DWP Physical Security Policy

Contents

1. 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.

2. 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.

3. 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.

4. 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 Physical Security Standards 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 This policy is also supported by several useful Good Practice Guides which will assist the policy audience with implementation.

5. 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 most senior grade based at each site, or in Moderate Risk and larger sites, the Senior Responsible Officer (SRO) has responsibility for ensuring physical security risk assessments are conducted annually. They MUST ensure the action plans created to address identified risks and instigate business continuity activities are up-to-date, clearly communicated, regularly rehearsed, implemented effectively and readily available in accordance with their significance/importance/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.

6. 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.

6.3 The most senior grade manager, or Senior Responsible Officer in Moderate Risk and larger locations, MUST ensure that their site adheres to the Response Level Security Measures Policy and ensure physical security risk assessment activity is conducted annually and that the action plans created to address identified risks are implemented.

7. 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 and HMG Security Policy Framework.
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 will be subject to annual review or more frequently if warranted.