Force Information Security Procedures Manual

Not Protectively Marked

Reference Information

Responsibilities	
Name of Policy that this SOP is attached to:	Force Information Security Policy
Name of SOP author/reviewer	Director of Information
Unit or Department:	Information Management Services
Directorate owning this SOP:	Intelligence & Information
Version control	
Date of latest version:	30 August 2014
Date Published:	*Strategic Development only*

Contents

A Procedures Manual Conext

A.1 Preface

Information security is vital to the Police Service to aid the quality, availability and management of its valuable information resources.

Security is a process, not a product; it is a management policy, strategy and tactic, fundamental to the well-being of every organisation in the modern digital world. Information security is a foundation for quality management processes, including Service Management (e.g. ITIL and ISO/IEC20000); of determining what you want to do and why, within applicable constraints (business, operational, statutory and governmental); doing it safely and securely and checking it is being done to the required standards. Security management is also an important component of change management and the continuous service improvement process.

Good security is not a goal, a target, a business model in its own right. It is a business enabler; a tool to facilitate safe and legitimate transactions for the business. Lack of appropriate security planning and management controls can lead to serious threats to the business.

All managers and users must play their part in delivering the 5 essentials of Information Security (Infosec):

1. **Confidentiality** – assuring information is available only to those authorised
2. **Integrity** – assuring information is not altered accidentally or deliberately
3. **Availability** – assuring information is available when it is required
4. **Non-Repudiation** – assuring inability to deny actions carried out
5. **Audit** – assuring records of who did what and when are maintained

Absolute security is impossible to attain, and ill-considered delivery will be ineffective and can be a financial and operational barrier to business efficiencies. Risks must be weighed against the business advantages, and appropriate risk management decisions made to efficiently and lawfully deliver the required service at as low a risk and cost as can be achieved. This is usually achieved by the Project Manager, Business Process Owner (or SRO), Accreditor and SIRO working together to assess the business requirements, risks and countermeasures, via the Risk Management and Accreditation Document Set (RMADS) process, and support of the security and operational requirements by adequate technologies, training and documentation for all users. This delivers operational efficiency whilst assuring compliance with national and Force Information Security Policy.

The City of London Police (CoLP) works within the national frameworks of ISO 27001, HMG SPF, the Police Community Security Policy (CSP), the Community Code of Connection (CoCo), and the Code of Practice for the Management of Police Information (MoPI) locally encapsulated into the Force Information Security Policy (FISP).

Police IT networks and systems are part of the National Critical Infrastructure, requiring a wider viewpoint than just City of London Police and national policing. This precludes any overseas access or processing without robust controls which may be demanded by the RMADS review or Data Protection Act. The City of London Police follow the HMG Security Policy Framework should used as context for requirements within the UK/HMG national information security scheme.

A.2 Audience

This procedures document is suitable for, and should be made available to, all staff and users of City of London Police IT systems and information. Non-employee users (such as Local Authority partner staff, contractors, 3rd party suppliers or temporary agency workers) should be given a copy of the FISP and this procedures manual by their CoLP sponsoring manager and briefed with their compliance responsibilities prior to allowing access. The document may be published to non-users, the public and any requesting parties. The document is structured to facilitate review of single sections most appropriate to the reader. Most users will obtain good practical guidance from Section F Personal Compliance; Managers should read the whole document and departmental users should, at a minimum, read the appropriate sections.

A.3 Understanding Risk

The Police Service is adept at risk management in relation to violence and other physical criminality. With the increasing demands for widespread use of IT, high security and sharing outside of the Police, information assurance must become a standard part of IT and governance in day-to-day processes and operations.

All information storage and processing – whether paper based or electronic – has weaknesses (or 'vulnerabilities'), which may be exploited by human frailty or inappropriate use, through to organised 'hacking' into Police systems to access information. To appreciate the risk, and hence what can be done in mitigation, two basic factors need to be considered:

(i) the likelihood of it happening

(ii) the impact if/when it does.

Virus threats provide a simple example:

> The likelihood is very high (there are hundreds of thousands of viruses in circulation and most home and SME personal computers have inadequate protection against them)
> The impact on the Police network can be very high – it may shut down the local Force network, including emergency calls, and cause wholesale disconnection from PNC and other vital Police systems, ultimately risking staff and public safety.

Deploying an effective, organisation-wide anti-virus (AV) system can reduce the risk to an acceptable level. But a single PC deployed without AV can immediately raise the likelihood and impact back to 'very high' by (accidentally or otherwise) plugging into the CoLP network or by using a removable storage device, then connecting that to a network PC. Repeating the same behaviour can cause risks to other sites (for example, a school, Local Authority, Partner's site).

Another risk example is sharing sensitive information by email across the open Internet, where there is a high probability of unauthorised access. This may put vulnerable persons at risk, cause loss of public confidence and render CoLP liable for compensation and/or prosecution – an unacceptable level of impact, and a breach of Police integrity.

Without appropriate training & understanding it is likely staff will not act in line with statutory obligations under the Data Protection Act and MoPI, to the detriment of the public and staff. The personal impact on the affected people can be profound; the professional impact on CoLP can also be high.

Over 70% of information security incidents are caused internally, by authorised users. Most of these are not due to malicious/unlawful intent, but by well-meaning people striving to do their job well, who do not understand risk management and have not been appropriately trained in information security awareness. Lack of IT and information security training raises the impact likelihood to unacceptable levels and facilitates poor business practice.

