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 Physical Security Policy

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.

1. Audience

1.1. This DWP Physical Security policy applies to all DWP employees, contractors, partners, service providers and includes employees of other organisations who are based on DWP premises.

1.2. This policy does not apply to DWP staff operating out of sites owned and/or managed by other public bodies.

2. Policy Objective

2.1. This provides our employees, contractors, partners and other interested parties with a clear policy direction that requires them to protect DWP premises and assets, and ensure that all necessary physical protective security measures are in place to prevent unauthorised access, damage and interference to DWP's assets and the occupants of its premises.

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 to DWP assets, information and personnel (including from terrorism, theft and insider threat actors) have been identified, risk assessed and appropriately mitigated to prevent interference, loss or compromise. 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, but it is supported by MANDATORY Security Standards and Compliance Statements 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 guidance products 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 remain accountable for the security,

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.

health and safety of themselves, colleagues and the protection of Departmental Assets including information and personnel.

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 regular 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. Except in a very small number of locations, managing the physical security controls of sites across the DWP estate is the responsibility of a contracted provider.

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). This will support all staff to ensure they remain observant, report suspicious behaviour and highlight non-compliance. This vigilance will 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 location 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 Security Standards and Compliance Statements.

6.3. The most senior grade manager, or SRO in Moderate Risk and larger locations, MUST ensure that their site adheres to the Response Level 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 threat 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 appropriate information security standards ISO27001/27002 and relevant HMG Policies and Standards.

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.

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. Therefore this policy and subsequent supporting guidance and standards will be subject to continual review and update.