Please click here for related Policy Statements

CORPORATE INFORMATION MANAGEMENT DEPARTMENT

Document Title:	Information Security Manual
Reference Number:	HD/9202/ISP/10
Author:	Gareth Davies
Revision:	Version 10
Date:	06.04.2011
Supersedes:	Version 9. 25.11.2009

CONTENTS

INTRODUCTION

This Manual is designed to achieve appropriate protection for information whether held on paper or electronically, whether corporate or operational, and including evidence.

The document is modelled on the British Standard "Information Security Management" BS7799-1 and –2:1999 (Part 1 of this is also referred to as BS ISO/IEC 17799); this is in turn consistent with the Security Policy Framework (SPF).

This policy is the constabulary's response to the issues raised in the British Standard document and the Security Policy Framework.

The policy is intended to be generally valid for all of the constabulary's information. It will be supplemented by a Security Operating Procedure (SyOP) for each system, and exceptions to the general rule will be identified and dealt with there.

This document is intended as a reference document for all members of the Constabulary, South West One (SW1) and partner organisations that have access to Avon and Somerset (A&S) constabulary systems and applications.

1 Scope

1.1 The purpose of the Information Security Policy is to protect the business of the A&S.

1.2 It is the duty of every member of A & S, and every person handling A & S information assets, including contractors, temporary staff, and visitors, to conform with this policy.
Failure to do so may:

a) Result in discipline proceedings
b) Amount to a criminal offence
c) Result in exposure to liability at civil law for compensation for individuals and / or the Constabulary.

1.3 It affects all information controlled by members of the Constabulary, whether based on paper, computers or other media. It refers also to the use by members of the Constabulary of information belonging to other organisations and to data sharing agreements in which the Constabulary is engaged.

1.4 A number of organisations whose employees are not A & S employees may subscribe to the A & S network, provided that they conform with this policy and subject to an agreed Network Affiliation Agreement (eg Police Authority, staff associations, Air Support Unit, Crown Prosecution Service and Magistrates Courts staff.).

2 Terms and Definitions

2.1 Information Security is the preservation of confidentiality, integrity and availability of information.

2.2 Risk Assessment is the assessment of threats to, impacts on, and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

2.3 Risk Management is the process of identifying, controlling and minimising or eliminating security risks that may affect Technical Services for an acceptable cost.

2.4 See also Glossary section.

3 Information Security Policy

3.1 This document is the policy of the Chief Constable. It supersedes all previous policies in the area of Information Security. It is published to all employees. It should not be released outside the organisation without the express authority of the Information Security Officer.

3.2 The purpose of the policy is to protect the business of the constabulary by protecting the confidentiality, integrity and availability of information, and by providing evidence of trustworthiness in information sharing arrangements. More specifically the policy is intended to:

a) Minimise the impact of security breaches
b) Reduce or avoid threats
c) Reduce vulnerabilities
d) Detect the occurrence of security breaches
e) Recover from security breaches.

3.3 This policy is owned by the Head of Corporate Information Management Department through the ISO. These policy documents will be reviewed, or as otherwise called for. Original documents will be retained by the ISO.

3.4 This version of the document supersedes Version 9 of this document.

3.5 This policy will be enforced by reference to internal discipline processes and, where appropriate, by reference to the law. The compliance process is detailed in 12 below.

3.6 This policy requires a number of authorities to be given in writing. The documents arising must be centrally retained in the District/Department so as to be capable of production at audit unless otherwise specified.

4 Security Organisation

4.1 Information Security Infrastructure

4.1.1 Management of Information Security

4.1.1.1 The forum for management discussion of Information Security will be the Change Management Executive (CME). This will be supported by a Strategic Information Management Board (SIMB) of practitioners and stakeholders, and by the Information Security Officer (ISO).

4.1.2 Information Security Coordination

4.1.2.1 An ISO post exists within Corporate Information Management Department. The purpose of this is to provide specialist services, coordination and advice in relation to Information Security. This post also incorporates the Force Vetting Officer role and has number of Assistants.

4.1.2.2 A Security Administrator post exists within the TS. The purpose of that post is to coordinate technical security issues and to administer technical security measures (such as firewalls) on a day-to-day basis.

4.1.3 Other Information Security Responsibilities

4.1.3.1 An audit facility, comprising three members of staff exists within the Corporate Information Management Department and is responsible for auditing Information Security.

4.1.3.2 The Information Security Team includes an Assistant Information Security Officer who will be responsible as Force Crypto Custodian.

4.1.3.3 Responsibilities of staff in relation to Information Security are as follows:

Senior Information Risk Owner

a) Information governance, including Risk Management including accepting significant (or greater) risks on behalf of the Constabulary
b) Ensure that the Constabulary complies with the necessary standards

District Commander/Departmental Head

a) System owner for information facilities (if solely within that unit – post holders nominated for facilities which are shared by more than one District/Department) – includes "owning" SyOps and risks relating to the system
b) Awareness of law, policy and the Security Policy Framework
c) Ensure that District / Department staff are aware and conforming with law and policy
d) Identify / appoint Super User for all systems serving more than one user
e) Identify / appoint Data Protection Liaison Officer
f) Authorises changes to systems

Super User

a) Not normally a user or a technical specialist
b) Day-to-day management of the system by reference to facilities within applications and configuring infrastructure)
e) Authorise and facilitate access to the application (liaising with technical specialists for access to infrastructure) also deals with revocation and modification – including maintaining records
f) Liaison with technical specialists
g) Normally involved in change handling process, including testing and implementation
h) Arrange training for new users
i) May be responsible for backup process
j) Report security incidents and risks to the Information Security Team as soon as practicable, by any available means.
k) May be super user for more than one system.

User

a) Obtain suitable training; seek appropriate advice if unsure
b) Maintain awareness of systems, and comply with relevant law and policy
c) Report security risks and incidents to the ISO (Ext 66168)
d) Securely retain ID card and produce it when requested.

Note: Users will not undertake technical or semi-technical tasks. Users will not move equipment.

Head of Corporate Information Management Department

a) Provide advice on all matters relating to information law, particularly the Data Protection Act and Freedom of Information Act, including disclosure of information
b) Ensure legitimacy of Technical Services
c) Arrange appropriate auditing of systems
d) Provide an appropriate service for Subject Access requests
e) Ensure that staff are suitably trained in relation to information law.

Information Security Officer

a) Accrediting new additions and changes to the Force network.
b) Providing advice and liaison for users, technical specialists and members of other organisations on Information Security matters, including cryptographic security
c) Maintaining a suitable level of security awareness
d) Identifying and assess risks to information security, initiating the implementation of suitable safeguards, monitoring the operation of security controls
e) Investigating security breaches and incidents
f) Receiving and appropriately disseminating Security Alerts
g) Maintaining a Security Policy
h) Develop and maintain a list of Exceptions to this policy
i) Initiate Risk Analyses in exceptional cases
j) Accept minor risks

Note: these functions may be delegated within the Information Security Team.

TS Security Administrator

a) Defining requirements for technical security
b) Implementing, publicising and maintaining effective levels of technical security
c) Implementing and managing appropriate firewall technologies
d) Providing effective security measures against incursion
e) Tracking and investigating breaches of system security and reporting to the ISO
f) Take primary responsibility for the key management (encryption)
g) Acting as an advisor within IS and to the Force in general on the maintenance of effective technical security

TS Service Desk Manager

a) Respond to calls from users for technical or other support
b) Ensure that calls which disclose security incidents and risks are passed to the ISO
c) Ensure that records are kept of preventive and corrective maintenance

Crypto Custodian

a) Take a lead in all matters relating to cryptography
b) Ensure compliance with policy
c) Management and accounting in relation to all cryptographic material in the force
d) Emergency action as necessary
e) Incident reporting including investigation and recovery

4.1.3.5 A System Owner will be identified for each information handling facility. Normally this will be the District/Departmental Commander controlling the relevant work. Where the facility affects several areas, then a specific agreement will be reached.

4.1.3.6 Authorities and responsibilities defined in this policy may be delegated unless the

contrary is stated.

4.1.4 Authorisation Process for Information Processing Facilities

4.1.4.1 Information processing facilities will be installed only with the authority of the Force Change Management Executive. This approval depends upon a Certificate of Accreditation issued by the Information Security Officer.

4.1.4.2 In the event of a dispute arising from a refusal of the ISO to sign a certificate, appeal may be made to CME.

4.1.4.3 Applications for CME approval will be submitted in writing via the Head of Information Services. They will be in the form of a business cases indicating the purpose, an indicative cost (and the funding arrangements), timescale and resource issues, and including the signature of the senior user.

4.1.4.4 Approval will identify the System Owner, and will always be conditional upon schemes for testing and training, and upon the provision of documentation including User Requirement, User Guide, Technical Specification, Risk Analysis and System Operating Procedures. Approval will refer to this Information Security Policy.

4.1.4.5 Approval will not be granted until an appropriate technical assurance has been signed by the relevant specialist in the TS.

4.1.4.6 All contracts for procurement of equipment (including software) and services relating to information will be through staff who are authorised to conclude contracts from the Purchasing and Supplies Department. Any exceptions to this rule will be formally authorised by the Technical Services Programme Executive. Computer and communications equipment must be procured via TS department.

4.1.5 Specialist Security Advice

4.1.5.1 The ISO will generally provide specialist security advice, on demand or on his/her own initiative. It may be necessary to obtain more specialised or authoritative advice, it will be necessary to obtain the services of consultants. Where this is done, the cost will normally be borne by the project which raises the need.

4.1.5.2 The following will be regarded as authoritative sources of guidance:

a) Law
b) British Standards
c) HMG Infosec Standards
d) Communications-Electronic Security Group (CESG) advice
e) UK IT Security Evaluation and Certification Scheme Certified Product List
f) Security Policy Framework
g) ACPO Code of Practice for Data Protection
h) ACPO Data Protection Audit Manual
i) Codes of Practice for Data Protection (e.g. CCTV).
J) Management of Police Information (MoPI)

4.1.6 Coordination between Organisations

4.1.6.1 The ISO will be responsible for ensuring that appropriate contacts are maintained with other government organisations, other organisations concerned with criminal justice, service providers, consumers of police information, and members of the Constabulary, including representative forums.

4.1.6.2 Exchanges of security information will be limited so as to ensure that sensitive information is not passed to unauthorised persons.

4.1.7 Independent Review of Information Security

4.1.7.1 An internal audit facility is described in 12.3. below;

4.1.7.2 From time to time, an independent review of the implementation of this policy may be procured to provide assurance that organisational practices reflect the policy and that it is feasible and effective. The review will be carried out by a service provider selected from the CESG Listed Adviser Scheme.

4.2 **Security of Third Party Access**

4.2.0 Disclosure of Police Information

4.2.0.1 Disclosure of police information to third parties is widely sought, formally and informally.

4.2.0.2 Generally, the Constabulary will respect the confidentiality of information in its possession. Disclosure will be permitted in the course of preventing crime, investigating offences and prosecuting offenders. Disclosure of personal information may take place with the consent of the individual/s to whom it relates. Disclosure may be required by law.

4.2.0.3 The Constabulary will not normally disclose personal information for the purpose of research.

4.2.0.4 The decision whether to disclose or not is to be made on a case by case basis there can be few blanket rules. A useful general approach is:

a) The law (Data Protection Act 1998) generally forbids police to disclose personal information to anyone

Unless

b) The subject consents

Or

c) It is necessary to a criminal investigation or prosecution, or to prevent crime (Section 29(3))

Or

d) Some law is identified which compels or at least permits disclosure.

But note that where police are *permitted* to disclose, the “human rights” factors of lawfulness, reasonability and proportionality must be considered before the decision is made.

4.2.0.5 In wholly exceptional cases an Assistant Chief Constable (or above) may authorise disclosure where he is satisfied that it is in the public interest.

4.2.0.6 In the first instance, disclosure issues will be decided by nominated officers at each District / Department.

4.2.0.7 In the event of difficulty, advice may be sought from the Corporate Information Management Department. That Unit will have access to the relevant protocols, contracts and agreements.

4.2.0.8 Improper disclosure can attract liability at criminal and civil law, as well as disciplinary proceedings. Best advice is therefore to disclose only when certain that it is proper to do so.

4.2.0.9 It is occasionally necessary to publish (by internet or in the media via the Press Office) personal information in an effort to detect offences and/or apprehend offenders (e.g. Crimestoppers).

4.2.0.10 Un-convicted images of offenders may not normally be published. In exceptional cases ACPO authority is obtained (in the public interest). This authority may be obtained via the Corporate Information Management Department.

4.2.0.11 Reference should be made to the Crown Prosecution Service before a decision is made to publish.

4.2.0.12 Where publication is contemplated, the accuracy of the information (and the correctness of the photograph) is critically important (double check information; consider PNC check at a late stage).

4.2.1 Reasons for Access

4.2.1.1. Generally, the systems of the constabulary will be available to members who have a business need.

4.2.1.2 Where the constabulary engages contract staff and temporary staff, they will be treated in the same way as ordinary members of staff (including vetting and access aspects). Section 9 below gives details for allocating passwords and user identities.

4.2.1.3 It will be possible for the constabulary to treat certain other organisations as if they are of staff (see 1.4 above), where a business case is identified. In such cases, the visitors" will be subject to this policy and the arrangement will be governed by a Service Level Agreement.

4.2.1.4 It will be necessary to employ the services of commercial organisations (e.g. software support, and hardware support). Access may be logical or physical. Access will be granted only where a business need for it outweighs the risks.

4.2.1.5 It will not be permissible to pass police information to third party organisations other than as defined by the SyOPs. This includes sharing information with other constabularies. In exceptional circumstances, the authority of the ISO or the Corporate Information Manager or the Corporate Information Management Department Senior Auditor may be sought.

4.2.2 Security Requirements

4.2.2.1 Irrespective of business need, persons will not be given access to police information or systems unless a formal agreement exists, defining responsibility and agreeing to vetting. A copy of agreements will be forwarded to ISO.

4.2.2.2 Irrespective of business need, persons will not be given unsupervised access to police information or systems unless they have been appropriately vetted.

4.2.2.3 Irrespective of business need, persons will not be given access to police information or systems unless they have read the Information Security Notice and signed an A&S Access to Information Form.