Provision of 'sensitive' information on the CoLP Intranet, will mean it is made available to all computer account holders, employees – unless specifically hidden behind access control mechanisms.

Where 'sensitive' or 'personal' information is involved, the Force does not want to publish to people without a real 'need to know'? Users must therefore always consider:

(a) who needs to know and why?

(b) assure appropriate availability separation – how are they going to keep it secure?

Technology can reduce the likelihood of security events, subject to staff not by-passing the technical and procedural controls, but cannot reduce the impact should an incident occur. It is thus important everyone is aware of information security risks, has good training, and complies with CoLP and national information security policies.

B Strategic Perspective

Information and Communication Technology (IT) must be deployed, with information strategies, to support the process of providing effective and efficient Policing services. These systems must be developed, operated and maintained in a safe and secure manner.

The aim is to provide information facilities for users. There are management and legal issues which need to be considered to ensure the effective and appropriate use of information technology.

Information is an asset that, like other important business assets, has value to City of London Police and consequently needs to be suitably protected. Information security protects data and its owners and subjects from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and Policing efficiencies.

Strategic Aim:

“To ensure that all Force information is kept secure and only accessible to those who are authorised to have access to it, and to be available when they need it”

City of London Police will allow the use, access and disclosure of information assets only in accordance with stipulated procedures and in conformance with applicable laws, regulations and directives.

It is City of London Police policy to ensure:

1. The Confidentiality of all Force information, whether electronic or paper-based
2. The Integrity of the information by ensuring its accuracy and completeness
3. The Availability of information systems and the information therein whenever required
4. That Information is disclosed only to those authorised to receive it

5. That Information so disclosed is used only for authorised purposes
6. That Regulatory and legislative requirements are met
7. That no IT systems handling protectively marked or personal information are to be made live prior to formal accreditation
8. That all staff and users will be made aware of their obligations with regard to Information Security
9. That each computer system/information process has an accredited set of Security & Data Protection Operating Rules where required by accreditation.
10. That Protection will be through an appropriate combination of personnel, physical, procedural, technical and management security controls.
11. That Enhanced security protection will be provided for information assets that are identified as being key to Force operations or are highly-valued under GPMS or GSC[1]
12. The Information Standards & Policy Group (ISPG) shall be responsible for all policies with respect to information gathered, stored and processed as part of any information system, whether manual or computerised
13. The Information Security Manager will have direct responsibility for maintaining the policy and providing guidance on its implementation
14. Divisional Commanders and Heads of Departments will be responsible for implementing the policy within their areas, and for monitoring adherence by their staff
15. All users are aware that it is their responsibility to adhere to this policy.

[1] GCP comes into effect on 2nd April 2014, replacing GPMS

B.1 Importance of Information Security

City of London Police has a significant investment in computer systems and communications networks. City of London Police is dependent upon criminal justice and other personal information, acquired from numerous sources, which is stored and processed on its computers and the management information that is generated from the data. Increasingly other criminal justice information is remotely accessed using CoLP networks (for example PNC, PND). Failure to maintain appropriate levels of information security could incur significant costs and adversely affect the Force in numerous ways:

1. Loss of information and/or computer processing facilities
2. Loss or unauthorised disclosure of sensitive information relating to individuals and/or other Police information being made available to interested parties (which may include organised crime)
3. Loss of public credibility and confidence, especially via bad publicity
4. Business activities being fully or partially suspended, including prosecutions
5. Loss of accreditation to use other Criminal Justice and external systems
6. Unlawful/criminal manipulation of information, money or goods
7. Having to restore the data, computer programmes and/or equipment
8. Threat to Police or Public safety
9. Payment of compensation and/or civil/criminal fines
10. Prosecution or internal disciplinary action against City of London Police users.

It is therefore essential that there is preservation of the confidentiality, integrity and availability of information held not only electronically within internal systems but also on paper, microfiche, floppy discs, USB drives, portable computers, portable hard disks or CDROM/DVD.

B.2 Objectives

The objectives of this Force Information Security Procedure are to protect City of London Police's information through clear direction and guidance to ensuring that:

1. Clear guidance is provided to all users
2. All users of City of London Police systems, other Criminal Justice entities and the public are confident of the security, accuracy and integrity of the information produced and used
3. Operational damage and interruption caused by security incidents are minimised
4. Confidentiality of personal and other sensitive information is assured
5. All legislative and regulatory requirements, as well as Police mandated standards, are met
6. City of London Police Information Technology is used responsibly, securely and with integrity at all times.

B.3 Scope

This procedure applies to all users granted access to City of London Police's information (paper or electronic), communications or computer facilities and their associated networks. Unless a specific formal exception is granted, all elements of this procedure shall be treated as mandatory within City of London Police.

'Users' include all employees, temporary employees, contractors, agency staff, as well as external partners, suppliers and support people who may be granted access to City of London Police systems and/or information.

B.4 Principles

The principles of Information Security applied by City of London Police are based on the HMG Security Policy Framework (SPF), ISO/IEC27001 and the (Police) Community Security Policy (CSP) and include:

- Physical and environmental security.
- Risk assessment and business impact analysis.
- Access control.
- Asset management.
- Human resources security.
- Communications and operations management.
- Information systems acquisition, development and maintenance.
- Compliance.
- Information security incident management.
- Business continuity management.

