



**TITLE** FORCE SECURITY POLICY

**CCMT Sponsor** Deputy Chief Constable

**Department/Area** Professional Standards Department

**Section/Sector** Force Security

---

**1.0 Rationale**

1.1 This policy establishes the overarching protective security strategy for Thames Valley Police which is designed to counter security related threats to key business activities and assets.

1.2 It sets out a framework to support legal obligations including:

- Official Secrets Acts – the need to protect information from unauthorised disclosure
- Data Protection Act – the need to ensure an appropriate level of security is employed to protect personal information and confirm the reliability of staff

**2.0 Intention**

2.1 Application of the strategy reinforces the profile and importance of a protective security regime that must feature within every aspect of business. This is achieved by integrating a number of complementary security measures to create a 'defence in depth' approach that includes personnel, information, technical and physical security.

2.2 The policy adopts national policy, codes of practice and guidance to provide consistent and transferable procedures across other police, government and partnership organisations. In particular, requirements and principles within the following documents have been adopted:

- Manual of Protective Security
- ACPO Community Security Policy
- ACPO National Vetting for the Police Community Policy
- ACPO Counter Corruption Policy

- 2.3 The complexity, relationship and inter-dependency of the various security requirements is such that policies and procedures have been structured in a hierarchy as follows:

Force Security Policy	<i>Strategic - Policy</i>
Vetting Policy Information Security Policy IT Security Policy	<i>Operational - Policy</i>
Security Standards	<i>Tactical – Procedures &amp; Guidance</i>

### **3.0 General Principles**

- 3.1 Thames Valley Police is responsible for activities that include the prevention and detection of crime, with substantial resources being engaged in combating serious and organised criminality. As a consequence the organisations activities and assets are under threat from those who seek to undermine or disrupt effectiveness in these areas, as well as the threat posed by terrorism, or the consequences of negligence or corruption by staff or others connected with the organisation.
- 3.2 Therefore the aim of this policy is to set out the broad security agenda to reduce risks and protect the organisation, staff, assets and the interests of those connected with Thames Valley Police including victims, witnesses and offenders.
- 3.3 In addition, the policy underpins the need for a combination of protective measures to be embraced within everyday activity by the engagement of all staff to ensure that security issues are identified and receive necessary, appropriate, proportionate and timely attention.
- 3.4 The policy also defines key principles of security risk management, and the roles and responsibilities of the managers and teams involved.

### **4.0 Challenges and Representations**

- 4.1 Challenges and representations concerning this policy should be directed to the:

Force Security Manager  
Thames Valley Police  
Headquarters  
Oxford Road  
Kidlington  
Oxon  
OX5 2NX

## **5.0 Guidance, Procedures and Tactics**

### **5.1 Threat Sources**

Damage to the business of Thames Valley Police can result from deliberate attack or exploitation of security failure. The principle sources of threat include:

- Criminals or associates
- Extremist Groups
- Investigative journalists
- Disaffected or corrupt staff
- Negligence or inadequate safeguards
- Partner agency weaknesses or failures

### **5.2 Means of Attack**

These can include:

- External, remote electronic attack
- Direct physical attack including forced or clandestine entry
- Internal activity through infiltration or corruption

### **5.3 Security Risk**

To protect the organisation it is essential that the security risks relating to key assets are managed effectively. Assets and risk management activity fall within three main areas – knowledge (information), people and other assets. For each of these categories objectives, risks and control measures provide the basis for more detailed monitoring and preventative activity.

#### **5.3.1 Objectives**

Knowledge - To maintain the required Confidentiality, Integrity and Availability of Thames Valley Police information including:

- All medium types
- All data held and processed
- Knowledge of Thames Valley Police business

People - To maintain an appropriate safe working environment for staff and others, regardless of employment location.

Other Assets - To maintain a working environment that is safe and secure from a deliberate hostile act, negligence or omission.

#### **5.3.2 Risk**

Knowledge - Failure to detect and counter internal or external threats, whereby knowledge becomes accessible to non-authorized persons.

People - That the operating environment is breached by a deliberate hostile act, negligence or omission, thereby putting people at risk.

Other Assets - That the operating environment is breached thereby putting assets at risk from theft, damage, compromise or other unauthorised interference.

### 5.3.3 Control Measures

All Assets - An effective protective security regime be developed and maintained through active security practice and management including:

- An integrated system of technical engineering, physical and procedural barriers
- Effective security risk management and procedures understood and observed by all users through awareness training and performance management
- Effective security vetting

### 5.4 Executive Roles and Responsibilities

Overall responsibility for Force Security rests with the Deputy Chief Constable who has established a Force Security Unit within the Professional Standards Department.

### 5.5 Force Security Manager

The Force Security Manager is accountable to the Head of Professional Standards Department and responsible for coordinating all aspects of security, defining appropriate security measures, monitoring and investigating security issues and providing guidance and advice throughout the organisation. The incumbent also holds the appointment of 'Departmental Security Officer' (DSO) and interacts with other Government departments and agencies.

