



Policy Title: Physical Security Policy

Date Published/Reviewed: January 2018

Thames Valley Police ensures that all policies have been assessed and comply with MoPI Guidance, and the Data Protection Act 2018. In addition, this Policy has been reviewed by The Force Head of Health, Safety and Environment and has undergone an Equality Impact Assessment.

1.0 About this Policy

1.1 Rationale

Providing an appropriate and proportionate range of measures to protect our buildings, estate and property is a key requirement of the Force Protective Security Framework. Physical Security involves a number of distinct security measures which form part of a 'layered' or 'defence in depth' approach to security, which must take account of the balance between prevention, protection and response.

Physical security forms the basis for all other security measures, including personnel and information security. A balanced security programme must include an effective physical security foundation. An effective physical security foundation protects and preserves information, physical assets and human assets. This policy sets out the approach to be adopted to manage, develop and improve Physical Security across the Force to ensure that our assets are effectively protected from loss or compromise and should be read in conjunction with other relevant security policies around personnel and information.

Thames Valley Police (TVP) is committed to managing its physical security arrangements and will:

- a. Maintain appropriate and proportionate physical security standards, specifically to comply with the Government (HMG) Security Policy Framework and other relevant security industry standards, e.g. ACPO 'Secured by Design'.
- b. Adopt a 'layered' approach to physical security, ensuring that the approach incorporates the identifiable elements of prevention, detection, and response.

- c. In protecting and managing Force assets apply both the Physical Security Baseline Controls Matrix and supporting Physical Security Assessment Questionnaire to identify appropriate physical security measures.
- d. Provide physical security information and awareness for all police officers, police staff and contractors, including induction briefings, to maintain the integrity of Force's assets.
- e. Ensure that all police officers, police staff and contractors are aware of their individual responsibility to comply with this 'Physical Security Policy' and supporting security standards

1.2 Legislation/National Standards

None applicable.

1.3 Intention

To provide TVP employees, contractors and partners and other interested parties with clear and concise policy guidance that enables them to safeguard and protect Force assets and ensure that all necessary physical protective security measures are in place.

To set out a Physical Security framework for the Force which will, by adopting a 'layered' approach to physical security, provide suitably secure environments from which the Force can operate to achieve its strategic aims and objectives.

1.4 General Principles

The Police Service and other organisations in general are faced with increasing security threats from a wide range of sources. These threats include:- espionage; sabotage; computer-assisted fraud; the more common threats of wilful and accidental damage; unlawful or unauthorised disclosure of data; human error; carelessness and ignorance. Such threats can lead to failure of core information systems, increase the risk to individuals and potentially breach the criminal or civil law. It is therefore necessary for the Force to ensure that we implement a range of appropriate and proportionate physical security measures.

In particular, this policy aims to ensure that the Force adopts a layered approach to security and will:

- a. Secure the perimeters of its buildings, including all property occupied but not owned by the Force, taking all reasonable measures to prevent unauthorised access.
- b. Limit building access to its police officers, police staff, contractors, partners and visitors in possession of a valid identity card.
- c. Further limit within its buildings, by physical means, access to areas and/or assets where a restricted level of access is either required or deemed as necessary.

- d. Ensure risk assessments are properly conducted in order to make certain that personnel hold the appropriate level of clearance to sensitive/high value assets or areas.
- e. In the event of failure of a physical security measure, to have in place appropriate levels of reporting and detection systems either physical; technical or both.
- f. Work with its policing partners to consider security in the design stage of new projects within or for our organisation to ensure cost effectiveness and value for money.

This Policy shall apply to all TVP employees, contractors, partners and employees of other companies who are on our premises.

The supporting Physical Security Standards define how the requirements are to be implemented. Compliance with the requirements contained within this policy and supporting Security Standards represents the minimum required to protect the security of Force assets.