4.2.2.4 Where Third Party organisations are used to process data, the organisation must complete and sign an A & S Data Processing Form prior to any work being undertaken. The agreement will be signed on behalf of the company requiring access and will list the personnel needing access.

4.2.2.5 Where there is a need for a third party to take possession of A & S equipment, the following criteria will be applied:

a) Equipment will be asset tagged/shown on inventory
b) Proposed location will be assessed for physical security
c) Third party will undertake responsibility for compliance with the law in respect of that equipment through a Data Processing Agreement
d) Third party will undertake responsibility for replacement of missing equipment (viz insurance)
e) Third party will clearly understand that there is no authority to pass possession on without written authority (and repetition of these criteria)
f) Ownership will remain with A & S
g) Return date will be set (amendable in writing)
h) Instructions for handling media will be given
i) Data Protection and Information Security Officer will be consulted
j) The third party will indemnify the Constabulary against loss brought about as a result.

4.2.2.6 The requirements of 4.2.2.2, 4.2.2.3, 4.2.2.4 and 4.2.2.5 above may be avoided in the following exceptional circumstances with the authority of the Technical Services Manager or the Network Services Manager:

a) Where the service provider is a List X company
or
b) Where the individual concerned can be personally supervised by a member of the Constabulary
c) Where the individual concerned has been cleared to a level which is appropriate for the classification of information (normally Basic Check)
d) Where exposed information is unclassified
e) Where the contract for the services specifies that individuals employed are suitably cleared.

4.2.2.7 In all cases, security requirements will be included in a formal contract which reflects the rules in this policy, and which details goods and services to be provided. These requirements will be formulated to ensure that all parties, including sub contractors are security cleared, and that they are aware of their responsibilities for security.

4.2.2.8 The contract will provide for auditing by A & S of the processes and work of the supplier when on A & S premises.

4.2.2.9.1 It will be Best Practice to include a clause in the contract which indemnifies A & S against costs incurred in the event that a supplier improperly handles (e.g. discloses) police information.

4.2.2.10 It will be Best Practice for the contract to refer to Business Continuity Planning.

4.2.2.10 The contract will specify circumstances under which police information can be copied and/or disclosed.

4.2.2.11 It will be Best Practice for contracts to specify targets and unacceptable levels of service in delivery and/or support, as well as methods for monitoring.

4.2.2.12 Contracts for the development/delivery of software will provide for intellectual property rights and copyright assignment.

4.2.2.13 Contracts should address any requirement for third parties to have special rights of access to systems, including electronic diagnostic links, higher levels of rights of administration of systems. They should also specify measures to be taken in the event of breach of these rules. They should specify hours of access.

4.2.2.14 Contracts will specify escalation procedures in the event of problems. It may be appropriate to consider contingency arrangements.

4.2.2.15 Contracts will specify arrangements for Change Control between contract and Acceptance.

4.2.2.16 Contracts will specify the Acceptance process.

4.2.2.17 Breach of the terms relating to security will be capable of being regarded as a fundamental breach of the contract.

4.2.2.18 Before concluding a contract, the procurer will assess the commercial stability of the supplier.

4.2.2.19 The "owner" of the system will be responsible for ensuring that access by third parties is monitored, and for initiating a solution in the event of difficulty.

4.3 Outsourcing

4.3.1 The Constabulary relies upon South West One to provide services in the following business areas:

- Information Services (except radio) (since 1st June 2008)
- Personnel (since 1st July 2008)
- Estates (since 1st July 2008)
- Purchasing and Supplies (includes procurement) (since 1st July 2008)
- Administration (includes operational stations' Enquiry Office (i.e. reception) facility (since 1st July 2008).

4.3.2 South West One is a Joint Venture Company in the nature of a partnership consisting of the constabulary together with Somerset County Council, Taunton Deane Council, and IBM. IBM is the major stakeholder. It is anticipated that other stakeholders will join this partnership.

4.3.3 The Contract for this arrangement pays particular attention to Information Security (see Schedule 39). The Joint Venture Company is thus committed to Police Information Security Policies, including policies on Vetting, that were effective at the date of contract (March 2008), including providing assistance throughout the Information Security Accreditation regime.

4.3.4 As a result, there will be no deterioration in standards of Information Security as a result of this change.

4.3.5 The network arrangements, including connection to Internet and Criminal Justice extranet, are unchanged. Any future changes will be managed in accordance with existing security standards.

4.4 Risks

4.4.1 Risks may be identified in a variety of ways, including discovered by users or technical specialists, arising from changes within the Force and outside, and arising from incidents for example.

4.4.2 Minor Risks may be accepted by the Information Security Officer. Moderate Risks may be accepted by the system owner. Significant or High risks must be accepted by the Senior Information Risk Owner.

4.4.3 Risks will be documented and the original documentation will be retained by the ISO.

4.4.4 Technical risks will be documented in accordance with HMG Infosec Standard 1.

5 Asset Classification and Control

5.1 Accountability for Assets

5.1.1 Inventory of Assets

5.1.1.1 The ISO will maintain an inventory of information assets, including continuity plans. Each District Commander/Departmental Head will be responsible for maintaining an inventory of formal documents which it publishes (eg Training Manuals by Training Department). Manuals and documentation will be retained by the senior officer or his/her nominee. (See also 8.4.1 on “backup copies” of electronically held information.)

5.1.1.2 The Technical Services Resource Management System Administrator will be responsible for maintaining an inventory of hardware and software, including network hardware and software, telephony and radio equipment.

5.1.1.3 Items of physical equipment which are included in the inventory will have an “Asset Tag” indicating the Force and a unique number affixed as part of the installation notice. This number will then serve as the main method of identifying the equipment.

5.2 Information Classification

5.2.1 Classification Guidelines

5.2.1.1 Information held within the force will be subject to the instructions of the current version of the Security Policy Framework as distributed by the Cabinet Office Security Division.

5.2.1.2 It will not be necessary to classify documents which are already in existence at the date of implementation).

5.2.1.3 Markings (including Descriptors) will be chosen only from the Manual. Local Code words are acceptable in accordance with the Manual.

5.2.1.4 Responsibility for the classification of information lies with the author. It is his/her responsibility to classify and change the classification during the life of the material.

5.2.1.5 Where staff receive information and doubt its classification, queries (including attempts to persuade him/her to reclassify) will be addressed to the author. Responsibility remains with him/her.

5.2.1.6 In case of dispute with the original author, staff should refer to his supervisor/manager.

5.2.1.7 Except for identified units, staff below the rank of Inspector (and Support Staff equivalent grade SO2) classifying a document above RESTRICTED will obtain approval from a supervisor. Approving supervisors will initial the classification and append their Force number. Approval should not be given unless there is reason to believe that the criteria apply.

5.2.1.8 Most police information is likely to be marked RESTRICTED. Informants' personal details, paedophiles' identities and modus operandi in a few serious cases are likely to be marked CONFIDENTIAL. A small proportion of the Force's computers will be geared to handling information above Restricted (e.g. HOLMES2, ViSOR & PND).

5.2.2 Information Labelling and Handling

5.2.2.1 Information will be labelled in capital letters and handled in accordance with the Security Policy Framework. It is not intended to reproduce that manual in this policy, however important points will be highlighted in the following.

5.2.2.2 The Need to Know principle is central to the handling of information. Information must be available only to those who "Need to Know".

5.2.2.3 The Baseline Classification of information held by a system will be shown in a log-on screen.

5.2.2.4 All forms can be regarded as NOT PROTECTIVELY MARKED when blank. The printed marking applies to the completed form only.

5.2.2.4 Material marked CONFIDENTIAL or above must be accounted for at all times. When information marked CONFIDENTIAL or above is created or received from another organisation, its existence will be notified to HQ Special Branch, where a register will be maintained. Subsequent movements, the making of copies and the destruction of the material will also be notified.

5.2.2.5 Loss of material which is Protectively Marked implies an embarrassing neglect of duty and is likely to attract disciplinary action. Loss will be reported as an Information Security incident in the first instance and will be reported to affected managers. Note that loss implies neglect, while covering up a loss is considered as a deliberate act against the interests of the Constabulary.

5.2.2.6 Protectively marked material will be held securely in containers (e.g. locked desk). Where material is marked no higher than RESTRICTED, and it is impossible to follow this rule, it will, for the time being, be acceptable to hold it in an unlocked container providing that the door/s of the room are locked and access is available only to members of that unit.

5.3 Retention and Destruction

5.3.1 Retention Policy is detailed in a separate document.

6 Personnel Security

6.1 Security in Job definition and resourcing.

6.1.0 Security responsibilities will be incorporated in all future contracts and monitored during employment. The methods will be as follows:

6.1.1 Job Descriptions

6.1.1.1 Job descriptions are documented and published in the Constabulary. They will reflect this Policy (see Responsibilities in 4.1.6.2).

6.1.2 Personnel Screening

6.1.2.1 A separate policy defines a Vetting regime in accordance with the ACPO / ACPOS document, the "National Vetting Policy for the Police Community".

6.1.3 Confidentiality Agreements

6.1.3.1 All staff will be issued with a Notice as part of accepting the offer of a post. This includes existing staff transferring to a new post.

6.1.3.2 Third parties users (eg Crown Prosecution Service staff) and casual staff and providers of services will sign agreements prior to being given access to information processing facilities.

6.1.3.3 Staff are not entitled to use police systems for private purposes. Generally (e.g. telephone, mobile 'phone, fax, e-mail and internet) they may be permitted to do so on condition that they accept that there is no expectation of privacy. Systems will be monitored for the purposes of:

- Formal investigation of complaints.
- Maintaining discipline.
- Criminal enquiries.
- Providing evidence of transactions.
- Providing evidence of other communications to establish facts.
- Ascertaining compliance with regulatory practices and procedures.
- For audit purposes.
- Detecting the unauthorised use of electronic communication systems.
- Protecting the network against malicious software/ code incidents, service denial and unauthorised penetration attacks.

6.1.4 Terms and Conditions of Employment

6.1.4.1 Terms and Conditions of employment will clearly state the need for vetting, the responsibility for information security, and will refer to the discipline procedures.

6.2 User Training and Publicity

6.2.1 Information Security Education and Training

6.2.1.1 Every opportunity will be taken to educate users in relation to security.

6.2.1.2 New staff will be supplied with a copy of the Notice during the recruiting process.

6.2.1.3 Staff will not be granted access to assets unless and until they receive appropriate training. However, in the case of short term temporary staff and other exceptional cases, temporary access may be authorised.

6.3 Responding to Security Incidents and Malfunctions

6.3.1 Reporting Security Incidents

6.3.1.1 All problems relating to computers will be reported to the IS Service Desk via Extension 66480, electronically or in person. Reports will include the following details:

a) Person reporting and contact number/arrangements
b) Details of system, including A & S asset tag from equipment concerned
c) Details of problem: including error message/s in full, other manifestations, time, date, place, activity engaged, whether the problem is capable of being replicated, whether it is thought to have occurred previously.

6.3.1.2 The Service Desk offers a 24 hour service (with electronic call queuing as necessary).

6.3.1.3 The ISO will have access to the information as reported, and will identify any security incidents.

6.3.1.4 All other security incidents will be reported in writing, electronically or by telephone to the ISO.

6.3.1.5 A Security Incident is defined in 8.1.3.1 below.

6.3.2 Reporting Security Weaknesses

6.3.2.1 All security weaknesses will be reported in writing, electronically or by telephone to the ISO. These will be investigated by the ISO, with the assistance of any appropriate technical resources.

6.3.2.3 Users will not attempt to prove or demonstrate that there is a weakness by exploiting it. To do so may amount to misuse of the system.

6.3.2.4 Centre for the Protection of National Infrastructure (CPNI) Alerts will be forwarded to the ISO promptly and be assessed for an appropriate response.

6.3.3 Reporting Software Malfunctions

6.3.3.1 Software malfunctions will be reported in the same way as any other computer problem to the IS Service Desk, as in 6.3.1.1.

6.3.3.2 The following information will be included in this type of report:

a) Person reporting and contact number/arrangements
b) Details of system, including A & S asset tag from equipment concerned
c) Details of problem: including error message/s in full, other manifestations, time, date, place, activity engaged, whether the problem is capable of being replicated, whether it is thought to have occurred previously.

6.3.3.3 Use of affected equipment should cease until further specialist advice is obtained from the Service Desk unless there are urgent and important operational reasons to the contrary. Users will be aware that further use of the system may well impede any investigation of problems.

6.3.4 Learning from Incidents

6.3.4.1 Primary purposes of the processes for handling incidents and weaknesses are to learn from them to prevent recurrence or development of the problem, and to implement “fixes” promptly and efficiently, in order to protect the business of the Force.

6.3.4.2 The ISO will be responsible for analysing the incidents in order to identify trends, formal Risk Analysis if appropriate, and initiating preventive action and in order to provide management information.

6.3.5 Disciplinary Process

6.3.5.1 Disciplinary processes exists for police officers and police staff. The process for police officers is defined in Police Unsatisfactory Performance, Complaints and Misconduct Procedures issued under Police Act 1998. The process for Police Staff is defined in an A&S document “Disciplinary Procedure”.

6.3.5.2 The investigation and analysis of Incidents may demand that this formal process be invoked. But where Incidents:

a) Are not repetitive
b) Do not suggest corrupt or malicious behaviour
c) Result in no serious damage
and
d) Result in no adverse publicity the ISO may instead consider giving advice. He/she may consider drawing the attention of the appropriate District / Departmental Commander.

6.3.6 Incident Handling

6.3.6.1 The purpose of an Incident Handling scheme is to protect or restore the business of the Constabulary, including learning from incidents.

6.3.6.2 Where an incident poses a threat to partner agencies, it may be necessary to report the matter to them.

6.3.6.3 All incidents, including losses of information assets such as Airwave terminals, are reportable to the NPIA Police Warning and Reporting Point (POLWarp). Where an incident poses a risk to other members of the Criminal Justice community, it is reportable immediately and it may be necessary to disconnect network connections. Where the incident is relevant to other government departments, it is reportable to the Government Computer Emergency Response Team (GovCERT) as maintained by CESG.

6.3.6.4 It will be important to ensure that the right people are aware / involved. The following should be considered:

a) Technical specialist and / or super user and / or system owner from other affected organisation.
b) Super User for affected system (may inform system owner)
c) ISO or IS Security Administrator or Corporate Information Manager or Senior Data Protection Auditor

Where the ISO is not informed at the time, notice of the incident will be sent to his office by fax forthwith on conclusion.

