



TITLE INFORMATION SECURITY POLICY

CCMT Sponsor Deputy Chief Constable

Department/Area Professional Standards Department

Section/Sector Force Security

1.0 Rationale

- 1.1 This policy sets out the approach adopted to develop, manage and improve Information Security to ensure that information assets are properly protected against loss or compromise.
- 1.2 Within the context of Information Security, 'information' includes data and any form of communication recorded or transmitted in transcript or verbally, manually or electronically. In terms of tangible assets, Information Security principles extend to paper documents, computer files, electronic records, CDs, disks, drives or any other storage or processing medium.

2.0 Intention

- 2.1 Information Security is different to 'Information Management' which embraces a much broader set of administrative procedures necessary to manage the entire life of information from origin, through processing, to disposal. However, Information Security is an integral component of Information Management and for this to be effective, a consistent, well organised and properly administered structure must be established in all working environments throughout the organisation.
- 2.2 Every aspect of business will involve Information security considerations, therefore it remains the responsibility of all people who work for or in support of Thames Valley Police to safeguard organisational assets and ensure that all necessary protective measures are in place.
- 2.3 In applying this policy it is also important that the breadth of protective security principles relating to information, IT, personnel and physical security are fully integrated to create sufficient depth and resilience to complement business continuity requirements and guard against all prevailing threats.
- 2.4 Finally, Information Security must take full account of a range of legislation

governing the manner in which information and data is managed and protected. A common theme is 'confidentiality' and, to remain legally compliant, obligations are placed upon staff to ensure that information is protected.

3.0 General Principles

3.1 The intention is to describe Information Security requirements and demonstrate the need for activity necessary to safeguard sensitive information, counter threats and comply with legislation.

3.2 Central to this approach is an understanding that the organisation cannot function without information, processes and networks that combine to create a complicated infrastructure. From this it is important to identify the more sensitive intelligence, operational, financial or business assets that require specific protection and to develop measures to prevent, detect and mitigate loss or compromise.

3.3 To balance business needs with information security requirements a proportionate response is necessary and this is achieved by adopting measures that preserve:

- **Confidentiality** – ensuring that information is accessible only to those authorised to have access, and protecting assets against unauthorised disclosure
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods, and protecting assets from unauthorised or accidental modification
- **Availability** – ensuring that authorised users have access to information and associated assets when required to pursue Thames Valley Police objectives

3.4 Another significant aim is to reinforce 'confidentiality' and 'need to know' principles. Information supplied in confidence, developed to produce intelligence, used to support operational initiatives or connected with other sensitive business activities, must be treated in a confidential manner and only imparted to others in the official course of duties on a strict 'need to know' basis. This requirement is supported by legislation including:

- **Official Secrets Acts** – require staff employed for or in support of the police service to avoid unauthorised disclosure of information
- **Data Protection Act** - requires personal data to be properly safeguarded and not disclosed unless properly authorised and justified
- **Computer Misuse Act** – renders it illegal to gain access to or use a computer without authority
- **Freedom of Information Act** - provides for disclosure of non-personal data, subject to exemptions including the prevention and detection of crime

3.5 While the intention of this policy is to identify a range of protective security measures, considerably more detail is necessary to provide practitioners with clear procedural requirements and guidance. Such detail will be contained in a series

of 'Security Standards' that 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 otherwise circulated to those who need to know the content.

- 3.6 Threats and Vulnerabilities - In adopting relevant protective measures, the nature of threats and vulnerabilities must be considered.
- 3.6.1 Much of the work of the police service is of interest to others and, while the organisation must operate as an open public service, it is important to protect sensitive assets and guard against infiltration by undesirable elements including terrorists, criminals, those who attack computers and, in some cases, the media.
- 3.6.2 As well as external vulnerabilities, the organisation must counter unauthorised or illegal internal activity including corruption or any other deliberate or accidental act or omission which could lead to loss or compromise of information.