B.5 Statutory Compliance

Some aspects of the City of London Police's security will be governed by statutory legislation. Data protection and privacy must be ensured as required in relevant legislation, regulations, and Police standards, and where applicable, contractual clauses. Key information records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and Police requirements.

The City of London Police fully supports lawful obligations on the Police, and many ACPO guidance documents are available within the service. Relevant ones should be consulted in addition to this procedure.

All infosec areas are also governed by National and Police standards, including:

1. HMG Security Policy Framework (SPF)

2. National (Police) Community Security Policy (CSP)
3. Code of Practice on the Management of Police Information (MoPI)

B.6 Implementation and Governance

The Force Information Standards and Policy Group (ISPG), chaired by an ACPO member (normally the SIRO), are responsible for establishing the required information security policies and standards and ensuring compliant delivery. The ISPG will periodically review the Force Information Security Policy to assure ongoing compliance and business relevance.

A subset of the ISPG, chaired by an ACPO member, forms the governance body for City of London Police implementation of PKI and similar services. This is known as the PKI Management Authority (PMA).

Internal and external audit will periodically evaluate security controls while undertaking audit reviews in addition to undertaking specific Information Security audits on a regular basis.

All potential breaches of Information Security, suspected or actual shall be reported and investigated by appropriate bodies (determined by the breach) with serious breaches nationally notified to NPIRMT/PolWARP.

Information Risk will be assessed in accordance with the Information Systems Risk Management procedure and managed in accordance with the Force Risk Management Policy.

B.6.1 Individual Responsibilities

The Accounting Officer (AO) is responsible for lawful and effective business use of Police information within City of London Police. This role is held by the Commissioner of the City of London Police.

The Force Senior Information Risk Officer (SIRO) is responsible for ensuring appropriate risk management and controls are emplaced within the Force.

This role is be held by the Assistant Commissioner of the City of London Police.

The Departmental Security Officer (DSO) is responsible for all aspects of Protective Security which includes physical, personnel and information security as defined within the Security Policy Framework.

The Chief Force Information Security Manager is responsible for ensuring appropriate information assurance controls and risk management is in place for all systems and acts on behalf of the SIRO to accredit their use. In addition the CISO ensures compliance with relevant legislation, including MoPI across the organisation. This role is held by the Director of Information.

The Force Information Security Manager (ISM), more commonly known as 'ISO' within the Police Service, is responsible for policy, assuring compliance, ensuring audits are conducted, together with and local and national incidents and compliance reporting.

The Head of IT is responsible for ensuring the IT Services department operates in accordance with statutory, regulatory, contractual, and business requirements.

The Information Access Manager is responsible for day to day assurance of Data Protection and Freedom of Information and compliance.

The IT Security Officer is responsible for ensuring security technologies and procedures are emplaced and guiding IT Services to lawful and policy-compliant delivery of IT services.

The IT Network Manager is responsible for ensuring that the networks and communications, operating systems and support software and computer centres are secure and meet Policy requirements. IT is responsible for implementation of the IT specialist technical controls.

Information Asset Owners shall value the information they are responsible for and work with project managers, IT Services and users to assure appropriate controls are emplaced and enforced.

Local managers must undertake regular assessments of security risks within their own areas to ensure that the implementation of controls complies with MoPI and the local security procedures (this document) and for ensuring security training is provided to all staff and users within their managerial control.

All staff must accept responsibility for initiating, implementing and maintaining security standards within the force, ensuring they are operationally aware of MoPI.

All users must accept responsibility for maintaining standards by conforming to those controls, which are applicable to them. In particular users must be aware of the risks of introducing unapproved equipment or software onto the network, inappropriate use of the Internet, of sending sensitive information via public (ie Internet-based) email and of inappropriate (or unlawful) use or sharing of Police information externally.

B.6.2 Official Secrets Act

All staff shall be aware/made aware that they are bound by the provisions of the Official Secrets Act 1989, which offers protection under criminal law to official information in certain specialised categories.

The Official Secrets Act 1989 makes it an offence to disclose official information which could be detrimental to the national interest. This definition includes disclosing information without lawful authority which results in the commission of an offence, aiding an escape from legal custody, or impedes the prevention or detection of crime.

Under the new GSC[2] there is an even greater emphasis placed upon personal responsibility for making decisions around the sharing and release of information.

C Acceptable Use

This procedure should be read in conjunction with the Force Acceptable Use Policy, which users must accept before accessing Force systems.

The basic acceptable use tenet is that all City of London Police IT systems and information are only authorised for legitimate business use; private use is normally disallowed. The acceptable use policy is separately documented in detail.

D Exceptions Management

D.1 Objective

To provide a process to enable exceptions to the Force Information Security Policy and Procedures Manual to be recorded, reviewed, authorised/rejected, and audited; and manage any appropriate appeals.

D.2 Justification

As the requirements of the Force become more complex, particularly with the growth and development of national, local and criminal justice partnerships, occasionally there is a strain on compliance with FISP, CSP, MoPI, (CJX) Community CoCo and ISO/IEC27001 security policies and standards.

Unmanaged non-compliance (or non-conformance in quality management terms) causes risk-conflict, audit difficulties and potentially affects security accreditation in addition to infosec problems. But, for valid business reasons, it may be occasionally necessary to provide and subsequently manage a concession, which technically falls outside of the current security policies, but where the risks can be considered manageable and justified.

[2] GSC, the new Government Security Classification, comes into general use on 2nd April 2014 across government.