6.3.6.3 Communication by telephone or mobile ‘phone is to be preferred.

6.3.6.4 Actions will be documented, in order to gather evidence of criminal/discipline matters, in order to defend litigation and in order to learn from the incident.

6.3.6.5 Files left or modified by intruders will be copied to a secure media (rather than opened in situ). Where possible, the Technical Support Unit should be consulted for assistance with this evidence gathering. This is intended to establish admissible evidence and to avoid unnecessary virus infection.

6.3.6.6 If there is no less disruptive method available for taking control of a breach, staff handling incidents are authorised to physically disconnect communications routes or take the information handling facility out of use. When this is necessary, affected users will be notified as soon as practicable.

6.3.6.7 In rare and exceptional circumstances, it may be possible to pursue a detection at the cost of allowing a breach to continue. This is a business decision to be made by the system owner or the super user (in consultation with other interested parties). The risks will normally outweigh the benefits of a detection.

6.3.6.8 In the event that an intrusion is detected, the software on all affected machines will normally be completely rebuilt to eliminate the risk that Trojan malicious software has been introduced unless all parties (ISO, IS Security Administrator, and system owner or administrator) agree that there is no risk of this.

6.4 Users – End of Service

6.4.1 It is vitally important to ensure that at the end of the service of a user, assets are recovered and IT accounts are closed.

6.4.2 It is the responsibility of the local immediate manager to identify the end of service and to initiate a checklist.

6.4.3 This Checklist will be passed to the relevant Administration unit. That unit head will be responsible for recovering and disposing of assets (e.g. car park-pass, ID, mobile phone) and passing a copy of the form to IS Service desk.

6.4.4 TS Service desk manager will be responsible for closing accounts as necessary.

7 Physical and Environmental Security

7.1 Secure Areas

7.1.0.1 Police buildings will at all times be secured so as to prevent unauthorised access.

7.1.0.2 The exterior security can be seen as a barrier which prevents access by those who have no known vetting status (or no vetting).

7.1.0.3 Authorised persons will gain access by reference to a token normally a “proximity card” but may be a PIN or code.

7.1.0.4 Certain areas, including communications facilities, custody facilities, offices handling particularly sensitive information and IT equipment rooms demand additional security. Wherever possible, equipment which is depended upon by more than one user, such as servers, hubs, routers, bridges, link equipment, will be sited in a room set aside for the purpose. These areas will be secured so as to prevent unauthorised access (by people who are authorised to enter buildings). Access will be by a token / PIN / code different to that used to access the buildings. (PINs / codes may be shared by installations in the same classification.)

7.1.0.4.1 Head of Administration will be responsible for maintaining registers of tokens. Tokens will be recovered at the end of the authorisation (e.g. when staff leave police employment, or move to other duties), and this will be shown in the register.

7.1.0.5 The Facilities Department will be responsible for making arrangements for the machine room to be cleaned at least quarterly.

7.1.1 **Secure Physical Environment for Confidential Assets (e.g. ISCAS, HOLMES ViSOR & PND)**

7.1.1.1 The crypto material ***must not*** be compromised: damage would be very serious to the force's credibility. The data is also important.

7.1.1.2 Crypto matters will be addressed in accordance with HMG Infosec Standard 4.

7.1.1.3 Crypto assets must be protected from the public by two barriers - normally exterior door and office door or locked cabinet/work area.

7.1.1.4 The asset must be protected from members of the force who have no need to know, or who do not have adequate vetting, by a second barrier (e.g. office door, cabinet or secure work area). Viz not in a shared office.

7.1.2 System Administration

7.1.2.1 Should be carried out in such a way that the administrator is separated from those who lack need to know and those who lack adequate vetting (e.g. separate office or work area) for Data Base Administrators (DBA)s for Confidential systems.

7.2 Equipment Security

7.2.0 Equipment is generally the responsibility of the Technical Services Manager.

7.2.1 Equipment Siting and Protection

7.2.1.1 Equipment will be sited and/or protected so as to reduce the risks from environmental threats and hazards and opportunities for unauthorised access.

7.2.1.2 Equipment will be sited so as to minimise unnecessary access into work areas.

7.2.1.3 Equipment will be sited so as to prevent any risk of being overlooked whilst in use.

7.2.1.4 Staff siting equipment will also consider the following risks in relation to equipment and users of the equipment:

a) Theft
b) Fire
c) Explosives
d) Smoke
e) Temperature
f) Water and dampness
g) Dust
h) Vibration
I) Chemical effects
j) Electrical supply interference
k) Electromagnetic radiation
l) Risk of violence.

7.2.1.5 Users will not eat, drink or smoke in proximity to information processing facilities (including paper information processing).

7.2.1.6 Where users consider that conditions develop which may adversely affect the processing of information, they will report the matter forthwith to the relevant District/Departmental commander.

7.2.1.7 Staff initiating the procurement of equipment will bear in mind the possibility of special protection methods in adverse environments (e.g. Custody Offices, or particularly dusty/dirty/greasy environments).

7.2.1.8 Risks arising from neighbouring environments will also be considered in locating information processing facilities (e.g. fires, leaks or infestations in neighbouring premises).

7.2.2 Power Supplies

7.2.2.1 Power supplies will be provided to conform with the manufacturers' specifications.

7.2.2.2 Equipment supporting more than one concurrent user (e.g. servers, and communications equipment) should be protected from power failures and electrical anomalies.

7.2.2.3 This equipment will be protected by un-interruptable power supply devices (UPS) – preferably "intelligent" devices capable of initiating controlled down time.

7.2.2.4 Contingency plans will be made for UPS failure. UPS equipment will be regularly maintained, checked and tested in accordance with the manufacturers' recommendations. The member of staff responsible for the UPS will arrange the checks in liaison with the IS system administrator.

7.2.2.5 Wherever possible, equipment will ***in addition*** be protected by the provision of generator support for the power supply (this protection will extend to associated necessities such as emergency lighting). All servers and communications equipment will be generator backed. Generators will be tested three times annually (two 30 minute on load tests and one two hour test on load). Adequate supplies of fuel will be maintained: this is the responsibility of the relevant Site Administration. The provision, testing and maintenance of generators will be the responsibility of the Estates Department Engineering Officer.

7.2.2.6 Lightning protection will be applied to police buildings. Lightning protection filters will be fitted to external communications lines.

7.2.2.7 Responsibility for UPS devices will lie with Head of TS for free standing devices and with the Head of Facilities Management Services for those which are hard wired into the power supply of a building.

7.2.3 Cabling Security

7.2.3.1 Wherever possible, power and data cables to/from police premises will be underground. This standard cannot be achieved in every case: it may be an accepted risk where the site is smaller than District Headquarters level.

7.2.3.2 All police-owned data cables to/from police premises which are above ground will be fibre optics. Fibre optic links may also be used in preference to Cat 5 cable (e.g. where distances are too great: often interlinking floors in larger buildings) at the discretion of the Technical Services Manager.

7.2.3.3 Wide area network (WAN) cables may be leased (currently from MLL, BT, C&W and Virgin).

7.2.3.4 Cabling within premises is/will be police owned.

7.2.3.5 Cabling will avoid areas which are accessible to the public.

7.2.3.6 Network cabinets will be secured; accessible only to the appropriate specialists/service providers. The Network Services Manager will be responsible for the security arrangements.

7.2.3.7 Cabling will be contained in purpose built channels, baskets and conduits. It will not be exposed.

7.2.3.8 These arrangements should ensure that there is visible evidence of an attack on cabling. Staff will report any such evidence as a Security Incident in accordance with 6.3.1 above.

7.2.3.9 Data and power cables will be segregated (in accordance with Institute of Electrical Engineers Wiring Regulations 17th edition BS 7671:2008 incorporating all subsequent amendments). Some exceptions exist as part of legacy provisions. Wherever practicable, these provisions will be upgraded. The exceptions will be identified and documented by the Network Services Manager, in order to assess risks.

7.2.3.10 A “Sniffer” device is deployed, mainly as an aid to network management. A programme for sweeping the network for unauthorised devices will be devised. At present sweeping will be carried out by network specialists under the Network Services Manager on an occasional basis.

7.2.4 Equipment Maintenance

7.2.4.1 It will be the responsibility of the Head of the TS to ensure that existing equipment is maintained in accordance with the manufacturer’s recommendations.

7.2.4.2 Any necessary maintenance will be initiated as new systems are procured. The procurement project will fund all maintenance costs to the end of the first year from being taken into live use. Persons procuring systems will be responsible for drawing the attention of the Head of the TS to the costs thereafter and ensuring a smooth transition.

7.2.4.3 Users will be responsible for cleaning equipment in their work areas each month, or more frequently as necessary.

7.2.4.4 Only authorised engineers will move, service or repair equipment.

7.2.4.5 Equipment will not normally be removed from police sites. In those exceptional cases where this proves to be necessary, the following steps will be taken:

a) Staff (including external service providers) will be subjected to Basic Check procedures, including checking identity
b) A responsible member of the organisation providing the service will sign a Data Access Agreement.
c) Copies will be retained by system owner and ISO.

7.2.4.6 The TS Service Desk Manager will maintain record of preventive and corrective maintenance.

7.2.5 Security of Equipment Off Premises

7.2.5.0 This aspect is relevant to portable computers and is found in the document “Security Operating Procedure for Portable Computers”. This document will be issued with all portable computers.

7.3 General Controls

7.3.1 Clear Desk and Clear Screen Policy

7.3.1.1 Information should not be left unattended. Unattended means unattended by a member of police staff who would normally have access to the information contained. So attendance by subordinates, members of other units, or non police personnel will not be acceptable.

7.3.1.2 Classified documents, including removable storage media (including disks and USB Sticks) should be kept in locked furniture rather than left on desks.

7.3.1.3 Computers should not be left unattended whilst logged on, unless they are “locked” and protected by a password.

7.3.1.4 “Time Out” (see 9.5.7.1 below).

7.3.1.5 White boards should be cleared after use.

7.3.1.6 Material on flip charts in common areas (eg meeting rooms) should be removed after use.

7.3.1.7 Care will be taken in decisions about publishing information on notice boards. E.g. Lists of staff addresses/telephone numbers will not be displayed.

7.3.1.8 Information which is unusually sensitive (including some RESTRICTED and all CONFIDENTIAL material and including software) should be stored in approved facilities when not in use.

7.3.1.9 In the procurement of security related items (eg furniture, office equipment and locks) and services, strong preference will be given to selecting from the Security Equipment Assessment Panel (SEAP) Catalogue of Security Equipment published by the Cabinet Office, or from items approved by General Information Assurance Products and Services Initiative (GIPSI).

7.3.1.10 Unit heads will arrange for a member of staff (normally a supervisor) to take responsibility for monitoring all areas for which they are responsible. This Responsibility will include occasional checks involving visiting the areas (at least weekly). Breaches of this policy which are not malicious may be dealt with informally with advice in the first instance, although repeated infringements may indicate a need for the monitor to take possession of vulnerable material; and possibly to report members of staff to line managers.

7.3.2 Removal of Property

7.3.2.1 Neither equipment nor information (on paper or other media) will be removed from police premises without authority conferred in documented policies or procedures, or given in writing on an individual basis by District/Departmental Commanders.

7.3.2.2 Procedures or authorities should specify the return of the equipment or information.

7.3.2.3 Security staff will conduct occasional random or targetted spot checks to ensure compliance and will maintain records of these checks.

8 Communications and Operations Management

8.1 Operational Procedures and Responsibilities

8.1.1 Documented Operating Procedures

8.1.1.1 A general Operating Procedure will be produced. An Operating Procedure will also be produced for each of the systems in use in the Constabulary. The documents will be maintained and reviewed bi-annually or more frequently if otherwise necessary. Each will be signed by the relevant system owner.

8.1.1.2 All members of staff will comply with these procedures. In the same way as this Policy, failure to do so may attract liability at civil or criminal law, and / or disciplinary action.

8.1.2 Operational Change Control

8.1.2.1 Changes to information processing facilities will be rigorously controlled. Inadequate control of change is a common cause of damage to the business of the Constabulary.

8.1.2.2 Changes will not be introduced to operational use without prior Acceptance Testing (detailed below in 8.2.2).

8.1.2.3 Proposed changes will be put into writing. Adoption will depend upon the written approval of:

a) The District/Departmental Commander or owner of the system
b) If separate the appropriate budget holder
c) Technical assurance (including impact assessment)
d) The provider of any resources necessary for procurement, production, implementation and/or training (bearing in mind that a user being trained must normally be removed from their normal duties).

8.1.2.4 Care will be taken to ensure that all relevant parties are notified of change.

8.1.2.4 The implementation planning will include identifying fallback procedures for aborting and recovering in the event that the change is unsuccessful.

8.1.3 Incident Management Procedures

8.1.3.1 A security incident is any event such as a security breach, threat, weakness or malfunction which has or could have resulted in the loss or damage of information assets including:

a) Accidental or deliberate destruction of information
b) Accidental or deliberate modification of information
c) Accidental or deliberate disclosure of information
d) Deliberately causing the unavailability of Technical Services
e) Unauthorised access to Technical Services
f) Misuse of information
g) Theft of any information asset
h) Any other event which affects information security.

8.1.3.2 The objectives (in descending order of priority) in the event of an incident will normally be:

a) To remove any ongoing threat
b) To recover any missing assets
c) To restore the business process
d) To investigate in order to prevent recurrence
e) To consider criminal / civil / disciplinary action.

In exceptional circumstances (such as of recurring malicious acts), a decision may be made by the ISO in agreement with the senior user available and the relevant technical specialists to pursue an investigation as a higher priority.

8.1.3.4 Details of the mechanisms for reporting and discovery of incidents are given at 6.3.1 above. Note that incidents may also come to light in the course of auditing or managing equipment (such as firewalls), in the course of discipline investigations and occasionally in the course of criminal investigations.

8.1.3.5 SyOPs will contain detailed procedures for:

a) Failures / loss of service
b) Denial of service
c) Errors from incomplete/inaccurate business data
d) Breaches of confidentiality.

