DWP Physical Security Policy

Contents

Audience

1.1 This DWP Physical Security Policy applies to all DWP employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This will also include employees of other organisations who are based in DWP occupied premises.

Policy Objective

2.1 This provides our employees, contractors, partners and other interested parties with a clear policy direction that requires them to ensure that all necessary physical protective security measures are in place to prevent unauthorised access, damage and interference (malicious or otherwise) to DWP's assets.

Scope and Definition

3.1 Physical Security refers to measures that are designed to protect physical locations and the assets, information and personnel contained within.

3.2 This policy sets out the approach to be adopted to manage, develop, improve and assure Physical Security across DWP.

3.3 It is essential that our business is conducted in an environment where potential threats (including those from both natural and human-made hazards, terrorism, crime and insider threats) to DWP assets, information and personnel etc. have been identified, risk assessed and appropriately mitigated to prevent interference, loss or compromise (malicious or otherwise). This includes ensuring physical perimeters are protected and entry controls are in place to provide proportionate protection against natural disasters and terrorist attacks.

Context

4.1 This policy sets out a framework to follow a ‘layered’ approach to physical security. It provides suitably secure environments from which DWP can operate to achieve its strategic aims and objectives by implementing security measures in layers, to appropriately protect personnel and DWP assets including material of differing levels of sensitivity.

4.2 This policy provides a high-level organisational objective for DWP with regards to Physical Security, supported by MANDATORY behavioural Physical Security Standards and Physical Technical Standards (add link) which MUST be followed to ensure compliance, as they represent the minimum measures required to protect the security of DWP assets, information and people.

4.3 The Physical Security Policy does not exist in isolation and where appropriate associated policies, standards and procedures are referenced within this document.

4.4 Physical Security controls and processes are implemented across DWP estate with some security systems, controlled or delivered by third party providers on other premises. Operational delivery is also undertaken on premises which are not part of DWP Estates and external landlords or providers are responsible for the implementation of the relevant security services and equipment.

Responsibilities

5.1 All DWP employees, contractors, partners, service providers and employees of other organisations who are on DWP premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues and the protection of Departmental Assets.

5.2 The Senior Responsible Officer (SRO) or delegated responsible manager for site, has responsibility for ensuring physical security risk assessments are reviewed annually, ensuring that any action to address risks and cover business continuity activities are up-to-date. These should be communicated, regularly rehearsed, and implemented. Plans should be available in accordance with their significance, importance and classification.

5.3 Managing the physical security controls of sites (e.g. perimeter control, guarding, site access etc.) occupied by DWP employees is the responsibility of a contracted provider. The controls will be measured in the form of Physical Security Reviews as undertaken by the Physical Security Group.

5.4 It will be the responsibility of those procuring supplier contracts for such physical security measures to ensure that the most up to date technical/industry standards are met and that the technology and processes in place are regularly reviewed to ensure that the security controls remain effective and fit for purpose. 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.

Policy Statements

6.1 Physical Security controls MUST be implemented that are proportionate to the risk appetite of the DWP and in adherence with the Information Security Policy and Acceptable Use Policy and other appropriate personnel and information security standards, including successful completion of Baseline Personnel Security Standard (link is external). All employees must ensure they remain observant, report suspicious behaviour and highlight non-compliance. This vigilance will help deter, delay, prevent and/or detect unauthorised access to, or attack on, a location and mitigate the impact should they occur.

6.2 Each DWP occupied premises presents unique physical security challenges and the measures introduced to protect each site must take into account the risk categorisation and the physical composition of that site. Effective approaches to Physical Security MUST follow the MANDATORY Physical Security Standards and Physical Technical Standards (add link).

6.3 The Senior Responsible Officer or delegated responsible manager for site, must ensure that the Response Level Security Measures Policy are noted and adhered to ensuring physical security risk assessment activity is conducted appropriately and that any action plans that address risks, are implemented promptly.

Compliance

7.1 The level of risk and potential impact to DWP information, assets and people will determine the controls to be applied and the degree of assurance required. DWP must ensure a baseline of physical security measures are in place at each site, and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required i.e. in response to a security incident or change in the Government Response Level.

7.2 The implementation of all security measures must be able to provide evidence that the selection was been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure (link is external), Government Functional Standard GovS 007: Security including Government Functional Standard GovS 004: Property and the HMG Security Policy Framework(link is external).

7.3 The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards shall be subject to annual review or more frequently if warranted.

7.4 Failure to report a security incident, potential or otherwise, could result in disciplinary action.

7.5 Physical Security risks and scenarios will be considered as part of Incident Management and Resilience planning, testing and compliance.

7.6 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.

Version Number	Date Drafted
2.0	08/03/19
2.1	06/05/22