D.3 Operation

Applications for an exception/concession must be made by the owning manager and approved prior to implementation. Applications must be in writing and sent to the Chief Information Security Officer (the Director of Information).

E Compliance

E.1 Legislation

All relevant statutory, regulatory and contractual requirements shall be complied with. The key laws associated with Police Information and their uses are included in the following table.

Act	Main issues addressed
Freedom of Information Act 2002	Public access to Police and Criminal Justice information
Human Rights Act 2000	Right to privacy and confidentiality
Electronic Communications Act 2000	Cryptography & electronic signatures
Regulation of Investigatory Powers Act 2000	Authorised access to electronic storage and messaging; includes covert surveillance of staff or suspects
Data Protection Act 1998	Protection and use of personal information
Police and Criminal Evidence Act	Assuring auditable procedural and evidential information
Protection of Freedoms Act	Limits retention of biometric information held about innocent individuals
Copyright Designs and Patents Act 1998	Software piracy, music downloads, theft of Police data
Computer Misuse Act 1990	Unauthorised access to computers,

unauthorised modification of data

E.2 Data Protection Act

The Data Protection Act controls the processing of personal data about *living* people. Processing covers any use of the data including its storage and retrieval. In order to process data legally the processing must be in accordance with the eight data protection principles.

See the Data Protection Policy for further details.

E.3 Freedom of Information Act

The 2005 Freedom of Information Act grants a general right of access to records held by public authorities, including the Police, to encourage an attitude of openness. It facilitates public access to scrutinise organisations' decisions and working practises. The key features of the Act, as it applies to the City of London Police, are:

1. The public has a general right of access to all recorded information held by City of London Police. Subject to exemptions set out in the Act, a requester has the right to know whether a record exists, and the right to a copy of that record supplied in a format of their choice.
2. Every Police Force must adopt and maintain a Publication Scheme, listing what kinds of records it chooses to publish, how to obtain them, and whether there is a charge involved.
3. The Information Commissioner’s Office will oversee the implementation and compliance with this Act and the Data Protection Act 1998. Freedom of Information requests are managed by the Information Access Manager.

E.4 Software Licensing

City of London Police uses software in all aspects of its business to support the work carried out by its employees. All commercial software is required to have a licence. Most non-commercial software has licence conditions[3]. City of London Police will not condone the use of any software unless correctly licensed; that is, that a valid licence has been purchased, or if free, that licence conditions are met in full.

Computer software must be purchased through IT Services and installed by a member of IT Services or appropriate arrangements may be made for a relevant member of the department to install the software. Acquisition exceptions may apply to covert or Computer Forensics departments, subject to legitimate licensing and suitable asset management.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto City of London Police systems without prior approval from IT Services.

Users may not make copies of computer software owned or licensed by City of London Police for private use. Misuse of software in this manner can result in disciplinary action.

Managers must ensure that all policies and procedures within their area of responsibility are carried out correctly to achieve compliance with licensing standards.

[3] Even free software will typically have a licence, such as the GPL, LGPL or BSD licence, which may impose restrictions upon the use and distribution of the software. Such licence conditions must be complied with if the software is to be used.

E.5 Force Information Security Policy (FISP) Compliance

E.5.1 Breaches and Discipline

All users who access or use any Force information, communications, computer or network system are responsible for using these resources in a professional, ethical and legal manner, compliant with this policy.

Where deliberate evasion of policies and procedures occurs, or where resources are utilised in unauthorised or inappropriate ways, this can result in withdrawal of IT privileges and/or disciplinary action, under the Force disciplinary policies or codes of conduct.

If abuse of IT systems does take place, the Commissioner reserves the right to regard those responsible for such abuse as being legally accountable.

Users found to have breached the Force Information Security Policy, may be subject to City of London Police's disciplinary procedure. Users who have broken the law may be subject to prosecution.

E.5.2 Seek Guidance

If you do not understand the implications of the Force Information Security Policy and this associated procedure manual or how it may apply to you, seek advice from:

- Your manager/supervisor
- The IT Service Desk
- The Force Information Security Manager
- The Information Management Board

F Personal Responsibilities and Compliance

ALL Users are to READ and RETAIN this section

F.1 Personal Responsibilities

All users are expected to be aware of the FISP and its contents, to operate within its guidelines and accept their responsibilities in assuring the integrity, availability and confidentiality of City of London Police and related information systems.

Users shall seek appropriate guidance and/or training from their line managers if there are any concerns over their ability to meet the FISP standards.

Non-employee users of City of London Police information systems, including contractors and agency staff shall be briefed, and if necessary trained, via their CoLP sponsoring managers, prior to being given access to City of London Police systems and information.

F.2 Acceptable Use Policy

The Force Acceptable Use Policy, which users must accept prior to being granted any access, must be read by all users. See Acceptable Use Policy on CityNet.

F.3 Email Retention

The email system is not to be used as a records management system. Emails must be stored with the associated parent record; all email will be automatically deleted at 12 months. It is the user's responsibility to store email in the most appropriate location and they are personally liable for the retention of material.

F.4 Information Classification

Users are expected to be aware of the relevant information classification, and respect the associated handling controls.

F.5 Information labelling, handling and disposal

City of London Police, in line with the national Police Service and ACPO requirements, have implemented HMG Government Protective Marking Scheme for appropriate information labelling and handling. It covers all formats of information, both physical and electronic. The labelling shall inform the user of the contents' value.