8.1.3.6 The TS technical specialist leading the solution will identify the cause. In the event that he/she considers recurrence likely, it will be his/her responsibility to highlight the matter to the Information Security Officer.

8.1.3.7 Where it is necessary to invoke disciplinary action (including criminal action against employees of the Constabulary), it will be the responsibility of the Information Security Officer to take the appropriate action to initiate it.

8.1.3.8 Where he/she considers a criminal investigation against a member of the public (or an external organisation) to lead to a successful prosecution (or otherwise necessary, having in mind the costs/resources involved), it will be his responsibility initially to preserve evidence and then to seek the services of the appropriate Technical Support Unit specialists, and Fraud Squad specialists if criminal action is contemplated. The rules for preserving evidence are as follows:

a) Ensure that a local supervisor is informed
b) Ensure that the evidence is not amended (switch off the machine, unless an image on screen amounts to evidence, in which case switch off *monitor only*)
c) Remove machine from force network (ie physically disconnect at wall socket
d) Secure the machine and retain for TSU specialist to gather evidence
e) Notify TSU and Information Security Officer and IS Service Desk
f) If an incident reveals facts/evidence to suggest a criminal offence or corrupt practice, then the duty officer of Complaints and Discipline will be notified.

8.1.3.9 Where the incident involves another organisation, the matter will be reported to the Data Protection and Information Security Manager.

8.1.3.10 Incidents may come to light in the course of normal supervision, audit or as part of the investigation of other criminal/disciplinary matters.

8.1.3.11 If the Incident suggests the possibility of recurrence (eg careless behaviour which is not addressed) the Information Security Officer may recommend to ISPE that the relationship is revised to prevent recurrence.

8.1.3.12 Action will be documented in detail and records maintained by the Information Security Officer.

8.1.4 Segregation of Duties

8.1.4.1 It will be the responsibility of the system “owner” to ensure that the risk of accidental or deliberate loss will be reduced by the segregation of duties. Care will be taken to ensure that no one person is in a position to perpetrate frauds without being detected.

8.1.4.2 Users will not normally be permitted to administer data such as passwords or system codes (in Super User roles) – separate roles will exist for that purpose. And the super user type of role will be separate from the technical specialists.

8.1.4.3 Users may be permitted to carry out super user tasks, and occasionally technical tasks in an emergency (in which there is a threat to life or property or the investigation of a Crime). This may be agreed in the implementation/procurement planning for single-user systems. If it is initiated in an emergency then the fact will be recorded on the records relating to the problem, and the position will be discontinued as soon as practicable.

8.1.4.4 These issues will be reflected in working practices as defined by SyOPs.

8.1.5 Separation of Development and Operational Development

8.1.5.1 In order to remove the possibility of deliberate fraud or accidental damage to information and facilities, development, including testing will be strictly distinguished from operational work. Every precaution will be taken to ensure that live databases are uncontaminated by data used in development and testing. Different hardware will preferably be used for development, testing and operational use.

8.1.5.2 New systems will not be introduced into operational use without Acceptance Testing.

8.1.5.3 Changes to existing systems will not be introduced into live use without Acceptance Testing.

8.1.5.4 Live personal data will not be used for the purpose of testing unless there is no alternative. Where there is no alternative, the authority of the Data Protection and Information Security Manager or the ISO will first be obtained in writing.

8.1.5.5 Development tools (such as compilers and editors) will not be available from equipment when used for operational purposes.

8.1.5.6 The same log-on identities should not exist in both operational and development systems.

8.1.5.7 Development staff, users and super users should not have access to each other’s passwords.

8.1.5.8 In exceptional cases, passwords may be divulged at the responsibility of the individuals involved. Where this takes place, the passwords will be changed as soon as the need has passed.

8.1.6 External Facilities Management

8.1.6.1 A&S do not at present employ or intend to employ External Facilities Management providers.

8.2 System Planning and Acceptance

8.2.0 The Constabulary deploys the PRINCE (Projects IN Controlled Environments) family of methodologies for managing projects of significant scale (currently projects with an indicative cost in excess of £15000, or with some other special significance).

8.2.1 Capacity Planning

8.2.1 Technical assurance for the procurement of new systems and changes to existing systems will take account of existing and planned capacity. Note that a Capacity Planning document is a suggested product in the PRINCE methodologies.

8.2.1.2 Capacity planning will normally be on a “worst case basis”.

8.2.1.3 Appropriate arrangements will be made for monitoring capacity issues during the life of a system. These will be the responsibility of the Technical Services Manager unless other special arrangements are agreed.

8.2.2 System Acceptance

8.2.2.1 Contracts for the procurement of systems for handling information (including those for NSPIS, the Criminal Justice Network, or other “off-the-shelf products”) will specify the mechanism for their Contractual Acceptance. That mechanism will include rigorous Acceptance Testing.

8.2.2.2 An Acceptance Test process will test to ensure that:

a) The system meets its contractual specification and
b) That its introduction will not detrimentally affect the business of the Constabulary.

8.2.2.3 These tests will be carried out on new systems, upgrades, enhancements and new versions. The process will be carried out even where an appropriate section is omitted from the contracts (part b in the above paragraph remains even when part a is in a legally ambiguous position).

8.2.2.4 An Acceptance Test Plan will be produced in writing and will address the following topics by including appropriate test criteria:

a) Performance and capacity
b) Error recovery and contingency arrangements
c) Routine operations including related manual procedures (the ability to print must always be tested)
d) Security issues, including backup arrangements and power supplies (e.g. passwords and audit facilities)
e) Business continuity arrangements (see 11.1 below)
f) Evidence that introduction of a new system will not detrimentally affect existing system (eg by competition for server or network resources)
g) Documentation
h) Support arrangements

The Plan should specify standards (e.g. moves from screen to screen within 1 second, when loaded with 200000 records, surname 20 characters – does not permit numeric characters).

8.3 Protection against Malicious Software

8.3.1 Controls against Malicious Software

8.3.1.1 A proprietary solution will be deployed on all servers and terminals for the prevention, detection and rectification of malicious software.

8.3.1.2 The solution will be configured to run routinely and automatically, without intervention by users, checking activities in real time, by a variety of methods, including:

a) Saves
b) Copies and all forms of modification
c) Execution of a programme and opening of a file.

8.3.1.3 It will be regarded as a serious disciplinary matter to disable or attempt to disable this control. Any such action must be reported forthwith in accordance with 6.3.1 above.

8.3.1.4 It will be regarded as a serious disciplinary matter to load, unload or attempt to load/unload any unauthorised software. Software may be loaded and unloaded only by authorised staff.

8.3.1.5 Software, including all kinds of e-mail attachments, will be regarded with suspicion. It will not be loaded on police equipment without rigorous checking as to source and content by an appropriate specialist.

8.3.1.6 All difficulties, anomalies and concerns relating to viruses and virus checking will be reported as a system problem in the first instance (per 6.3.1 above). If necessary it will then be noted as a security incident.

8.3.1.7 The Information Security Officer is responsible for maintaining an up-to-date view of malicious software and taking appropriate steps to disseminate it to interested parties.

8.4 Housekeeping

8.4.1 Information Back-up

8.4.1.1 Information, including software and operating systems, held by electronic means will be “backed up” regularly.

8.4.1.2 Wherever practicable, this will be carried out automatically. In any special exceptional cases, the arrangements will be defined by the SSP.

8.4.1.3 The Backing Up/Restoring procedures and media will be tested before Live use of the system and then twice annually.

8.4.1.4 Security copies (backup copies) will normally be held in a heatproof safe. Where the information is classified at Restricted or above, it will be held in a separate building. In any exceptional cases, the arrangements will be defined by the SyOps.

8.4.1.5 Wherever practicable, the following versions will be retained:

a) Current live version
b) The version from the last working day
c) The version from the last but one working day
d) A version which is between one and two weeks old.

In any special exceptional cases, the arrangements will be defined by the SyOps.

8.4.1.6 Restoration procedures will be included in the SyOPs. A copy of the procedure will be stored with the back-up media.

8.4.1.7 Faults, errors and problems relating to back-ups will be regarded as particularly important and will be reported and progressed in the usual way (see 6.8.1 above), expeditiously.

8.4.2 Operator Logs

8.4.2.1 IS specialist operators will keep a log of their activities showing the:

a) System start/finish times
b) System errors and any corrective action
c) Confirmation of successful operation
e) The name of the operator.

8.4.2.2 These logs will be the subject to the Audit process as defined in 12.3.

8.4.3 Fault Logging

8.4.3. In the event that a fault is discovered by IS specialists, they will initiate appropriate corrective action and record the matter through the Service Desk system.

8.4.4 It will be the responsibility of the Information Security Officer to keep the system under review.

8.5 Network Management

8.5.0 Information assets will not be added to the force network, or changed, without a signed document of accreditation by the ISO.

8.5.1 Network Controls

8.5.1.1 The Constabulary's network of data, voice and radio is the responsibility of the TS Network Services Manager, Telephony Services Manager or Radio Services Manager. It will not be modified or tampered with by any unauthorised member of staff. Operational responsibility for the network is separate from that for computer operations.

8.5.1.2 This responsibility includes responsibility for remote sites and equipment.

8.5.1.3 Information which is personal or otherwise sensitive will not be passed across public networks (as distinct from the A & S WAN provided by MLL, BT, C&W and Virgin).

8.5.1.4 At present there are no special controls to protect data passing over public networks. Controls will be developed in harness with the implementation of the Protective Marking Scheme.

8.6 Media Handling and Security

8.6.0 This section is subject to the Government Protective Marking Scheme (GPMS).

8.6.1 Management of Removable Computer Media

8.6.1.1 Data on tapes, disks and other removable media will be treated as erased only when:

a) Erased by an approved proprietary solution
b) The medium is destroyed.

8.6.1.2 It will be permissible for media to be formatted permitting re-use provided that no personal data or classified information has been held on it.

8.6.1.3 Re-use of media which have held personal or classified information is discouraged. But it is permissible where the information is an extension (eg a new version or new generation) of that originally held. So it will be permissible to reuse media as part of back-up regimes, for example.

8.6.1.4 Media will not be removed from police premises except:

a) In accordance with the rules on working away from the office (see 7.2.5 above)
b) With the written authority of the District Commander/Departmental Head
c) With the written authority of the Information Security Officer or the Corporate Information Manager.

Written authorities will be retained for audit by the Information Security Officer.

8.6.2 Disposal of Media

8.6.2.1 Media will be disposed of safely and securely when no longer required.

8.6.2.2 The following table provides a set of general rules for disposal:

Medium	Disposal
Paper Documents	Shred, burn or confidential waste
Voice or other recordings	Physical destruction
Carbon paper	Shred, burn or confidential waste
Output reports	Shred, burn or confidential waste
Printer ribbons	Physical destruction
Magnetic tapes or cassettes	Physical destruction
Removable disks	Physical destruction or approved device
Optical storage media	Physical destruction
Program listings	Shred, burn or confidential waste
Test data	Shred, burn or confidential waste
System documentation	Shred, burn or confidential waste

8.6.2.3 SyOPs will provide detailed instructions for logging the destruction of media which contains sensitive information.

8.6.2.4 The system for handling confidential waste within the Constabulary is managed by the HQ Facilities Manager. It is designed to ensure that all confidential waste, at all police sites, is placed in distinctive blue bags in marked containers. This is collected by police staff at least weekly (or more frequently if required) and securely disposed of by a vetted service provider.

8.6.2.5 Waste paper baskets are not a secure form of disposal and will not be used for sensitive information including personal data. This waste is treated as ordinary commercial waste and disposed of under separate commercial arrangements.

8.6.3 Information Handling Procedures

8.6.3.0 Media containing police information will be kept and handled securely. The constabulary is committed to the standards of the Security Policy Framework. The following is intended to establish a baseline to be enhanced by the implementation of those standards.

8.6.3.1 Media will be labelled. The labels should indicate the following (in accordance with the relevant SyOP):

a) A name and/or description
b) Version and/or date
c) Owner
d) If it contains personal data, is otherwise sensitive or is classified.

8.6.3.2 Media will be handled in accordance with the SyOP of the system to which it relates. Distribution will generally be kept to a minimum.

8.6.3.3 Media, including paper, should be stored only within locked offices and/or locked furniture. It will not be acceptable to leave disks unattended in an unlocked office in a locked plastic case, for example.

8.6.3.4 Media will be stored in accordance with any manufacturer's instructions (e.g. as to temperature, humidity, magnetism, stacking). Storage will be defined by SyOPs.

8.6.3.5 Persons not authorised to have access to data will not be given access to the media containing it (even after formatting). SyOPs will clearly identify authorised persons. Persons will be taken as unauthorised unless the contrary is established.

8.6.3.6 Staff will note the "aggregation effect": that larger quantities of sensitive information become more sensitive, if only as a matter of the credibility of staff and the organisation.

8.6.3.7 SyOPs will establish rules to ensure that Input data is accurate and complete.

8.6.3.8 SyOPs will refer to distribution lists for paper and electronic data. These will be reviewed at intervals not exceeding 6 months.

8.6.4 Security of System Documentation

8.6.4.1 System documentation will be protected from unauthorised access. The level of protection will be commensurate with the sensitivity of the information contained, and the level of availability of the documentation (e.g. there is little point in protecting documentation on MS Word, however some tailored solutions will be sensitive and all but unique).

8.6.4.2 SyOPs will specify the arrangements for each system, including where the documentation will be retained, under what circumstances copies may be made, and who is authorised to have access.

8.6.4.3 Unless otherwise specified, each system will be procured with two sets of documentation. One will be held by the System Owner and one held by the relevant technical specialists in the TS.

8.6.4.4 Documentation held on computers will be appropriately protected.

8.6.4.5 At the end of the life of the system, the documentation will be destroyed or treated as confidential waste.

8.7 Exchanges of Information and Software

8.7.1 Information and Software Exchange Agreements

8.7.1.1 There will be no exchange of information and software with other organisations or individuals, without consultation with the Corporate Information Manager or the ISO.

