined assurance lifecycle. Physical Security risks and scenarios must also be considered as part of Incident Management and Resilience planning, testing and compliance. For more information, please see DWP Business Continuity and Resilience Team.
7. Any physical changes to a DWP site, building, location infrastructure, or significant equipment failure should be managed under a risk-based Statement of Need (SoN), providing clear and prioritised security recommendations.

8. A consistent approach is required across the DWP's estate to ensure access control is standardised. An 'Access to Buildings Policy' must be in operation at each site to support and protect the DWP's physical premises, data assets, information, and people. This must be communicated to all building users to enable them to comply. **(This to be suspended until confirmation of a published generic Access to Buildings Policy)**
9. Sites must ensure that applicable measures under the **Response Level Security Measures Policy** are followed in accordance with designated threat and response levels.
10. Every DWP office is considered private land and, as such, the Department retains the right to restrict filming and audio recording to protect customer data, personal privacy, and the health and safety of staff and visitors.
11. This policy and supporting standards must be subject to annual review, as a minimum.

Accountabilities and Responsibilities

a) The safety and security of the DWP is the responsibility of all staff, however, additional responsibilities may be assigned to specific roles. The DWP Chief Security Officer is the accountable owner of the DWP Physical Security Policy and is responsible for its maintenance and review, through the DWP Deputy Director for Security Policy and Central Services.

b) All DWP employees, contractors, partners, service providers and employees of other organisations who are on DWP premises, including co-located sites, must follow all DWP policy regarding minimum standards of behaviour. Any breach of such guidance or policy may result in disciplinary action leading to a sanction, dismissal, and/or reference to external authorities.

c) The Senior Responsible Officer (SRO) or delegated responsible manager for site has responsibility for ensuring site level physical security controls and risks are regularly reviewed and managed, with the use of a Risk Register, ensuring that any action to address risks is conducted appropriately. The risks held within the Risk Register should form part of a handover to a new SRO.

d) Where defined in a commercial contract, the management of designated physical security controls at site is the responsibility of third-party providers (e.g., security officer provision, site access management, and automated security systems).

e) It is the responsibility of those procuring supplier contracts for physical security controls to ensure that the most up to date technical/industry standards are provided by suppliers. Procurement teams must seek Enterprise Security Risk Management (ESRM) and DWP Estates security input prior to committing to contract. This includes technical/industry standards for Closed Circuit Television, Access Controls, Intruder Detection Systems, and any other relevant alarm systems which are managed by a contracted supplier. Technology must be regularly reviewed, at least annually, to ensure that the security controls remain effective and fit for purpose.

f) Physical security risks and controls will be assured in the form of site level assurance assessments, as undertaken by the ESRM, in accordance with a defined assurance plan.

g) Physical security risks and controls will be assured in the form of site level assurance assessments, as undertaken by the ESRM, in accordance with a defined assurance plan.

Compliance

a) DWP must ensure a baseline of physical security controls is in place at each site and ensure that such measures provide appropriate protection to all occupants and assets, and that these controls can be strengthened when required i.e., in response to a security incident or change in the Government **Response Levels**.

b) If for any reason users are unable to comply with this policy or related standards, they should discuss this with their line manager in the first instance and then the Security Advice Centre who can provide advice on escalation/exception routes.

c) An **exception to policy** may be requested in instances where a business case can be made to undertake an activity that is non-compliant with DWP's

Security Policies. This helps reduce the risk of non-compliant activity and security incidents.

d) Failure to **report a security incident**, potential or otherwise, could result in disciplinary action and, in the most severe circumstances, dismissal. A security incident is the attempted or actual unauthorised access, use, disclosure, modification, loss, or destruction of a DWP asset (or supplier asset that provides a service to the Authority) in violation of security policy. Assets include people, property, or information. The circumstances may include actions that were actual, suspected, accidental, deliberate, or attempted. Security incidents must be reported as soon as possible. DWP users must report security incidents via the DWP Security Incident Referral Webform; third parties and suppliers must follow the DWP Security Incident Management Standard (SS-014).

e) Members of the DWP Security and Data Protection Team 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. All DWP employees, contractors, partners, and service providers, including those on co-located sites and sites owned by other public bodies will be required to facilitate, support, and when necessary, participate in any such inspection. This may also include employees of other organisations who are based in DWP occupied premises.

f) The DWP Physical Security Policy will ensure activities and behaviours comply with UK Data Protection Regulations.
