Ministry of Justice

Physical Security Policy

Contents

Physical Security Policy

Audience

This policy complements the Ministry of Justice (MoJ) overall security policy.

Physical security is the practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (tangible, real-world) environment.

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

Executive Agencies and Arm's Length Bodies (ALBs) are expected to comply with this corporate framework, but might establish their own arrangements tailored to operational needs, and should therefore supplement this policy with local policy or guidance for any business-specific risk.

Objective

This content provides employees, contractors, partners and other interested parties with a clear policy direction. It requires them to ensure that all necessary physical protective security measures are in place to prevent attack, unauthorised access, damage, or interference (malicious or otherwise) to MoJ assets, and most importantly to prevent physical harm to our people and the public.

Scope and Definition

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

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

It is essential that MoJ business is conducted in an environment where potential threats - including those from both natural and human-made hazards, terrorism, crime, and insider threats - to MoJ assets, information, and personnel 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

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

This policy provides a high-level organisational objective for the MoJ with regards to Physical Security, supported by **MANDATORY** Physical Security Standards which **SHALL** be followed to ensure compliance, as they represent the minimum measures required to protect the security of assets, information and people.

Responsibilities

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

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 **SHALL** 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, or classification.

Managing the physical security controls of sites occupied by MoJ employees is the responsibility of a contracted provider. The physical security controls include, for example:

- Perimeter control.
- Guarding.
- Site access.

The controls are measured in the form of Physical Security Reviews, as undertaken by the Group Security and Governance Team.

It is the responsibility of those procuring supplier contracts for such physical security measures to ensure that the most up-to-date technical and 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 and 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

Physical Security controls **SHALL** be implemented that are proportionate to the risk appetite of the MoJ, and in adherence with the Information Security Policy and Acceptable Use Policy and other appropriate personnel and information security standards, including successful completion of the Baseline Personnel Security Standard.

All employees must ensure they remain observant, report any suspicious behaviour, and highlight non-compliance. This vigilance will help deter, delay, prevent, or detect unauthorised access to, or attack on, a location, and mitigate the impact should they occur.

Each MoJ occupied premises presents unique physical security challenges. The measures introduced to protect each site **SHALL** take into account the risk categorisation and the physical composition of that site. Effective approaches to Physical Security **SHALL** follow the **MANDATORY** Physical Security Standards.

The most senior grade manager, or SRO in "Moderate Risk" and larger locations, **SHALL** 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.

Compliance

The level of risk and potential impact to MoJ information, assets and people determines the controls to be applied, and the degree of assurance required. The MoJ **SHALL** 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, for example in response to a security incident or change in the Government Response Level.

The implementation of all security measures **SHALL** 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 Government Functional Standard - GovS 007: Security.

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

Physical security advice

Physical security advice, including specific advice on this guidance, can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.