8.7.1.2 Any exchange will be the subject of a formal written agreement. That agreement will define the following arrangements:

a) Management responsibilities and escalation procedures in the even of difficulty
b) Procedures for notifying despatch and receipt
c) Standards for packaging and transmission
d) Responsibilities and liabilities in the event of loss
e) Labelling
f) Ownership and legal responsibilities
g) Technical standards (e.g. details of media and file formats)
h) Any special measures required (e.g. encryption)
i) For onward transmission/sharing

8.7.2 Security of Media in Transit

8.7.2.1 Media will normally be passed by hand.

8.7.2.2 Media may be transmitted by post or approved courier.

8.7.2.3 Transmitted media will be contained in a sealed envelope.

8.7.2.3 If moving within the Constabulary, the envelope should show if the information is sensitive or classified. If moving outside the organisation, it should not indicate sensitivity.

8.7.3 Electronic Commerce Security

8.7.3.1 Electronic Commerce is not widespread. This issue will be dealt with in the security documentation for Finance Department and Purchasing and Supplies.

9 Access Control

9.1 Business Requirement for Access Control

9.1.1 Access Control Policy

9.1.1.1 Persons will not be allowed access to police information unless authorised by the owner.

9.1.1.2 Authorised persons and other details of Access Control Policy will be defined (not necessarily listed) by the SyOPs rules will generally be formulated in terms of what is forbidden unless an exception is identified. Rules will balance the business need against the need for security.

9.1.1.3 Authorised persons will normally receive training, including passwords before they use the system.

9.1.1.4 All members of staff may be granted access to police premises. But note that some areas are protected by enhanced security measures and only staff authorised by the owner will be allowed access to these.

9.2 User Access Management

9.2.1 User Registration

9.2.1.1 SyOPs will define formal procedures for the registration and de-registration of users of information handling procedures. These procedures will include rules as to temporary users. They will not assume that technical specialists (authorised by the Technical Services Manager TS) need access to operational information.

9.2.1.2 Access will normally be by reference to the collar number of the user (not function, initials, informal name, title, rank, location or unit). In the case of individuals who are not members of staff, it will be important to preserve the principle that each has a unique identifier and password (e.g. CPS1) and these will not be reissued when staff change.

9.2.1.3 Access to corporate systems, including the Personal Computer network, will be managed and operated by technical specialists in the TS.

9.2.1.4 Formal records of authorised users will be maintained.

9.2.1.5 Users will be given a written notice as to their access rights.

9.2.1.6 Service providers will be careful to avoid granting access in contravention of these procedures.

9.2.1.7 Technical specialists will routinely check for redundant IDs and remove them, from time to time.

9.2.1.8 It is the responsibility of District/Site Admin Officers to identify staff leaving the organisation and notify affected departments. All assets (such as ID cards, keys, “Prox cards”, laptop computers, PDAs, mobile ‘phones and car park passes) will be recovered, as well as uniform and equipment. When members of staff leave, Collar numbers will not be re-issued until at least six months later.

9.2.1.9 Discipline codes (see 6.3.5 above) and contracts will specify the sanctions for unauthorised access. Every effort will be made at publicity.

9.2.1.10 Other locking mechanisms (eg keys, and smart cards) may be deployed in addition or as an alternative to passwords.

9.2.2 Privilege Management

9.2.2.1 Privilege Management will be defined in SyOPs. Privileges will be granted only if they are needed and for the period of time for which they are needed. The notion of special privileges generally available is to be questioned.

9.2.2.2 Operating systems and database management systems will be selected / specified with this in mind.

9.2.3 User Password Management

9.2.3.1 SyOP documents will specify arrangements for password management for specific systems.

9.2.3.2 Users will normally be able to maintain their own passwords, once granted.

9.2.3.3 Passwords will normally be managed for all systems capable of supporting more than a single user at any time, by a nominated Super User who is not normally a user of the system. For corporate systems, passwords will be managed through the TS Service Desk (with some exceptions including NCALT).

9.2.3.4 Users will be allocated individual passwords.

9.2.3.5 Passwords will be confidential. Every effort will be made to protect that confidentiality.

9.2.3.6 Passwords will be passed to users by methods ensuring maximum security. Receipt of passwords should be acknowledged unless it is given in person.

9.2.3.7 Initial passwords will be changed by users promptly. Administrators will remind users of this requirement.

9.2.3.8 Wherever possible, passwords will be encrypted. Encryption will preferably be one-way encryption.

9.2.3.9 Best Practice will include a mechanism to detect passwords used under duress.

9.2.3.10 Passwords will not be held as part of audit trails.

9.2.3.11 Passwords, including temporary passwords, will be supplied only following positive identification of the user.

9.2.3.12 Passwords will be communicated securely, taking care to ensure that the process is not overlooked or overheard.

9.2.3.13 Passwords will not be automated.

9.2.3.14 All procurements of systems will specify:

a) A minimum password length of nine characters
b) At least one capital letter, one lower case letter, one number and one symbol)
c) Password validation
d) Enforced monthly changes.

9.3 User Responsibilities

9.3.1 Password Use

9.3.1.1 Users will be responsible for keeping passwords secret. Passwords will not be shared.

9.3.1.2 SyOP documents will specify arrangements for password management for specific systems.

9.3.1.3 Passwords should normally be of at least nine characters in length (this may be varied by SyOPs. Where systems allow the selection of shorter passwords, users will select passwords of six characters or as long as possible.

9.3.1.4 Users will avoid keeping a paper record of passwords.

9.3.1.5 Passwords should be changed at least monthly.

9.3.1.6 Passwords should be changed immediately there is any suggestion of compromise.

9.3.1.7 The following kinds of password should be avoided:

a) Names
b) Registration numbers
c) Months
d) Telephone numbers
e) User Ids
f) Those having more than 2 consecutive characters the same
g) All numerics
h) All alphabetical characters
i) Previously used passwords.

9.3.1.8 Passwords should be easy to remember

9.3.1.9 Default passwords will be changed before any system is taken into live use. This is of enormous importance. Temporary passwords will be changed at the first opportunity.

9.3.2 Unattended User Equipment

9.3.2.1 Equipment will not be left logged on and unattended. Users should lock their machines when they leave them unattended (usually via Ctrl Alt + Del).

9.3.2.2 Systems will be configured to “time out” (see 9.5.7.1 below).

9.3.2.3 It is not generally considered necessary to limit connection time to systems.

9.4 Network Access Control

9.4.1 Policy on Network Access Control

9.4.1.1 Most of A&S Technical Services depend upon access to the Force network. That network is structured as a single network rather than as a series of domains. Most users therefore also depend upon the network. Which emphasises the importance of the network and its security.

9.4.1.2 Reliance on the network will be defined in SyOPs.

9.4.1.3 The following primary controls will be deployed to protect the network:

a) Passwords
b) Firewalls
c) Endpoint security controls on removable media
d) Intrusion detection/prevention systems
e) Physical measures
f) Controlling external links
g) Authentication
h) User profiles.

9.4.1.4 Users will not be permitted or able to choose their route through the network. Systems will be configured to predefine the routes, and any network services which may be provided, without reference to users.

9.4.1.5 SyOPs will define the procedures for authorising the users of systems. Authority to use a system will imply authority to use networks/services. Authority to use networks/services will not normally be granted separately, except among technical specialists – who will be granted those facilities necessary for their work.

9.4.1.6 The use of the network for new purposes will be subject to accreditation, via the Information Security Officer.

9.4.1.7 Under no circumstances will the force network be compromised by an external connection. External connections will be protected by firewall technology configured generally to prevent access to the network.

9.4.1.7 Users will not be able / required to choose or configure external connections.

9.4.1.9 Any systems requiring external connections which are unable to be protected by firewalls will be provided on a stand alone basis; disconnected from the network.

9.4.1.10 In order to protect the network while allowing users some flexibility, laptops may be configured in such a way as to allow the user to choose a network connection or to choose a modem link (usually to the internet) – but the configuration will prevent the possibility that both kinds of connection are made simultaneously.

9.4.1.11 Isolated equipment may access assets within the network by reference to an approved facility for Remote Access. The facility is described and defined in a SyOps.

9.4.1.12 Where it is necessary for suppliers of software to have direct access to systems in order to diagnose problems, any connection will be made by reference to the dial back facility after identification by voice (see 9.4.5).

9.4.2 Enforced Path

9.4.2.1 Router technology will be deployed on each Local Area Network (LAN) and at network exit points (ie points at which the network links to an external connection) to automatically enforce routes through the network.

9.4.2.2 Firewall technology will be deployed at each point at which traffic may cross the boundary of the police network inwards or outwards. The firewall will be configured on the basis that in general, traffic will be rejected, except for traffic which is expressly authorised. (Details of the configuration will be maintained in a separate document entitled “Enterprise Firewall Facility”, which is maintained by the TS Security Administrator).

9.4.2.3 User profiles will enforce paths through the network.

9.4.2.4 Paths will be defined consistent with SyOPs. Unlimited network roaming will be prevented.

9.4.2.5 All links with the force network will be by dedicated lines.

9.4.3 User Authentication for External Connections

9.4.3.1 The rules in sections 9.4.1 and 2 are designed to ensure that external connections are either:

a) Protected by firewalls

Or

b) Connected for the occasion and connection established by a dial back facility.

9.4.3.2 The connection of remote users is under review: the review will have regard to security issues. This section will be revised if/when access by remote users is planned.

9.4.3.3 Call Line Identification will be disabled for police telephone lines (including mobile telephones).

9.4.4 Node Authentication

9.4.4.1 With the exception of dial back connections for diagnostic purposes (see 9.4.1.12 and 9.4.3.1) there will be no dialled connections to the force network (connections are fixed).

9.4.5 Remote Diagnostic Port Protection

9.4.5.1 Remote diagnostic links will be securely controlled. They will be protected by the following methods.

9.4.5.2 A procedure by which service providers call the technical specialist and identify themselves. The specialist then establishes the physical connection and causes the system to call the service provider on a previously known number. At the end of the process, the link is logically and physically disconnected. The service provider should be supervised whilst the link is in operation wherever possible.

9.4.5.3 Facilities to which such connections can be made will normally be in secure areas (e.g. computer rooms).

9.4.6 Segregation in Networks

9.4.6.1 The A&S police network runs within and between police stations. It includes police facilities in buildings belonging to the Crown Prosecution Service and Wiltshire Police (3 locations). It excludes a facility in premises belonging to the Avon and Somerset Magistrates Courts at Taunton (they share the use of a computer system, but do so by reference to a firewall from outside the network, and they are considered to be an external connection).

9.4.7 Network Connection Control

9.4.7.1 In circumstances where external users connect to police networks, or police systems accept incoming data (e.g. the Police National Networks and VP / FPO users from Magistrates Courts), the relevant SyOP will rigorously define the rules in terms consistent with 9.4.2.2 above, including defining in advance file and data standards, and firewall implementation.

9.4.7.2 A separate SyOPs will address the special issues relating to internet connection. That connection will also be via a firewall gateway if it is to a machine which is part of the force network. The policy will address e-mail standards and monitoring, the use of the facilities, and will address the risks relating to virus infection especially from e-mail attachments.

9.4.8 Network Routing Control

9.4.8.1 9.4.2.1 above prescribes the deployment of routing equipment. This equipment will be configured to manage traffic within the network and across its boundaries by reference to its source and destination, among other criteria.

9.4.8.2 A scheme will be operated for the translation of network address information for the purpose of preventing the identification of IP addresses from inside the Constabulary. IP address information will be confidential.

9.4.9 Security of Network Services

9.4.9.1 Network services are provided by external service providers. The procurement of value added features is not envisaged. If the procurement of such services is planned, this document will be revised.

9.5 Operating System Access Control

9.5.1 Automatic Terminal Identification

9.5.1.1 Automatic Terminal Identification will not normally meet police requirements of a computer system. SyOPs will deal with any exceptions.

9.5.2 Terminal Log-on Procedures

9.5.2.1 Access to information services will be available only through a secure log-on process. SyOPs will provide a detailed rules for each system. The following rules are to be taken as a baseline.

9.5.2.2 Users will preferably access information services through a proprietary Operating System log-on. This log-on will be linked to the user profile which defines facilities, routes and constraints for the user. Note that some legacy systems have tailored log-on facilities.

9.5.2.3 Log-on facilities should not disclose information about systems within until the password has been checked.

9.5.2.4 Log-on facilities will include a password check (see 9.2.3 and 9.3.1 above).

9.5.2.5 Wherever possible, Log-on facilities will include a notice warning off unauthorised users.

9.5.2.6 Where an error arises during the process the system should not disclose where/how the error arose to the user.

9.5.2.7 Wherever possible, log-on facilities will prevent a user from making more than three attempts to log on. Unsuccessful attempts should be logged.

9.5.2.8 Successful log-on should provide the user with information as to the last time he/she logged on, and details of any unsuccessful attempts to log-on since the last successful log-in. Users should compare this information with personal recollection in an effort to spot any bogus attempts to log-on.

9.5.3 User Identification/Authentication

9.5.3.1 Each member of the constabulary is issued with a unique Staff ID number. That number will normally be used to identify the individual as a user of information facilities in order to trace activities.

9.5.3.2 “Collar numbers” are normally issued for the life of the employment. It is occasionally necessary to re-number some individuals.

9.5.3.4 Numbers are never in concurrent use by more than one individual – never shared.

9.5.3.5 Other access controls may be permitted as an alternative with the authority of ISPE. In the first instance, proposals should be made to the Information Security, who will make recommendations. Combination of mechanisms/technologies will be favoured.

9.5.4 Password Management System

9.5.4.1 Passwords will be managed in accordance with 9.2.3 and 9.3.1 above.

9.5.5 Use of System Utilities

9.5.5.1 9.5.2 above refers to the implementation of user profiles. These will be deployed to prevent users from access to programs capable of overriding security controls unless the programs are removed.

9.5.6 Duress Alarm

9.5.6 There is no general requirement for duress alarms on police computer systems, although they may be implemented in areas of particular risk (see SyOP of the system concerned).

9.5.7 Terminal Time-out

9.5.7.1 Terminals will be configured, using standard operating system facilities, to “time out” after 10 minutes.

9.5.7.2 Exceptions may be authorised by Information Security Team.

9.5.8 Limitation of Connection Time

9.5.8.1 Limitation of connection time will normally be consistent with the business requirement.

9.6 Application Access Control

9.6.1 Information Access Restriction

9.6.1.1 Access restrictions will be specified within System Operating Procedure. It is not possible to provide a general rule.