All staff, temporary workers and sharing partners shall be adequately informed/trained about GPMS procedures and have simple access to support documentation in order to assure appropriate recognition and handling of valuable information assets throughout their life-cycle.

Once National Guidance is available about the adoption of the new Government Security Classification (GSC), this information and training will be updated accordingly.

F.6 Sharing Police Information

Sharing of Police information external to City of London Police may not occur without formal authority and until due consideration for MoPI is in place. For example, all appropriate security must be in place, end-to-end, and any Data Protection compliance enforced and a formal Information Sharing Agreement (ISA) must be registered within the Force. All users must refer to the Information Sharing Procedure, associated with the Information Management Policy.

F.7 Remote Access / Off-site Use of Police Information by Staff

Where classified or personal information is to be accessed/used external to Police premises (e.g. on a Force laptop, at home or in partner agency premises), the user must ensure that FISP and Data Protection principles are maintained and the information is appropriately secured.

Staff may not connect their Police computer to other organisations' networks or systems without authority and appropriate security in place.

Prior to taking/using information off-site, authority shall be obtained. Information Asset Owners are responsible for ensuring that the appropriate use and security of the information asset is maintained when information is removed, or accessed externally, from City of London Police premises.

Staff working away from police premises must only use CoLP equipment to access systems and/or process data.

F.8 Removable Storage Devices and Media

Information valued above GPMS **RESTRICTED** or GSC **OFFICAL – SENSITIVE** may not be abstracted from its secure environment onto removable devices without appropriate authorisation. This will not be given without a written risk review. Any means of abstracting the data must maintain the appropriate security for the GPMS/GSC classification.

Only approved devices may be used. This applies to USB pendrives (or similar) and removable hard disks. When not actively in use, all removable media must be secured appropriate to its residual information GPMS / GSC valuation[4].

Police information may only be abstracted to removable devices for authorised business purposes. All removable storage devices must have approved encryption if removed from site.

F.9 Incident Reporting

Information Security incidents are varied and the implications and impact of an incident may not be fully understood at the outset.

[4] For example, a suitably encrypted approved USB device might be suitable for CONFIDENTIAL information and, when locked, require protection as a RESTRITED asset.

Guidance on what is classified as a security incident is listed at Appendix F and also can be found here:

http://citymoss.colp/SiteDirectory/IMS360/SecurityMatters/SIR/default.aspx

Guidance on the reporting and management of a security incident is provided within this procedure.

G Access Control

G.1 General Procedures

G.1.1 Overview

Access to City of London Police's IT systems and information must be protected. Whilst different business applications have varying security requirements, these individual requirements must be identified through risk assessments that will establish appropriate controls to the IT/information systems.

It should be accepted that everything is generally forbidden unless expressly permitted, this should be the starting position for any access control policy for a specific information system.

The relevant information asset owners must ensure a process is in place to cater for exceptional cases, for instance in an emergency, where access is required to information through another User ID/password combination.

Access control rules should be supported by formal procedures and clearly defined responsibilities.

G.1.2 Scope of this Procedure

This procedure applies to everyone with any form of access to a City of London Police computer device or IT system.

G.1.3 User access management

User registration

The user should obtain authorisation from their line manager specifying the reasons for access. The line manager if satisfied that the request fulfils the relevant access control policy, will forward it to the relevant information asset owner for approval and implementation.

The relevant information asset owner must ensure that, before authorising access, the individual has received relevant training in the system, information security and data protection. The relevant information asset owner will maintain an accurate record of authorised users their access rights and training.

The relevant information asset owner should obtain a signature from every user indicating that they are aware of their rights, responsibilities and limitations with respect to the system.

The information asset owner will ensure that a formal user registration and de-registration procedure is in place, granting and revoking access to the appropriate information system. The level of access granted, should only be appropriate, to the business purpose and ensure it's consistent with the FISP.

Records must be maintained for the life of the system and disposed of in accordance with the Force Review, Retention, and Disposal Policy.

Privilege management

Access to special privileges, such as administrator rights, will be subjected to further controls. Allocation of privileges must be limited to as few persons as possible.

Privilege account identities should be kept separate from normal day-to-day user identities and should avoid obvious descriptors such as 'administrator' etc.

An authorisation process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorisation process is complete.

! Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

User password management

Passwords are the most frequently used device for providing computer access control; other authentication mechanisms include IDs, smart cards and biometrics. Normally implemented by software, password systems range from the very simple to the highly complex and can be adapted to meet most needs. Because they are usually a first line of defence, they are particularly prone to attack and if broken, provide the easiest path into a machine.

The relevant information asset owner will ensure that systems incorporate a formal management process for controlling password access. Users must be required to keep passwords confidential. Initial, the user, preferably forced by the system, must change replacement or temporary issue passwords immediately. (See Appendix A - Secure use of Passwords)

Information asset owners are required to establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password.

A secure and effective means of issuing replacement or temporary passwords must be devised. Passwords shall not be sent by e-mail.

Review of user access rights

The relevant information asset owner will review access every 6 months and any redundant accounts deleted. Users who have not used their accounts for 6 months (3 months for privilege accounts) should be contacted and if necessary their accounts deleted. Accounts of users who leave the force must be deleted immediately or where individuals have been suspended the account must be disabled for the period of their suspension.

