



<u>TITLE</u>	IT SECURITY POLICY
<u>CCMT Sponsor</u>	Deputy Chief Constable
<u>Department/Area</u>	Professional Standards Department
<u>Section/Sector</u>	Force Security

1.0 **Rationale**

1.1 This policy describes the approach adopted to develop and improve IT Security to complement measures required to protect information assets and minimise the opportunity for compromise.

2.0 **Intention**

2.1 Much of this work is initiated within ICT Group at the commencement of a project, but principles must extend to all business areas as misuse or abuse of information renders the organisation vulnerable in many ways.

2.2 In overall business terms, IT security and resilience demand a high priority as virtually every aspect of work is dependent upon effective and reliable IT systems. Furthermore, the complexity, intensity and scale of operational responsibilities could not be managed without access to the sophisticated IT facilities available throughout the force.

2.3 It should also be recognised that any internal initiative or desire to maintain the security of our IT systems and networks must take full account of four important external influences:

- The complexity of networks and the extent to which connection through the Internet and other routes can expose the organisation to electronic attack from anywhere in the world
- The facility to introduce portable or peripheral devices onto the network and thereby bypass externally facing controls
- Accreditation requirements stipulated within the Community Security Policy that embrace British Standard 7799, and those associated with network sharing through PITO projects and other similar developments
- Compliance with legislation including Data Protection, Freedom of Information and Computer Misuse Acts.

3.0 General Principles

- 3.1 The aim of this policy is to provide a general overview of IT security and to translate IT industry developments into local initiatives that should be adopted to provide the necessary protection and resilience.
- 3.2 The policy describes a set of generic requirements founded on Government, ACPO and industry standards that are applicable to all systems and must be embraced as an integral component of every IT project.
- 3.3 This complements the approach to information security and is characterised in this context as the preservation of:
- **Confidentiality** – ensuring that information is accessible only to those authorised to have access
 - **Integrity** – safeguarding the accuracy and completeness of information and processing methods
 - **Availability** – ensuring that authorised users have access to information and associated assets when required
- 3.4 Developing effective IT security systems and procedures is an evolving and continuing process and a cycle will be adopted to audit, prioritise, implement and review required improvements of all existing and new IT systems and applications.
- 3.5 Overview - IT systems and applications throughout Thames Valley Police have evolved over several years through influences including developments in technology, business needs, availability of finance and the technical capacity to implement and maintain the facilities.
- 3.5.1 Although acquisition has been formally planned and managed, growth has inevitably been adhoc in terms of type, range and compatibility of systems. In addition, many of the systems purchased had limited, inconsistent or passive security features and these have to be combined to provide an active and coherent foundation to support data sharing and warehousing initiatives, as well as the need to meet legal requirements.
- 3.5.2 Two further dimensions impact upon future design and development:
- Remote Access – an increasing business need for access to data or transfer through mobile networks, lap top computers, PDA or portable memory devices
 - Confidential Networks – the requirement to process and transmit sensitive data classified to CONFIDENTIAL or SECRET on designated secure networks (given that all conventional police networks are accepted as being suitable for processing and transmitting RESTRICTED data only)

4.0 Challenges and Representations

- 4.1 Challenges and representations concerning this policy should be directed to the:
Force Security Manager
Thames Valley Police HQ
Kidlington, Oxon
OX5 2NX.

5.0 Guidance, Procedures & Tactics

5.1 Community Security Policy (CSP)

The Community Security Policy is an adopted ACPO standard relating to information and IT security for implementation across the criminal justice community. It is based upon Government standards that embrace British Standard BS 7799 (ISO 17799) and the organisation is expected to demonstrate compliance by December 2005 and beyond.

5.2 CSP Components

The CSP identifies the following 10 elements that need to be implemented to provide effective and in depth protective security measures:

- Architecture resilient and secure to baseline
- Intruder detection systems deployed and monitored
- Access to systems controlled in accordance with policy
- Solutions to ensure authentication and authorisation implemented
- Anti virus solutions deployed and managed
- Solutions to ensure protective marking deployed
- Appropriate audit controls deployed
- Segregation of assets of differing values managed
- Appropriate encryption solutions deployed
- Independent health checks commissioned

5.3 Architecture resilient and secure to baseline

The baseline is a requirement that systems and networks throughout Thames Valley Police and other police organisations have the required policies, controls and procedures in place to enable them to process and transmit data classified to RESTRICTED level. Supplementary to this is the use of the Police National Network (PNN) that provides sufficient safeguard to communicate RESTRICTED information using fixed telephone, fax and email.

5.4 Intruder detection systems deployed and monitored

This requires a sophisticated barrier beyond the facilities offered by a 'firewall' to protect the organisation from electronic attack or infiltration. To provide the depth of security required to protect assets, supplementary solutions must be deployed to include an investigative capability to monitor, analyse and counter unauthorised activities.

5.5 **Access to systems controlled in accordance with policy**

To control access, a combination of user standards, hardware and software controls need to be employed. The ability to lock hardware facilities is important to ensure that the system is protected and data are not used or copied in an inappropriate manner, or deleted either accidentally or deliberately; but beyond that clear user guidelines and requirements are essential. Therefore, from inception, all systems and applications will have a documented security profile and set of security standards compiled and these will be used to educate and inform users, as well as providing a basis for monitoring, auditing and regulating usage.

5.6 **Solutions to ensure authentication and authorisation implemented**

PITO has recommended a solution that is based upon a Public Key Infrastructure (PKI) to provide encryption between users – although other types of encryption are available. This involves an active directory structure that should enable authentication and authorisation to be addressed on all devices. In addition, solutions must be employed to address the need for secure, remote access to the internal network through the internet.