9.7 Monitoring System Access and Use

9.7.1 Event Logging

9.7.1.1 Information processing facilities will include audit facilities to record events which are relevant to security.

9.7.1.2 The main purpose of an Audit Log is to detect unauthorised activities.

9.7.1.3 The following information should be recorded for all monitorable events:

a) User ID/s

b) Date/time
c) Terminal identity
d) Description of event
e) If done On Behalf Of, then whom.

9.7.1.4 Monitorable events are:

a) Log on
b) Log off
c) Attempt to log on
d) Rejected attempts to access data
e) Create User record
f) Delete User record
g) Amend User record (including password)
h) Creating a record
i) Amending a record
j) Deleting a record
k) Search
l) Access to a record
m) Use of a function (eg printing or transmitting)
n) System halt
o) System restart

9.7.1.5 In relation to items v to xiii above, the Log must identify records which are affected. A copy of the relevant record would preferably be available through a computer system. Changes to system data, such as time/date, or codes on which the system depends (e.g. offence codes, section codes, or staff IDs) are especially to be protected.

9.7.1.6 The Logged information should be retained online for two months (viz 60 days). It should then be archived (preferably via electronic media) for a further 18 months, stored securely in a fireproof safe.

9.7.1.7 The Audit Log facility must not be accessible to system operators or supervisors.

9.7.1.8 It should be presented, on demand, as part of the application through the user interface. The facility should be presented on machines available in the Corporate Information Management Department.

9.7.1.9 It must be capable of printing.

9.7.1.10 It must be capable of searching according to event type, user, terminal and date.

9.7.1.11 It must be protected to ensure that Log records are not amended or accessed without authority. It should be incapable of running the system in the absence of the Audit Log.

9.7.1.12 Any test/training databases would be protected as the main database.

9.7.1.13 Where it proves to be impossible/impractical to meet this requirement, the assistance of the Information Security Officer or the Corporate Information Manager must be obtained in writing before a contract is let.

9.7.2 Monitoring System Use

9.7.2.1 Audit facilities will be used by authorised audit staff from the Corporate Information Management Department only.

9.7.3 Clock Synchronisation

9.7.3.1 Clock synchronisation is the responsibility of the IS Technical Services Manager.

9.8 Working Away From the Office

9.8.0 See 7.2.5 Security of Equipment Off Premises above.

9.9 Identity Cards

9.9.1 All members of police staff will be issued with an identity card which certifies their name and ID number and displays a photograph.

9.9.2 Cards are issued by video technicians in Human Resources Department.

9.9.3 For police officers and Special Constables this card serves as a legal document to establish legal powers.

9.9.4 Production of the document may be required to gain access to police premises or to identify the holder for operational purposes or for security purposes within premises. Production may be required by any member of staff irrespective of rank or role. Only officers engaged in covert work are exempt from the need to produce, although they must expect to be asked to identify themselves and should make appropriate arrangements.

9.9.5 Staff having any difficulty with obtaining production or producing the document will report to ISO.

9.9.6 The loss of ID cards will be reported immediately. In the first instance the report will be to appropriate Site Admin and Finance Manager or District Admin Officer, who will report (by e-mail) to video technicians, so as to arrange replacement, and ISO, who will treat this as a security incident.

9.9.7 Where one individual loses the card more than once in a calendar year, costs of replacing the card may be recovered.

9.9.8 Staff at Police Headquarters are required to display their identity card unless in full uniform which bears identification numbers.

10 Systems Development and Maintenance

10.1 Security Requirements of Systems

10.1.1 Security Requirements Analysis and Specification

10.1.1.1 Any statement of requirements formulated for the purpose of procuring of information handling facilities will include a statement of the security requirements. It is emphasised that it cannot be assumed that suppliers will comply with the law, or with the other standards to the satisfaction of A&S. It is also emphasised that security introduced early is much cheaper than security introduced late.

10.1.1.2 The statement of requirements should normally be based on this policy. Where there are special circumstances suggesting any departure from this policy, the Information Security Officer must be consulted.

10.1.1.3 New systems and changes to existing systems will normally require a Risk Analysis. This will be carried out by, or with the assistance of, the Information Security Officer.

10.1.1.4 Where possible, IT security products (including operating systems and database management systems) will be selected from those accredited in ITSEC Certified Product List.

10.2 Security in Application Systems

10.2.1 Input Data Validation

10.2.1.1 Data may be entered incorrectly deliberately or by accident. Errors in police data can have serious legal consequences for members of staff and for data subjects. Staff will take care to enter data accurately.

10.2.1.2 Wherever possible input data will be validated. Staff and user identities, offence codes and dates are leading examples of data to be validated. This demands careful analysis/specification in relation to new systems. It is unlikely to be feasible to improve the position in relation to legacy systems, but any opportunities to do so will be taken.

10.2.2 Control of Internal Processing

10.2.2.1 Every effort will be made to include controls to detect the corruption of saved data during the design, development, implementation and operational life of information handling facilities.

10.2.2.2 Data corruption will be a criteria included in all acceptance test schemes.

10.2.2.3 The discovery of corrupt data demands an immediate review of the continued use of the system. The review will be carried out by the system owner in liaison with the Information Security Officer and stakeholders such as consumers of information from the system.

10.2.2.4 Operators will ensure that data is not corrupted by the running of programs in the wrong order, or of the wrong programs.

10.2.2.5 Procedures will be included in SyOPs and Business Continuity Plans to recover from significant corruption of data.

10.2.3 Message Authentication

10.2.3.1 Message authentication (e.g. electronic signature) is not currently widely used within A&S at present.

10.3 Cryptographic Controls

10.3.1 Policy in the Use of Cryptographic Controls

10.3.1.1 The Constabulary will adopt the rules contained in Her Majesty's Government Infosec Standard 4 on Communications Security and Cryptography.

10.3.1.2 The Constabulary aspires to the standards of the document "Cross Government Actions: Minimum Mandatory Measures" and "Data Handling Procedures in Government: Final Report" (also known as "The Hannigan Report"). However it is a new standard.

10.3.1.3 Approved (ITSEC Certified Product List) cryptographic controls will be deployed where police information containing personal data, data which is otherwise sensitive, or data which has been classified as RESTRICTED (or above) is to be transmitted or received to/from outside the A&S network.

10.3.1.4 Information which is classified CONFIDENTIAL or above will not be held within the force network unless encrypted to an approved standard.

10.3.1.5 Encryption will be managed by reference to a single central Crypto Custodian.

10.3.2 Encryption

10.3.2.1 Subject to the principles in 10.3.1, encryption arrangements will be documented in SyOPs.

10.3.3 Digital Signatures

10.3.3.1 There is considered to be no requirement for a baseline rule on Digital Signatures. Where such controls are necessary, they will be defined by SyOPs.

10.3.4 Non-Repudiation

10.3.4.1 It may be necessary to deal with the possibility that recipients of messages deny receipt or authors deny authorship, or dates of despatch. No baseline measure is considered to be necessary at present. Where such controls are necessary, they will be defined by SyOPs.

10.3.5 Key Management

10.3.5.1 Primary responsibility for Key Management will lie with the Crypto Custodian nominated by the DPE. A Deputy is also appointed.

10.3.5.2 This responsibility includes:

a) The ordering, accepting delivery, checking and storing of key material and administering accounts
b) Certification of crypto equipment
c) Distribution and accounting for crypto material
d) Destruction of crypto material
e) Dealing appropriately with violation in accordance with SPF.

10.3.5.3 Where it is necessary to involve a super user in this process as a Holder, that individual will already possess the appropriate security clearance and will first receive appropriate training as a crypto-custodian.

10.3.5.4 All keys will be protected by the measures prescribed in Infosec Standard 4.

10.3.5.5 Grades of encryption will be in accordance with SPF.

10.3.5.6 Note that for historical reasons Crypto Custodianship in relation to the Cougar radio system will remain within the Targeting Team.

10.4 Security of System Files

10.4.1 Control of Operational Software

10.4.1.1 The updating of operational software will be carried out only by authorised specialist staff (of IS) or authorised external providers.

10.4.1.2 Wherever possible, operational systems will hold only executable code.

10.4.1.3 Careful version control is essential – to ensure that the version accepted is the version tested, and the version taken into use is the same as the version accepted. A log will be maintained of versions for every information handling facility, to establish control of versions tested, in training, loaded and in use.

10.4.1.4 It will be the responsibility of the TS Technical Services Manager to ensure that earlier versions of software will be retained and securely held.

10.4.1.5 Technical specialists responsible for change to operational software will ensure that a contingency plan exists before change is effected.

10.4.2 Protection of System Test Data

10.4.2.1 Use of operational data for test purposes will be avoided.

10.4.2.2 When, in exceptional cases, it is necessary, authority will first be obtained from Data Protection Officer or the Information Security Manager or ISO. If operational data is used, it will be subject to the same handling rules as live data.

10.4.2.3 As soon as the test is completed, the data will be erased from the testing facility.

10.4.2.4 A log will be maintained by the system owner of live data used for testing, in order that an audit trail exists.

10.4.3 Access to Program Source Library

10.4.3.1 Program source libraries will not be held in operational systems.

10.4.3.2 Libraries will be available only to technical specialists and service providers. Specialists and service providers will not have unrestricted access to libraries. Access will be logged.

10.4.3.4 Libraries will be maintained in a secure environment.

10.4.3.5 Old versions will be archived, labelled as to dates when they were in use, together with any supporting material necessary to restore them to use.

10.5 Security in Development and Support Processes

10.5.1 Change Control Procedures

10.5.1.1 Formal Change Control Procedures will be enforced on all multi-user and any business critical systems.

10.5.1.2 Requests for Change should be submitted in writing to the system owner with an indication of cost, resource implications and impact on other users or consumers of the data. If approved by the system owner, technical assurance will be obtained from an appropriate technical specialist from the TS. If a system owner wishes to proceed in the absence of technical assurance, the matter will be resolved by ISPE. The scale of changes may in any case demand review at ISPE.

10.5.1.3 Documents relating to change control will be retained by system owners.

10.5.1.4 It will be important to address the implementation of changes. It may be necessary to arrange for technical work and/or testing to be carried out outside office hours. Otherwise consultation with the system owner will be necessary.

10.5.1.5 Operating Documents will be kept up to date in relation to changes.

10.5.1.6 Changes will not be implemented on operational systems unless the acceptance procedures in 8.2.2 have been followed.

10.5.2 Technical Review of Operating System Changes

10.5.2.1 Changes in operating system or database management system will not be implemented unless the acceptance procedures in 8.2.2 have been carried out.

10.5.2.2 The Head of Technical Services will be responsible for initiating and planning operating system changes, including budgetary provision and availability of human resources.

10.5.2.3 Wherever possible, operating systems and database management system software will be selected from the current ITSEC Certified Product List. Failing that preference will be given to software which is proven in a relevant environment.

10.5.2.4 Proposed changes will be subject to the agreement of the system owner including the implementation and testing arrangements, and contingency plans.

10.5.2.5 It is important to note that even these software changes can bring significant changes for users and business processes.

10.5.3 Changes to Software Packages

10.5.3.1 Modifications to “off-the-shelf” software, or software supplied by external service providers, are discouraged. The following considerations must be taken into account:

a) The effect on support contracts and software licences, and the need for consent from the vendor
b) Change control and acceptance procedures
C) The effect on security controls

10.5.3.2 The rules in 10.5 become even more important and applicable when such changes are contemplated.

10.5.4 Covert Channels and Trojan Code

10.5.4.0 This section introduces some special controls designed to avoid Trojan code and covert channels.

10.5.4.1 Software will not be acquired except from reputable sources.

10.5.4.2 Where commercially feasible, especially in systems developed specifically for A&S, programs should be acquired in source code form. Wherever possible, this source code should be examined before implementation.

10.5.4.3 Products should be evaluated and tested (see 8.2.2) before being taken into live use.

10.5.4.4 Access or modification to the products will be by or under the supervision of TS technical specialists once in A&S possession.

10.5.4.5 The following process for dealing with virus infections is designed to protect the operation of the business, to learn from the incident, and to identify any criminal/disciplinary issues:

a) Report to TS Service Desk
b) Deployment of appropriate technical specialist
c) Identify the virus
d) Establish the circumstances of infection
e) Identify and quarantine other possible infections
f) Identify and quarantine any infected media
g) Technical steps to resolve/clean up (rebuild if necessary)

10.5.4.6 It is not considered necessary to disable facilities for handling removable media (e.g. USB ports).

10.5.5 Outsourced Software Development

10.5.5.1 Where software is procured which is developed particularly for A&S, or for a small number of organisations, the following points will be resolved in writing in the relevant contract/s and documented in SyOPs:

a) Licensing arrangements, code ownership and intellectual property rights
b) Quality/accuracy issues, including checking procedures and rights
c) Escrow arrangements (in case of failure of the supplier's business)
d) Acceptance criteria and arrangements
e) Documentation
f) Training arrangements
g) Delivery and implementation arrangements
h) Timescales

11 Business Continuity Management

11.0 The Constabulary will maintain Business Continuity Plans (related to SyOPs) to protect and mitigate the effects of worst case developments for its information handling.

11.0.1 These plans are currently under review.

11.1 Aspects of Business Continuity Management

11.1.1 Business Continuity Management Process

11.1.1.1 Each system owner will be responsible for ensuring that plans exist for Business Continuity in the event of a major security incident (eg loss of the system, widespread corruption of data, or widespread disruption).

12 Compliance

12.1.1 The constabulary, all its staff and all those treated as if they are members will comply with the law.

12.1.1.1 The following legislation is applicable and gives rise to criminal and civil liabilities:

Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988

Data Protection Act 1998
Electronic Communications Act 2000
Freedom of Information Act 2000
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000.

12.1.1.2 Relevant contracts will be detailed in SyOPs.

12.1.1.3 Admissibility of evidence which depends on computers may also depend upon conformance with the law and this policy.

12.1.2 Intellectual Property Rights

12.1.2.1 Where a member of the constabulary develops software for use by the constabulary, intellectual property in that software normally lies with the constabulary unless it is developed outside working hours.

12.1.2.2 Any member of staff claiming intellectual rights in software will notify the Head of Technical Services before it is taken into use. It is important to establish ownership before the system is taken into use.

12.1.2.3 Software will not be taken into police use in contravention of the Copyright Designs and Patents Act 1988 (or if there is any doubt about contravention).