Privilege accounts will be subjected to greater scrutiny. Quarterly checks will be made to ensure that unauthorised privileges have not been acquired.

G.1.4 User Responsibilities

Password use

Users must ensure that their password is kept secret. Users should adopt best practice in the creation of passwords. Guidance is provided at appendix A of this procedure.

Users should be aware that any activity logged against their user identification is their responsibility.

Relevant information asset owners will adopt an effective password management system. The following controls, to ensure user authentication, are recommended.

1. Where possible passwords should only be issued to individuals. This will ensure accountability;
2. Users should be able to change their password;
3. A secure means of delivery for the initial password should be devised;
4. The initial password must be changed immediately, if not the account should be locked;
5. Previous passwords should not be reused;
6. Passwords must never be capable of being displayed on screen when being entered;
7. Password files should be encrypted;
8. Consideration should be given to providing duress alarm passwords for critical or sensitive systems or users.

Users must not disclose their passwords to others or use another user's User ID or password without authority.

Users must change their passwords if they suspect it has been compromised.

Passwords must not be written down.

Passwords must not be stored in macros or included in any automated log-on process.

Users who need access to multiple services/applications and are required to maintain multiple passwords may use a single quality password, but must exercise stringent security control of this password.

The Force Force Information Security Manager can provide further guidance on password design and usage on request.

Unattended user equipment

All unattended equipment must be subject to appropriate protection depending on its criticality or confidentiality. The relevant information asset owner will determine the appropriate level of protection for each piece of equipment. Users must be made aware of these requirements.

Terminals should be logged-out when not in use and the terminal lock (**ctrl, alt, del** then **Lock Workstation**) facility should be used if the terminal is left temporarily, however briefly.

Clear Desk and clear screen policy

All users should take into account the information classifications, legal and contractual requirements, and the corresponding risks and follow the Government Protective Marking Scheme controls as identified within this procedure for Asset Management and Classification.

The following controls are recommended:

1. Sensitive or critical business information, e.g. on paper or on an electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the work environment is vacated;

2. Computers and terminals should be left logged-off or should be protected by a screen and locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;
3. Incoming and outgoing mail points and unattended facsimile machines should be protected;
4. Unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;
5. Documents containing sensitive or classified information should be removed from printers immediately.

!

> A clear desk/clear screen policy reduces the risks of unauthorised access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

G.1.5 Duress alarms

It is considered appropriate to provide duress alarms for critical or sensitive systems or systems outside force buildings – this must be an agreed procedure between the relevant Information Asset Owner and the Chief Force Information Security Manager. The procedure will include specific use cases as well as determining appropriate counter measures.

G.1.6 Mobile computing and teleworking

Working on protectively marked assets away from official premises (remote working)

Remote working refers to work carried out in a work place that is away from force premises. Although remote working is widely associated with home working, the guidance in this section applies equally to other types of remote working, for example, in hotel rooms, at conference venues. It is assumed that remote working is inherently less secure than when working in the controlled environment of official premises where the level of security in place is determined by the level of threat to that organisation and its assets.

When using mobile computing and communication facilities, e.g. smartphones, laptops, tablets, special care should be taken to ensure that force information is not compromised. This mobile computing section takes into account the risks of working with mobile computing equipment in unprotected environments.

Authorising remote working

Users have the authority to work away from force premises at the discretion of their line manager and can access information remotely where approved by the relevant Information Asset Owner – this is generally undertaken on a system basis rather than by specific users. However, when remote working on protectively marked assets, whether at home, in hotels or other places away from official premises, users are responsible for deciding on appropriate security controls within the environment. For example sitting in a hotel lobby accessing protectively marked assets where information can be easily viewed by others would not be acceptable, but accessing the material from within the hotel room would be.

Information asset owners are required to ensure that when they authorise remote access to the protectively marked information, appropriate physical, document and IT security controls are in place to provide required levels of protection before the access is permitted. In many cases such controls are unlikely to be onerous or limiting in their effect, but it should be recognised that it is rarely possible to provide the same level of security outside the work place as within. Users working from home should not be aware of the risk of 'advertising' that they work on official information at home.

When individuals remotely work on protectively marked information in the absence of appropriate security controls, including procedural controls and other less formal safeguards, such as the presence of colleagues, there is an increased risk of deliberate and accidental compromise.

A remote worker also faces threats that are not necessarily directly linked to their employment. These include equipment theft and accidental or deliberate overlooking or eavesdropping. Continuous personal custody is rarely realistic and in some circumstances may be insufficient. For example, portable IT equipment is a highly attractive target for theft or robbery. IT threats are likely to be higher for the remote worker and could include:

- theft
- viruses
- hacking
- abuse of access rights
- interception - local and remote eavesdropping
- incorrect operation of transmission equipment
- denial of service

The level of physical security in official premises is often not realistic in the home or other remote work places. The vulnerabilities connected with remote working include:

- Weak physical defences;
- Poor IT discipline, for example, the use of insecure hardware and software, the use of unapproved network connections, introduction of malicious software to the remote worker and force systems;
- Insecure handling of documentation and electronic communications.

Exploitation of remote IT system vulnerabilities could lead to compromise of force systems. Whether remote working involves the use of IT, the preferred option, or simply the reading of documents, personal acceptance of responsibility for the protection of the assets involved is fundamental to good security practice.

The security procedures required for remote working include both technical and non-technical controls. Such controls will depend on the level of any protective marking, the requirements for business continuity and the degree to which IT systems are to be used for processing and transmitting information.