### 5.6 Force Security Unit

The unit is managed by the Force Security Manager and comprises:

- Central Vetting Unit – responsible for all staff and contractor vetting
- Data Protection – responsible for receiving and processing data protection enquiries, and the provision of guidance and advice
- Freedom of Information – responsible for receiving and processing related enquiries, and the provision of guidance and advice
- Information Security – responsible for establishing standards necessary to safeguard information assets, and the provision of guidance and advice

### 5.7 Local Commanders, Managers, Supervisors and Staff

All managers, supervisors and staff are responsible for ensuring that security measures are adopted to prevent or minimise vulnerability to the organisation, staff or assets.

### 5.8 Security Liaison Officers

Good practice encourages the adoption of locally appointed security liaison officers of management status to fulfil delegated responsibilities for implementation and compliance with security standards. The person should retain a security focus by ensuring that security issues are raised with local commanders and that incidents or breaches are reported to the Force Security Manager.

## 5.9 **Force Security Committee**

The Force Security Committee is chaired by the Deputy Chief Constable and meets quarterly to monitor security developments, direct strategy and authorise security standards. A number of sub groups coordinated by the Force Security Manager have been established to progress issues relating to physical, technical and information security, the product of which is reported to the Force Security Committee for approval.

## 5.10 **Security Standards**

A small number of key policies have been compiled to guide security measures relating to vetting, information and IT security. However, the breadth of security measures necessary to provide an integrated 'defence in depth' regime is such that considerable procedural requirements and guidance are required. Therefore, a series of 'Security Standards' will define specific measures and these will be approved by the Force Security Committee and regarded as policy insofar as compliance is required. Security Standards will be published on the intranet or circulated to those who need to know the content.

## 5.11 **Breaches of Security**

Any security incident or occurrence that has the potential to compromise the organisation, staff, information or other assets, must be reported to the Force Security Manager for assessment and decision regarding further action.

## 5.12 **Documentation**

Security policy and standards will be documented and approved by the Force Security Committee. All activity relating to security meetings, reports, investigation, surveys and decisions impacting upon people will be documented.

## 6.0 **Communication**

6.1 This policy is not protectively marked and can be made available to the general public if requested.

6.2 The policy, together with relevant 'standards' will be included on the Force Intranet and Internet.

## 7.0 **Compliance and Certification**

### 7.1 **Chief Constable**

The Chief Constable has a statutory obligation to run an efficient and effective police force. The Chief Constables responsibilities include the establishment of policies and procedures necessary to ensure the effectiveness of the organisation in pursuit of its lawful aims.

## 7.2 Human Rights

- 7.2.1 Consideration has also been given to the compatibility of the policy and related procedures with the Human Rights Act; with particular reference to the legal basis of its precepts; the legitimacy of its aims; the justification and proportionality of the actions intended by it; that it is the least intrusive option necessary to achieve the aims; and that it defines the need to document the relevant decision making processes and outcomes of actions.
- 7.2.2 Within the Human Rights legislation, Thames Valley Police is defined as a public authority and it is unlawful for the authority to act in a manner incompatible with the rights enshrined within the European Convention of Human Rights. This extends to the requirement to protect information received in confidence and for staff who have access to confidential information to protect it from unauthorised disclosure.
- 7.2.3 It is also acknowledged that Article 8 of the ECHR relating to right of respect for private and family life may be engaged by this policy and that any interference will be in accordance with the law and necessary and proportionate in the interests of national security, the prevention of crime and the protection of the rights and freedom of others. (Human Rights audit completed on 1 March 2005).

## 7.3 Discrimination

In the application of the policy, the Force will not discriminate against any persons regardless of sex, sexual orientation, race, colour, language, religion, political, or other opinion, national or social origin, association with national minority, property, birth, or other status as defined under Article 14, European Convention on Human Rights (ECHR).

## 7.4 Data Protection

- 7.4.1 All personal information processed within Thames Valley Police must be managed in accordance with the Data Protection Act. It is not anticipated that personal data will be processed as a direct result of compliance with this policy.
- 7.4.2 The Data Protection Act prohibits any person, knowingly or recklessly, from disclosing personal data or information contained within personal data, without the consent of the Chief Constable (Data Controller).

## 7.5 Official Secrets Acts

The Official Secrets Acts impose obligations on staff that have access to sensitive information to protect it from unauthorised disclosure.

## 7.6 Health and Safety

The Health and Safety at Work Act imposes a duty of care upon the Chief Constable to ensure, as far as is reasonably practicable, the health, safety and welfare of all staff.

**8.0 Monitoring and Review**

- 8.1 This policy will be reviewed annually and will take account of relevant legislation, national policies and procedures.