12.1.2.4 Designs and trademarks will not be taken into police use in contravention of the Copyright Designs and Patents Act 1988 (or if there is any doubt about contravention).

12.1.2.5 Where a software licence exists, software will be used and copied only in accordance with that licence. Note that software usually permits copying only for back-up purposes. It will be necessary to refer to the licence to discover the details of what is permitted, including rules about copying and how the software may be used.

12.1.2.6 It will be the responsibility of the TIS Technical Services Manager to hold software licences. It will be good practice for system owners to ensure that a local copy is also held.

12.1.2.7 This policy is supported by the maintenance of asset registers (see 5.1 above) and an audit process (see 12.3).

12.1.2.8 Procurement projects are permitted to select the appropriate kind of software licence according to the planned use and the commercial issues at hand.

12.1.2.9 The copying of police software for private use is strictly forbidden.

12.1.2.10 The introduction of privately owned software to police equipment is strictly forbidden.

12.1.2.11 The constabulary will not normally transfer software to others. Where this is contemplated, it will be the responsibility of the system owner to resolve any licensing implications.

12.1.3 Safeguarding Organisational Records

12.1.3.1 Organisational records are not distinguished from other kinds of police information such as evidence, intelligence and mail. All information may be treated as sensitive and all information will be subjected to the Protective Marking Scheme.

12.1.3.2 SyOPs will specify rules for retention and handling of information including organisational records, addressing the possibility of degradation of media and having regard to any manufacturer's recommendations, data formats and any encryption arrangements.

12.1.4 Data Protection and Privacy of Personal Information

12.1.4.1 A Corporate Information Management Department exists with the objective of ensuring that the constabulary conforms with all aspects of information legislation. The unit head (Data Protection and Information Security Manager) will take a lead in the Data Protection matters, supported by a team of auditors and staff assigned to provide a Subject Access service to staff and members of the public.

12.1.4.2 SyOPs will contain detailed rules in support of this objective for each system, including addressing the collection, processing and transmission of data, and having special regard to the issues of disclosure.

12.1.4.3 It is the responsibility of all managers to consult with the appropriate member of the unit in respect of changes in processing information.

12.1.4.4 It is the responsibility of all staff to comply with all legislative requirements.

12.1.5 Prevention of Misuse

12.1.5.1 Any use of police information processing facilities for non business or unauthorised purposes will be regarded as improper use.

12.1.5.2 All staff are responsible for reporting any such misuse.

12.1.5.3 Misuse will be reported and investigated as a Security Incident (see 6.3.1 above), with a view to disciplinary action and/or criminal prosecution (e.g. under Sections 1, 2 or 3 of Computer Misuse Act 1990).

12.1.5.4 Appropriate warning messages will normally be displayed during log-on processing.

12.1.6 Cryptographic Controls

12.1.6.1 Members of staff will neither import nor export any form of cryptographic control (including cryptographic functions and hardware) in the course of their work.

12.1.6.2 Staff considering importing or exporting data which is encrypted will obtain and follow advice from the Information Security Officer before acting. 12.1.6.3 This is not to be taken to imply that any other organisation will have rights or opportunity to view police information except as laid down in this policy and the subordinate SyOPs.

12.1.7 Collection of Evidence

12.1.7.1 Police Technical Services handle evidence in relation to a vast range and number of criminal prosecutions. Admissibility of evidence may depend (will be assumed to depend) upon the security of the systems handling that evidence.

12.1.7.2 Where disciplinary or criminal action is contemplated in relation to the misuse of information or information handling facilities, it will be vitally important to gather evidence of the misconduct. When an incident is discovered which may lead to prosecution and/or disciplinary action, it will be Best Practice to cease use of the system until evidence is collected by the appropriate specialist/s.

12.1.7.3 It is recognised that this need will be balanced against the operational importance / urgency of the work. The senior officer available at the time may authorise in writing the continued use of the system, providing that he takes every practicable step to collect evidence.

12.1.7.4 Evidence gathered will be treated in accordance with the Disciplinary Procedures.

12.1.8 Quality of Evidence

12.1.8.1 Evidence is relevant both to the investigation of security issues and to the conduct of the core business of prosecuting offenders.

12.1.8.2 Most members of staff will be familiar with the rules of evidence. Those who are not, and who become involved through Information Security issues should obtain advice/training.

12.1.8.3 A&S Fraud Squad has a facility for obtaining computer based evidence. All cases where it is necessary to gather evidence (in respect of A&S Information Security) will be referred forthwith to Fraud Squad Detective Inspector.

12.1.8.4 The following is provided as minimal advice for emergencies:

a) Keep originals of paper records
b) Take one copy of any computer data and retain it untouched, logging in detail the action taken during the process, and preferably having the process witnessed.
c) Log conversations verbatim
d) Do not attempt to interview offenders – there are detailed and complex legal rules for this and it must be done by those with appropriate training if the evidence is to be useful.

12.1.8.5 Note that failing to conform with law, including the Data Protection Act and its codes of practice may render evidence inadmissible. It is important to ensure that police systems conform with the law for this reason. It is also important to ensure that any systems upon which evidence depends are compliant (especially CCTV systems, in the light of the recent Code of Practice).

12.2 Compliance with Security Policy

12.2.1 Managers at every level will be responsible for ensuring that their subordinates comply with this policy.

12.2.2 Minor breaches may be dealt with locally. Breaches of the policy will be regarded as major if there is loss, injury or adverse publicity arising, and will be reported to the Information Security Officer in writing (e.g. e-mail) as soon as practicable.

12.2.3 Minor breaches discovered by the Information Security Officer, including those disclosed by the Incident Handling procedure (see 6.3 above), may be dealt with informally. Repetition is likely to result in reference to the District Commander or the Professional Standards Unit, as appropriate.

12.2.4 Major breaches will be treated as discipline matters. Including those disclosed by the Audit process (see 12.3. below).

12.2.5 Breaches may indicate the need for further Risk Analysis.

12.2.6 It will be Best Practice to review information handling facilities annually.

12.2.7 Staff and management in the IS will monitor the technical compliance of systems for which they have a responsibility.

12.2.8 An authoritative external organisation will be procured by the ISO during the year following adoption of this policy to test Information Security ("Penetration Test"). Criteria and results of these tests will be developed by the ISWG, to be approved by the DPE.

12.3 System Audit Considerations

12.3.1 System Audit Controls

12.3.1.1 The Corporate Information Management Department will be responsible for system auditing in accordance with the ACPO Data Protection Audit Manual.

12.3.1.2 The unit will formulate a plan annually, taking into account prevailing risks and priorities, resource availability and consultations with users designed to minimise disruptions to the business process.

12.3.1.3 Audit Plans will be agreed with the managers of units affected and the scope of the checks will be defined in advance.

12.3.1.4 The checks will be limited to read-only access to software and data. If additional access is required, special arrangements will be made to ensure that this does not endanger or detract from the business process in any way.

12.3.1.5 If necessary, technical specialist resources will be identified and agreed in advance with relevant TS management.

12.3.1.6 A reference trail, including an access log will be produced as part of each audit activity.

12.3.1.7 Audit procedures, requirements and responsibilities will be documented.

12.3.2 Protection of System Audit Tools

12.3.2.1 Any tools used, or data generated in the course of system audits will be protected.

12.3.2.2 They will be confidential within the audit team.

12.3.2.3 They will be kept separate in all respects from operational and development material.

12.3.2.4 They will be retained as required by the Manual, within the Corporate Information Management Department.

12.4 Migration/Conformity

12.4.1 This policy is generally applicable. However it is acknowledged that not all systems are conformant at the date of publication. An Exception List, indicating decisions/actions for each will be developed and maintained by the ISO.

12.4.2 Where significant difficulties are encountered with conforming with these rules, the ISO will undertake a Risk Analysis, weighing the risks and the benefits of any proposed action. This document will be presented to CME for decision.

BIBLIOGRAPHY

ACPO Community Security Policy

ACPO National Vetting Policy for Police

BS 7799 Information Security Management7799

Catalogue of Security Products

CESG Memos

Computer Misuse Act 1990

Copyright Designs and Patents Act 1988

Data Protection Act 1998

Freedom of Information Act 2000

Her Majesty's Government Infosec Standards:
- 1 Risk Management
- 2 Accreditation Documents
- 3 Connecting Business Domains
- 4 Communications Security and Cryptography
- 5 Secure Erasure of Protectively Marked Information

HO Working Away From the Office

Human Rights 1998

ITSEC Certified Product List

"The Code Book" by Simon Singh

"The Cuckoo's Egg" by Clifford Stoll

"The Art of Deception" by Kevin Mitnick

Security Policy Framework.

"Secrets and Lies" by Bruce Schneier

"The Next World War" by James Adams

GLOSSARY	
Abbreviation	**Description**
A & S	The Avon and Somerset Constabulary
Access Control	The prevention of access to data by those without appropriate access rights.
Accountability	Tracing actions to the individual who took them
Accreditation	A formal statement by a relevant Information Security authority that a system meets security requirements
ACPO	Association of Chief Police Officers
Assurance	Level of confidence
Attack	Deliberate attempt to interfere with police information or information facilities. May be to breach confidentiality, to amend or delete, to flood a system so as to deny service, a virus.
Audit	Monitoring to detect and warn of events which might threaten security.
Authentication	Verifying the identity of an individual or system.
Availability	Provision of timely access to assets (by authorised users).
Biometrics	The use of physical features (eg fingerprints) to identify individuals
Breach	Any loss of confidentiality, integrity or availability of information.
BS 7799	Information Security Management – the British Standard, also adopted by the International Standards Organisation.
CESG	Communications-Electronic Security Group – the technical authority for information security.
CIMD	Corporate Information Management Department
Classified	Not Protectively Marked, Restricted, Confidential, Secret or Top Secret.
CLEF	Commercial Licensed Evaluation Facility – in which security solutions can be authoritatively tested
CME	Change Management Executive
CNI	Critical National Infrastructure. Includes PNC.
COMPUSEC	Computer security – another specialist area of Information Security
COMSEC	Communications Security – a specialist area of Information Security
CONFIDENTIAL	Compromise would be likely to prejudice individual security or liberty, cause damage to the effectiveness of valuable intelligence operations, impede the investigation of serious crime, or facilitate its commission.[1] (Likely to be rare in A&S)
Configuration Management	Control of system changes
Control	Technique for protecting information assets.
COTS	Commercial Off The Shelf (rather than tailored) products
CPNI	Unified Incident and Reporting Structure managed by the Security Service.
Crack	Overcoming password or encryption. Techniques include “brute force” repetition, and social engineering.
CRAMM	A formal methodology for identifying and managing risk
CSP	ACPO/ACPO(S) Community Security Policy – the basic rules for the systems linked to the Police National Computer
Data Controller	Legally responsible for data in the organisation, whether on paper or electronic, or spoken. In the case of A & S this is the Chief

	Constable.
Data Owner	District Commander or Departmental Head having responsibility for the unit.
Denial of Service Attack	Attack on Technical Services designed to prevent the owners from using it. Often by use of bombardment with network / communications traffic. May be by virus. May be an attack on passwords.
Digital Signature	A technique from Public Key Cryptography for proving that a message has not been tampered with.
Disclosure	Beware – this has two meanings ! In information security, it relates to the disclosure of police information to others: it may be lawful or unlawful; it may be accidental or deliberate. In the criminal justice community it relates to disclosing evidence (e.g. giving details of police evidence to defence).
DPO (or DP &ISM)	Data Protection and Information Security Manager (an A & S post)
Encryption	Translating information into code. May be done by encrypting a medium (eg all on a hard disk), or a message, or all communications by a particular route.
Escrow	Placing software with a third party (viz other than supplier or purchaser) – for commercial reasons. May also be used in encryption arrangements.
FAST	Federation Against Software Theft
Firewall	Device at the gateway to/from a network, controlling and checking information passing through. Purpose – to prevent hacking.
Force Network	See Infrastructure below.
Freak	Hacking into telephone systems.
GPMS	Government Protective Marking Scheme
GSI	Government Secure Intranet. Secure up to RESTRICTED.
Hack	A deliberate attempt to evade information security. Techniques include social engineering, “dumpster diving” in bins, shoulder surfing (see below), “sniffing” (of network connections by use of monitoring software) and “spoofing” (ie masquerading as a computer system with a legitimate link to the target).
Hardware	Physically identifiable equipment in information handling facilities (e.g. computers, servers, printers, routers, hubs, scanners, modems).
Health Check	The process of testing to ensure that an environment is secure. Hijacking Where the hacker takes over a session from a legitimate user, by force fear or fraud.
Information Assets	Information – ***whether on paper or on electronic media***, or spoken - and Technical Services, including computers, telephones, radios and paper processes.
Information Handling facility	See System
Information Security Also known as INFOSEC	Anything affecting the Confidentiality, Integrity or Availability of the Constabulary’s information.
Infrastructure	The A&S information network (often referred to as “the Force Network”), including cabling, network hardware, generic servers and desktop computers and generic implementations of the operating system (currently MS Windows NT4) and desktop applications (word processing and spreadsheet).
Integrity	The assurance that information has been created, amended or

	deleted only by the proper actions of authorised users.
Internet	A global public computer network. With no single proprietor.
Intranet	The use of internet technology on a private network.
IP address	Kind of address for a computer – so that another system can communicate with it. Has a good deal in common with a telephone number.
ISO	Information Security Officer (a post within A & S).
ISP	Internet Service Provider.
ISPE	Technical Services Programme Executive (of the). A group of senior staff which meets quarterly, chaired by the Deputy Chief Constable, for dealing with the strategy of Technical Services in A&S.
IT	See TS
ITSEC	IT Security Evaluation and Certification Scheme – an authoritative national agency.
IW	Information Warfare
LAN	Local Area Network
Malicious software	Usually means viruses. Note that there is a variety of species of virus (e.g. worms).
Message Authentication	A check to ensure that a message has not been tampered with in transit.
Media	Includes disks, tapes, USB storage devices (“sticks” or “pens”), and includes hard disks contained within computers and other devices (such as printers).
Need To Know	The principle that dissemination of information should be no wider than necessary for the efficient conduct of the business in hand and restricted to those authorised.
NOT PROTECTIVELY MARKED	A low level of document protection, a level in the Government Protective Marking scheme
NPIA	National Police Improvement Agency
NSPIS	National Strategy for Police Technical Services
Packet	A recognisable parcel of information: the form in which information passes through networks.
Password	A method of restricting access to known and verified individuals.
Penetration Testing	Using “ethical hackers” to test the security of systems.
Personal data	Information capable of identifying a person.
PGP	Pretty Good Privacy. A system of encryption.
PIN	Personal Identification Number. A kind of password.
PKI	Public key encryption. A modern technique for communicating securely – which requires time, money and resources.
PND	Police National Database
Protective Marking	A government scheme for information security, defined by the Cabinet Office). Characterised by classifying information, and applying security controls according to the classification. of MPS standards.
Removable Media	Excludes hard disks except those designed to be removable. Includes all other forms of media (see above). Main examples are CDs, DVDs, and USB storage devices (“sticks” or “pens”).
Repudiation	Denying receipt or authorship of a communication, or the time of despatch.
RESTRICTED	Compromise would be likely to cause substantial distress, to prejudice investigation or facilitate the commission of crime, to break the law (eg Data Protection Act) or contractual promises, or to disadvantage government or A&S.[2] Likely to include most operational information in A&S.