Before protectively marked assets are handled remotely, information asset owners should be satisfied that:

- Remote workers understand and accept their obligations in respect of the security controls necessary for the appropriate protection of the assets involved;
- All the necessary practical security controls and arrangements are in place;
- Where applicable, remote workers have been briefed on all security aspects of using IT equipment installed in the remote location.

Using your own software, computing equipment, or removable media

You must not use your own software, equipment, or removable media to process any protectively marked force information i.e. information that will attract a RESTRICTED, CONFIDENTIAL, SECRET, or TOP SECRET marking. NOT PROTECTIVELY MARKED work can be undertaken provided that you have the express authorisation of your line manager and the aggregation of such work would not attract a protective marking.

The use of privately owned computers, personal organisers, other technology or manual systems for the creation or processing of force 'owned' personal data is not permitted except where expressly authorised. Such activity will be conducted in accordance with the Force Information Security Policy, Procedures Manual and guidelines. Information asset owners must ensure this is clearly articulated in their relevant documentation.

Other than for diary, notes and contacts type information[5], all such authorisations for processing force information on personally owned equipment will be in writing through your line manager.

[5] Unless individual entries, or the aggregation of such information held, would attract a protective marking

Connections to the force computer or telecommunications networks will not be permitted for any personally owned computing equipment.

Remote working at home

Individual domestic circumstances and the level of protectively marked information involved will determine what physical security controls are needed and what is practicable to avoid compromise or embarrassment. It should be borne in mind that other users of the home may not share the home workers understanding of the need for discretion.

Mobile remote working (within the UK)

Accidental loss, overlooking or eavesdropping are the greatest risks when an individual is required to remotely work on protectively marked assets, e.g. while travelling. Mobile employees will often be at locations offering even lower levels of privacy than at home and it is essential that a high level of vigilance is maintained.

Normally, protectively marked assets should remain in the individual's personal custody and should not be set down in a public place. They should not, for example, be left in a cloakroom or on a train luggage rack while the individual goes for a meal. Where suitably protected, for example, by the use of a removable hard disk or an approved encryption product, portable computers are preferred to paper documentation.

Mobile remote working (outside the UK)

The threat to the remote worker overseas is, with few exceptions, greater than in the UK. In addition to the greater threat from deliberate theft of sensitive information, there may also be a greater threat from eavesdropping and interception. Individuals should take guidance from Special Branch and the Force Information Security Manager on the local threats.

The situation needs to be assessed on a country-by-country basis. It is not advisable, even in notionally friendly countries, to work outside secure premises without a full prior assessment of the risks.

Remote IT equipment, even when off-line, should be regarded as an extension of the work place system. It requires the same effective level of physical, technical and procedural security. Remote working is only permitted on dedicated force owned equipment with all the hardware, software and access control supplied and controlled by the force.

Transfer of Data (outside the UK)

Personal data shall not be transferred outside the European Economic Area, unless that country has an adequate level of protection for the rights and freedoms of data subjects.

Transfer of personal data to the United States is possible under the Safe Harbour arranged by the European Commission and the US Department of Commerce. This enables lawful transfer of data to US organisations that have signed up to comply with a set of data protection principles and to follow agreed guidance.

Otherwise, in determining what amounts to an adequate level of protection consideration will include the following:

- the nature of the personal data;
- the country of origin and destination;
- the purpose for which it is intended to be processed; and,
- the laws, and controls in force in the country in question.

The Data Protection Act (Sch. 4) provides for circumstances in which the above does not apply to a transfer. These include where the transfer has been consented to by the data subject or forms part of a contract with them, is necessary in the substantial public interest, the vital interests of the data subject or is in connection with legal proceedings.

Information asset owners should develop procedures for the assessment, authorisation and recording of transfers of personal data from their system to countries outside the European Economic Area.

The Recording and Dissemination of Intelligence Material Code of Practice and associated local procedures are recommended as a model of good practice in this area. Overseas transfers should be thoroughly risk assessed, documented and receive a Superintendent’s authority.

Internet access

Internet connections should not be used for transmitting protectively marked information unless protected by approved encryption (at least 256bit).

There are a number of problems associated with connection to the Internet. The most damaging are viruses, spyware and hackers. Viruses, in particular, pose a threat to both the remote worker's own system and, where networked, to the department's or agency's on-line system.

Internet traffic may be routed anywhere in the world, regardless of the source and destination of the material; therefore great care must be taken, when sending personal data electronically, to ensure that the level of protection is adequate in the circumstances.

Remote access to force systems, if permitted and properly authorised, from abroad will amount to processing personal data in that country. Any such access must be subject to adequate protective measures by the information asset owner.

As a general rule, personal data, including photographs that are not already openly available should not be placed onto the Internet without the consent of the data subject.

Communications security

Intercepting communications can often be complex and difficult to achieve, but in the right circumstances can be relatively straightforward. Some simple rules can be applied to voice, fax, video and data transmissions to manage the risks.

Remote workers who are required to transmit information protectively marked CONFIDENTIAL and above should only use approved secure communications equipment. Further advice can be obtained from the Force Information Security Manager.

Transmission of documents and other assets

The carriage of protectively marked assets to, from and between official premises and remote work places should be conducted in accordance with the Government Protective Marking procedure provided within this document.