5.7 **Anti Virus solutions deployed and managed**

Thames Valley Police has anti virus solutions in place on the perimeter of the network and incorporated as part of the standard desk top specification. To build resilience and resistance to attack, a parallel solution must be incorporated and it is essential that these remain actively deployed and up to date. In defining solutions to combat viruses, internal introduction through peripheral devices or data storage medium must be considered.

5.8 **Solutions to ensure protective marking deployed**

Protective markings are defined within the Government Protective Marking Scheme (GPMS) and comprise four main classifications of RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. There is a need to develop systems and applications to allow endorsement of GPMS by default, and to ensure that printed documentation contains the requisite marking. Linked to this must be an understanding that non-designated systems and applications are suitable for processing data classified no higher than RESTRICTED.

5.9 **Appropriate audit controls deployed**

Effective and regular auditing of systems is important to monitor and control access, and both manual and software solutions must be employed to prevent, detect and resolve security weaknesses.

5.10 **Segregation of assets of differing values managed**

GPMS standards include the need to apply different security and storage requirements to data having a different value or classification. This includes an assessment of the vulnerabilities associated with aggregation or dilution of assets, and adoption of preventative measures including use of designated secure networks and routine application of clear desk and need to know principles.

5.11 **Appropriate encryption solutions deployed**

Encryption is required to support storage and transmission of data and product specification must be approved by CESG. Encryption key material must be properly managed and secured and clear responsibility established for this function, including appropriate vetting for the staff concerned.

5.12 **Independent health checks commissioned**

Independent health checks need to be implemented at regular intervals to confirm the integrity of systems and preventative measures. A complementary series of internal and external, random and targeted, checks and audits must be programmed to satisfy both internal requirements and those of the CSP.

6.0 **Preventative Measures and Standards**

6.1 **Implementation**

The combination of IT and Information security procedures requires a general awareness and acceptance of responsibilities by all users. However, setting the control parameters and specifications, particularly those depending upon a technical solution, is a joint ICT Group and Force Security responsibility and as such will be a mandated requirement within any related project.

6.2 **Security Standards**

A standard format will be used to compile a system or application profile together with security standards to stipulate user requirements. These documents will be owned by the Force Security Unit and the Information Security Officer will liaise with the Project Manager to obtain the relevant information.

6.3 **Accreditation Document Set (ADS)**

Where systems are being developed for use within or across the police service in general, adoption is dependent upon compliance with certain security standards and accreditation. The ADS supports this process and comprises a series of policy and procedural documentation as well as risk assessment. It is the responsibility of the project manager to compile relevant documentation and this will be supported by the Information Security Officer who will present draft documentation to the Force Security Manager for approval.

6.4 **System and Data Ownership**

A senior manager will be nominated to be the system and / or data owner in all cases. The nominee will contribute to the creation, maintenance and implementation of security standards and audits.

6.5 Asset Register

Accountability for assets helps to ensure that the appropriate level of protection is afforded and maintained. Therefore all major assets used for or in support of processing the organisations information will be listed in an inventory of assets and compilation will be the responsibility of:

- **ICT Department**
 - Computer hardware including desk top computers, laptops, printers and servers
 - Communications equipment including radios, mobile telephones and PDA's
 - Software and licenses including that relating to applications, systems, development tools and utilities
- **Area and Department Business Managers**
 - Locally purchased hardware and software including a record of issue and return

6.6 Penetration tests

Periodically externally sourced penetration tests will be undertaken to simulate the activities of an unauthorised intruder in attempting to gain access to the network and any system or application. Any risk of intrusion into sensitive systems or data is managed by using CESH approved testers and setting clear parameters regarding supervision and permission phases. Authorisation for the tests will be obtained from a Chief Officer and they will be undertaken without general communication to users. The outcome of the tests will be reported to the Force Security Committee.

6.7 Access to Systems

Access to systems by staff or non-police personnel will not be permitted until after satisfactory completion of vetting and allocation of a staff number. Thereafter, access permissions will be granted on the basis of role and business need as defined in the system security standard. Designated system owners will be responsible for introducing procedures to withdraw access permissions immediately after a person leaves the organisation or role for which access was granted.

6.8 Training and Awareness

It is the responsibility of the designated system owner to ensure that users are given appropriate training and security briefing before being given access to the system. IT Training must ensure that current security procedures are included within training sessions and manuals, and all students will receive a specific briefing about confidentiality, computer misuse, unauthorised access to information and related criminal or disciplinary implications.

6.9 **Monitoring at Work**

Use of systems, applications and data will be monitored using software and manual checks to detect unauthorised, inappropriate or unlawful use.

6.10 **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.

6.11 **Documentation**

Security policy and standards will be documented and approved by the Force Security Committee. All activity relating to security measures and decisions impacting upon people will be documented.

7.0 **Communication**

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

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

8.0 **Compliance and Certification**

8.1 **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.

8.2 **Human Rights**

8.2.1 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.

8.2.2 It is acknowledged that this policy has the potential to engage Article 8, Right to respect for private and family life. However, the legitimacy for the engagement is provided within the text which states: there shall be no interference by a public authority with the exercise of this right such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety ... for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights or freedoms of others. (Human Rights audit completed on 1 March 2005).

8.3 **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).

8.4 **Data Protection**

8.4.1 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).

8.4.2 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.

8.5 **Official Secrets Acts**

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

8.6 **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.

9.0 **Monitoring and Review**

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