Risk Assessment	The assessment of threats to, impacts on, and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.
Risk Management	The process of identifying, controlling and minimising or eliminating security risks that may affect Technical Services for an acceptable cost.
SATAN	Security Administrator's Tool for Analyzing Networks. Also extensively used by hackers.
Secret	Compromise would be likely to threaten life directly, or cause serious damage to the continuing effectiveness of highly valuable intelligence operations. (Unlikely to be widely used in A&S)
Security Incident	Any event such as a security breach, threat, weakness or malfunction with has or could have resulted in the loss or damage of information assets including: i. Accidental or deliberate destruction of information ii. Accidental or deliberate modification of information iii. Accidental or deliberate disclosure of information iv. Deliberately causing the unavailability of Technical Services v. Unauthorised access to Technical Services vi. Misuse of information vii. Theft of any information assets viii. Any other event which affects information security.
Sensitive information	An ambiguous expression. Sensitive personal data consists of information as to ethnicity, political opinions, religious beliefs, trade union membership, health, sex life, commission of offences and court proceedings (Data Protection Act 1998). May simply mean information which the writer subjectively regards as sensitive.
Shoulder Surfing	Eg a hacker watching a legitimate user log in so as to be able to copy the process.
Social Engineering	Tricking people to obtain passwords, or access to information or systems. May include searching rubbish bins or masquerading as a technical specialist.
Software	Computer programs.
Super User	Member of the user unit who is not normally an operational user, but who has a responsibility for day-to-day running of the system. Would normally have access to all areas within a computer application, but would normally have access to infrastructure, or database administration only as a user.
SyOPs or SOP	Security Operating Procedure: one document for each system providing detailed operating procedures. These procedures *may (where justified)* amend the general rules in this policy which is a baseline.
System	This expression, which is synonymous with Information Handling facility, poses considerable difficulty. For the purpose of this document a system can be recognised by reference to purpose, and software.
System owner	The District/Departmental head owning the system. Identified postholders where systems are shared by more than one District/Department. List maintained by Information Security Officer.
TEMPEST	The inadvertent communication through radiation from equipment. Threat A recognised security risk, calculated according to risk, vulnerability and impact. Some risks may be accepted.
TOP SECRET	Compromise would be likely to lead directly to widespread loss of life or cause exceptionally grave damage to the continuing

	effectiveness of extremely valuable intelligence operations.[4] Unlikely to be used in A&S.
TS	Technical Services; virtually synonymous with IT – Information Technology; and an old synonym DP – Data Processing.
Unclassified	Not Classified. Viz lower than Restricted. Likely to include information which does not contain personal data.
Virus	A program designed to secretly infect other computer systems. Usually brings detrimental effects. Eg “Trojans” - e-mail attachments containing programs designed to provide a hacker with access to the system; and “worms” which multiply themselves.
WAN	Wide Area Network

APPENDIX A

PHYSICAL SECURITY PROCEDURAL GUIDE

BACKGROUND

Policy specifies that any system should meet Government security guidelines and only Government approved products are to be used. The Security Services Group (SSG) an agency of the Ministry of Defence drew up the specification to these guidelines

ADT Ltd are supplying a Grosvenor Technologies product called Janus as the forces new access system. The system was to consist of personally allocated cards and a proximity card reader on selected doors. The system reads the card on presentation to an external card reader and unlocks the door. The system can be configured to allow certain personnel access to more sensitive sites or offices. Leaving the building will be via a handle or press button door release. (no card is needed to exit a building) This document is intended to define how the new system will be used. For responsibilities and use of cards see appendix ‘A’.

1. Control of proximity card issue and validation

1.1 Current personnel

1.1.1 All force personnel (Police Officers, Police Staff, Specials and temporary staff including contractors and cleaning staff) names and collar / ID numbers have been entered onto a database created to accommodate the new system. On signature, each person well be issued with an individual proximity card which allows access to every controlled external door within the force area where access has been authorised.

1.1.2 The Janus system records access to police buildings by identifying the proximity card used, and it can identify individual doors used.

1.1.3 The system can limit access to specific doors and if needed specific times.

1.1.4 The proximity cards should be carried during periods of duty, they should not be carried in the same holder as a warrant card police Officers & Specials) or identity card (Police Staff).

1.1.5 Proximity cards carry no identifying marks, so if lost / stolen they cannot be connected to police buildings, being found with a warrant / ID card could compromise security.

1.2 New personnel

1.2.1 Each Administration department on a District will hold a stock of un-validated (not programmed) cards. When someone new begins the next card will be allocated to them and their details faxed to the Janus database coordinator using a template drawn up for this purpose. No other means of notification will be accepted. It will be necessary to maintain a register of cards and allocations.

1.2.2 The database will be updated with the new details and the card added to the system. This will validate the card and allow the cardholder to access the doors that have been mandated.

1.3 Leavers

1.3.1 On the last day of employment the proximity card will be recovered by the District / Site Administration department. Admin staff will fax the leaver’s details to the Janus database coordinator.

1.3.2 The database coordinator will then delete the details from the database,

which will invalidate the card.

1.3.3 The card is then available on District for re-use once re-programmed, and this process must be recorded in the register.

1.4 Temporary staff, Contractors and Cleaners

1.4.1 It will be for Districts to decide whom they issue a proximity access card to and for how long.

1.4.2 The same procedure is to be followed as per “3.2. New Personnel” for issue of access cards to temporary staff, contractors and cleaners and the reporting of details to the Janus database coordinator.

1.4.3 Where practicable Districts should arrange for cleaners or contractors to enter buildings via reception areas in preference to allocating cards.

2. Lost / stolen card reporting procedure

2.1.1 Lost cards should be reported to the issuing Site Administration department as soon as possible. The department should immediately report this fact to the Janus database coordinator using the procedure at 3.3.1.

2.1.2 It will be for Site Administration departments to decide if a new card is to be issued and whether a replacement fee (£4) is to be charged.

2.1.3 Worn out or defective cards will be replaced free of charge on receipt of the old card. Stocks of new cards can be ordered from the data base coordinator.

3 Summary of responsibilities

3.1 Users

3.1.1 To keep their proximity card safe and not carried with warrant / ID card.

3.1.2 Avoid tail gating where possible.

3.1.3 Report all incidents involving the security of police buildings to:
Ext. 66103, 66392 or 66168
Fax 66316
E-mail #information security

3.2 Site / District Administration Offices

3.2.1 Issue and retrieval of proximity cards

3.2.2 Update the database co-ordinator regarding issue and retrieval of cards

3.2.3 Report any security incidents or problems with the system to those at 3.1.3

3.3 Data Base Co-ordinator

3.3.1 Activate and de-activate proximity cards on the Janus system following advice from Site / District Admin offices.

3.3.2 Order new cards from ADT

3.3.3 Update the Excel database with details of new staff and delete those that have left.

3.3.4 Amend access levels for those personnel entitled to gain access to restricted offices

3.3.5 Report to those at 3.1.3 any security incidents experienced or reported to them

3.4 Information Services

3.4.1 Make automated backup of the database daily

3.4.2 Maintain the system as per service level agreement

3.4.3 Report any security incidents or problems encountered to those at 3.1.3

3.5 Corporate Information Management

3.5.1 Investigate all incidents and problems associated with the Janus system and seek acceptable or successful conclusions.

3.5.2 Report security breaches to the relevant authorities where necessary
3.5.3 Liaise with the database co-ordinator, District / Site Administration offices, users and suppliers to keep the system running and problem free.

3.6 HQ security staff

3.6.1 Act as database co-ordinator outside of normal office hours including weekends and Bank Holidays, and to assume duties as at 3.3.1, 3.3.3 & 3.3.4 during these periods.

Appendix B
Identification for Staff
Procedural Guide

Introduction

All staff are required to carry and display Identification on the Avon and Somerset Constabulary Headquarters site.
It is intended that this policy will eventually extend to all of the Constabulary's sites.

Valid Identification

Police officers and Special Constables will be issued with warrant cards.
Police staff, including contractors engaged for more than three months will be issued with identification cards.
Other visitors to the headquarters site (including to Training School) will be issued with identifying badges for the duration of their visit at the relevant reception. Badges will be recovered at the end of the visit.

Unaccompanied Visitors

There will be no valid reason for individuals to be found unaccompanied and without identification displayed within police sites, whether they are visitors or members of the Constabulary.
Visitors are normally to be accompanied on police sites.

Carrying Identification

All staff will carry their identification/warrant card at all times.

Producing Identification

Staff will produce this identification on the demand of a member of the public and when exercising a legal power or authority.
Staff will produce this identification on the demand of any other member of staff within police sites, whether on or off duty.

Displaying Identification

All police officers and staff will display identification prominently, at all times while on the headquarters site. Staff will be provided with a lanyard or card holder,

designed to be worn around the neck and to contain warrant cards/police staff ID cards for this purpose. Cards must be displayed above waist height and to the front of the carrier.
Uniformed police officers are excepted if they are visiting the Headquarters site for less than a week provided that their collar number is displayed.
Card holders will be issued where necessary for Health and Safety reasons.
Lanyards must not be used for carrying door access cards (or "prox cards") as this provides the finder with useful information about where the card may be exploited.
Enamel badges are no longer a part of policy: their use will not replace the need for the display of the formal ID document.

Lost/Stolen Cards

Lost or stolen cards will be reported immediately to the Information Security Team by e-mail. The team can arrange replacements.

Reports will include the time, date and place of the loss, details to identify the loser and a brief report of the circumstances.

The Information Security Officer will be responsible for investigating these security incidents.

1.8 Administration

1.8.1 Initially, lanyards have been issued to existing staff through Department Heads.

1.8.2 Identification cards for staff and lanyards for new recruits will be issued by Video Unit and Uniform Stores during Induction.

1.8.3 Replacement cards will be issued on the approval of the Information Security Officer. Replacements for existing cards (viz not lost or stolen) will be issued direct by Video Unit, only where appearance has changed to the extent that the holder is unrecognisable.

1.8.4 Recruits will be issued with cards and lanyards.

1.8.5 A stock will be maintained by Head of Purchasing and Supplies.

1.8.6 Where a member of staff loses his ID more than twice, a charge may be levied on the individual for replacement on the third and subsequent occasions.

1.8.7 Cards and lanyards will be recovered from staff at the end of their service in all cases. Commencement of a career break will be treated as the end of service.

1.9 Compliance

1.9.2 All levels of Management and HQ Security staff will be responsible for enforcing the rules relating to Identification cards.

1.9.3 Staff are required to challenge persons who are within police sites and who are not displaying identification. If they are not satisfied, the person may be required to leave or return to the reception point.

1.9.4 It will be acceptable to allow the visitor to contact the office they are visiting in order to be accompanied on the site.

Appendix C

MONITORING FOR ELECTRONIC DEVICES

1 Introduction

It is possible that sophisticated attackers will attempt to place electronic devices so as to overhear police. This document is intended to address this possibility.

Attackers may be external, but it is quite possible that police employees are involved as principals or accomplices.

Devices are extremely small – and decreasing in size as technology develops. They may be concealed in furniture, equipment, or in the fabric of a building. They may be installed during building work, removals, technical support, a visit or an unlawful intrusion; technical skills are not necessarily required.

At this stage, the risk of such an attack is considered to be low. There are no known instances of this happening in police forces. Yet.

The Information Security Officer is in possession of Receiver and Spectral

Analysis equipment (a “sniffer”). Members of the Information Security Team are trained and authorised to use it.
It is important to note that this work is an additional task for these operators and not their primary role.

2 Strategy

This equipment, its deployment, its operator, and this section of the policy are classified as RESTRICTED.
This equipment/operators will be deployed on the authority of the ISO, as indicated by the risks.
High risks are indicated by the handling of material marked CONFIDENTIAL and above.
High risks may also be indicated by particular threats or vulnerabilities, including:

- Intelligence indicating a threat which demonstrates both intent and capability
- Previous history of threats or attacks
- Operations involving high profile people or events.

3 Operation

3.1 Managers may request a sweep of police accommodation where they believe that it is called for by the risks. Requests can be made in writing, to the Information Security Team.
3.2 This equipment will be deployed on accommodation which is owned by the Avon and Somerset Constabulary. In exceptional cases where it is desirable for the accommodation of other organisations to be swept, a charge of £250 per day plus travel costs will be made (assume one site per day). No liability can be accepted in relation to the provision of this service (see 3.4 below.)
3.3 The equipment will be used only by qualified operators.
3.4 Because of the risk of involvement of internal staff, this work is best carried out discreetly.
3.5 It is important to note that while sweeping reduces the risks, it does not guarantee that there are no operable electronic listening devices. It is also important to remember that this is a snapshot in time.
3.6 The availability of this service cannot be guaranteed.

4 Sweep Results

4.1 Where a device is found, the operator will report to the District Commander/Departmental Head with ownership of the facility and the Information Security Officer without delay. This will be treated as an Information Security Incident. Preference will normally be given to protecting assets over detecting offences.
4.2 It is important to note that results of the sweep may well be ambiguous, requiring further investigation as an Information Security Incident.
4.3 Results will be recorded. The “owner” will be notified.