4.0 Challenges & Representations

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

Force Security Manager
Thames Valley Police HQ
Oxford Road
Kidlington, Oxon
OX5 2NX.

5.0 Guidance, Procedures & Tactics

5.1 Confidentiality

Information available to staff and others who work in support of Thames Valley Police is provided for official use only. Personal use or communication to unauthorised persons is not permitted. In addition, much of the information is sensitive because of its operational, business or personal content, and this demands that strict rules of confidentiality apply.

5.2 Need to Know

Knowledge and possession of sensitive information must be limited to those who have a genuine 'need to know' to allow them to pursue their official duties. A particular rank, grade or function does not confer any right of access to sensitive assets and the key test relates to a specific 'need to know' to allow the recipient to do their job.

5.3 **Government Protective Marking Scheme (GPMS)**

5.3.1 GPMS provides a consistent standard for marking sensitive assets. The GPMS classifications commence with RESTRICTED and progress through CONFIDENTIAL and SECRET to TOP SECRET. It is the responsibility of the originator to classify the asset and control initial circulation which should be limited to those who 'need to know'. Thereafter, any processing or handling of a GPMS marked asset must follow approved procedures which include secure storage and disposal methods.

5.3.2 It should be noted that most Thames Valley Police computer systems are secure for RESTRICTED information only. In addition, internal fax or email, or external email using the PNN (Police National Network) address can also handle RESTRICTED material.

5.4 **Data Protection**

Particular care must be taken to protect personal data and to apply the Data Protection Act principles to ensure that collection, use, retention, disclosure and disposal follow legal requirements.

5.5 **Clear Desk Practice**

Sensitive assets including those marked with a GPMS classification must be managed in a way that prevents unauthorised access. This includes securing assets in appropriate cabinets when not in use, particularly outside normal working hours.

5.6 **Clear Screen Practice**

Password protected screen savers must be activated when the user is away from their computer terminal to prevent unauthorised access to information or systems.

5.7 **Computer Access and Passwords**

Staff and others working in support of Thames Valley Police are only permitted access to computers and systems for which they have been specifically authorised. Access permissions include the requirement to use the personal Staff ID number as well as a unique password known only to the user. Passwords must not be divulged to others, nor written down. In addition, the password configuration should not comprise obvious names or dates that could easily be associated with the user.

5.8 **Corporate Software**

No unauthorised software must be loaded onto any Thames Valley Police system, whether part of the network or a stand alone facility. In addition, approved software loaded onto Thames Valley Police systems will not be downloaded or copied.

5.9 **Mobile Computing**

Mobile computing devices such as Personal Digital Organisers (PDAs), portable memory devices, laptop computers and mobile telephones that belong to Thames Valley Police, or contain Thames Valley Police data, must be properly secured at all times. Access control (e.g. PIN) must be activated and particular care taken to safeguard equipment when travelling or in a public place. Unless equipment includes specific security measures then classification of data contained on these devices must not exceed RESTRICTED.

5.10 **Removal of Assets from Police Premises**

Authority is required from line managers for any asset to be removed from police premises. For assets classified RESTRICTED or higher, specific authorisation is required together with arrangements to ensure that material is properly secured and safeguarded.

5.11 **Oversight or Eavesdropping**

When discussing or processing issues of a sensitive nature on police premises or in public, extra care must be taken to avoid oversight of mobile computing devices, or eavesdropping.

5.12 **Disposal**

Information assets of a sensitive nature, and particularly those containing a GPMS marking, must be destroyed using approved methods. RESTRICTED and CONFIDENTIAL material can be placed in confidential waste bins, whereas SECRET material must be shredded.

5.13 **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. Reporting requirements are detailed in the relevant security standard.

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 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).

7.4.2 The Computer Misuse Act creates offences relating to gaining unauthorised access to a computer (including internal misuse), illegally using a computer to commit crime or illegally altering the contents of a computer.

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.