The Force Security Committee (FSC) has been established to define the strategic security requirements necessary to protect the interests of the Force, staff and assets. Central to this is ensuring that all elements of information, personnel, technical and physical security are integrated and balanced to provide 'defence in depth' and resilience. The FSC which is chaired by the DCC who takes responsibility for monitoring compliance with this Policy and supporting Security Standards.

The Physical Security Sub-Group is a working group combined with the Information sub group. This group was established to review force wide information and physical security issues, provide general advice and draft policy for consideration by senior management. This will include advice and recommendations regarding appropriate security standards for specific locations or initiatives. The group is subordinate to the Force Security Committee and will review and recommend tactical requirements in accordance with appropriate standards. Progress will be reported to the Force Security Committee, which is chaired by the DCC, to provide an overview for the Chief Officer Team.

The successful implementation of this Policy and supporting Security Standards shall rely on the development of an effective approach to partnership working between Force HQ, Local Police Areas (LPA), Operational Command Units (OCU) and other Support Departments, those staff dedicated to security matters, and ultimately all staff employed by the Force.

2.0 Statement of Policy

2.1 Physical Security Standards

While the intention of this Policy is to provide TVP employees with clear and concise policy direction considerably more detail is necessary to provide them with clear procedural requirements and guidance. Such detail is contained in a

series of 'Security Standards' that have been approved by the Force Security Committee and are regarded as policy insofar as compliance with their instruction is required. Security Standards are published on the intranet or otherwise circulated to those who need to understand and comply with the content.

This policy is enacted by the following Physical Security Standards:

- Identity Card Standard
- Key Fob Standard
- Physical Security Principles
- Physical Security Sub Group Terms Of Reference
- Reporting Security Breaches
- Operation Roundup
- Security Liaison Role Types
- Security Sweeps

3.0 Human Rights Articles Engaged

3.1 Certification Human Rights

There is no legal basis for this policy. It is designed to ensure the provision of an acceptable level of assurance as to the integrity of all staff and contractors who are to be given authorised access to information or other assets belonging to or entrusted to the force.

3.2 Equality Impact Assessment

An equality impact assessment has been carried out by the Single Equality Scheme Coordinator. The conclusion of this review is that there is nothing discernible in the policy that negatively impacts the protected characteristics contained in the Equality Act 2010.

4.0 Health and Safety at Work

There are no Health & Safety concerns connected with this policy

5.0 Communications, Challenges and Representations

5.1 Communication

This Physical Security Policy is underpinned by a series of physical security standards. It is also linked to the Protective Security Policy, Personnel Security Policy and the Information Security Policy the latter of which is owned by Joint Information Management Unit.

This policy will be available via the Professional Standards section and the Policies & Procedures section of the TVP intranet site and on the public TVP website. It will also be circulated in Mangers Briefing. Supporting security standards are published on the Professional Standards site.

5.2 Challenges and representation

Head of Professional Standards Department
Thames Valley Police HQ
Oxford Road
Oxford
OX5 2NX

6.0 Review Date

The current security environment has necessarily dictated that Protective Security Requirements must be constantly reappraised and evaluated in order to meet new threats and other emerging vulnerabilities. Therefore this policy and supporting standards shall be reviewed annually.

7.0 Related Guidance

Physical Security Standards

8.0 Freedom of information

This policy can be made available under the Freedom of Information Act.

9.0 Government Security Classification Policy

This document is not protectively marked and is classified as Official.

10.0 Relevant Supporting information

10.1 Data protection

It is recognised that sensitive personal data will be processed in compliance with this policy. This and personal data will be managed in accordance with the specifications of the Data Protection Act 2018.

10.2 Management of Police Information (MOPI)

This policy does not affect any of the key business areas as identified by Management of Police Information (MOPI). However any information deemed 'for a policing purpose' or any data about an individual that is circulated or received by e-mail, or published/downloaded via the intranet or internet or circulated in any other format must comply with MOPI guidelines