G.2 Technical Procedures

G.2.1 Network access control

Network Security

Network Security is concerned with the management and control of all the elements, that is, hardware, software, information and documentation contained within the network infrastructure. Connections between networks can be complicated by the differing security profiles of the two connecting networks, and the business requirements of the connection. Such connections should conform to the standard outlined in HMG standards, advice on which can be obtained from the Force Force Information Security Manager

Access to the network infrastructure should be limited to using procedural, physical and logical controls, and supported by network monitoring, accounting and audit functions.

All users of the network must be identified, and have their identity confirmed by a suitable authentication process. The creation of false users must be prevented by the protection of the associated management functions.

Passwords provide only one level of user authentication, and stronger mechanisms, such as Personal Identification Devices (PIDs), tokens and biometrics, should be used whenever highly privileged user-IDs are being protected. Passwords that are stored for use in verification processes must be protected from disclosure, modification and replay. Normally storing passwords in an encrypted form does this. Wherever possible, passwords should not be transmitted across networks in their plain form.

Policy on use of network services

Users will only have access to the network and services they have been authorised, by the relevant information asset owner, to use.

Due to various technical changes to the UK public telecommunications networks over the last few years, including the phased switch to new and digital networks, the National Technical authority for Information Assurance (CESG) can no longer guarantee the protection of RESTRICTED data sent over these networks (e.g. PSTN, which includes GTN). This is largely due to the fact that the specified routes of calls cannot be guaranteed, and in some cases can be re-routed outside of the UK.

As a result there is an inherent increase to the risk of vulnerability and therefore potential compromise.

This is NOT an outright limit on RESTRICTED telecommunications on existing systems, but rather departments are now required to conduct a risk assessment to ascertain whether they can accept the risk.

Protectively marked information up to and including RESTRICTED may be transmitted via Government Assured Networks, this includes GSI, PNN, MOD, CJSM but **does not include** GOV.UK, GCSX or NHS.

The Criminal Justice Extranet (CJX) links forces and other criminal justice agencies to each other via a common backbone allowing for the exchange of e-mail and information within that community. It also provides a link to the Internet and other external networks for both e-mail, Web browsing and information access.

Inter-Force/Agency e-mail at the RESTRICTED level does not require encryption within the CJX or Government Assured Networks..

User authentication for external connections

The relevant information asset owner will determine the level of authentication-required dependent on the criticality or confidentiality of the information system. The risk assessment may determine that authentication is desirable even at the level of the force network or the application itself.

External connections will be subject to authentication consistent with the criticality or confidentiality of the information system concerned and not less than that prescribed in the Criminal Justice Network (CJX) Code of Connection and HMG S(E)N 99/1. The security policy for external connections to the force network, incorporating these standards, will be adhered to.

It is important to ensure that protectively marked information is transmitted only to the correct recipient. Originating callers should be satisfied that they are speaking to the intended recipient and that the recipient is authorised to receive that information. Verbal authentication would be usual for telephone calls and radio transmissions.

Facsimile transmissions should also include an authentication procedure since misdialling could transmit to an unauthorised machine, or faxes could be sent to an unattended device.

Remote diagnostics and configuration port protection

Physical and logical access to diagnostic ports will be securely controlled. A documented procedure to authorise and control access to a diagnostics port must be established.

Ports, services, and similar facilities installed on computer or network facilities, which are not specifically required for business functionality, should be disabled or removed.

Segregation in networks

The IS & T Director is responsible for the control of the force network and for ensuring that network services users and systems are segregated and securely routed.

Network partitioning is a powerful method of separating different communities and restricting user access within a network. It can be implemented in a number of ways:

Physical - this is the process of maintaining physically separate networks or infrastructures for different systems to ensure that one does not allow unauthorised access to the other. It provides the most assured overall security but at the price of duplicated equipment and administrative overheads.

Logical - there are a number of different techniques to achieve logical partitioning by:

- **Physical Address** The network defines a group of physical addresses, a subset of all the physical addresses on the network, as a community. It enforces controls on which physical addresses can be used to access other addresses within the community. Some networks can control which protocols may be used from a given address, for example, allowing e-mail but not file transfer.
- **Identifier** The network recognises different user communities by the user identifier. Such communities are often known as a Closed User Group, and tend to be implemented by vendor dependent applications.
- **Encryption** All users of a particular community (sometimes called a COI or Community of Interest) or sub-network are equipped with encryption facilities, thereby creating a Virtual Private Network or "Tunnel". Distributing keys only to the authorised members of the community enforces the partition. This provides very effective partitioning.
- **Routers** These are network communications devices allowing, or barring, packets from being transmitted across sub-network boundaries. Their

routing tables can be set up to control access between LANs according to either the sender's or recipient's network address. These devices are not normally considered by their vendors to be security devices, but communication devices for the efficient implementation of network infrastructure.

- **Secure Gateways** Commonly known as Guards or Firewalls, act as bridges or routers that perform a greater level of security checking before passing on data packets across network boundaries. They act as barrier devices, and are often implemented where a trusted network interfaces to an un-trusted network. It is important to realise that a Firewall is a collection of trusted devices forming an architecture that provides Firewall functionality.

Security of network services

The Technology Section will maintain a clear description of the security attributes of all network services used by the force.

Network connection control

For guidance on how to determine the nature and level of IT security controls required depending on the differing security profiles of the connecting networks – contact the Force Information Security Manager who can advise about connecting business domains. An approved circuit may be used to pass information protectively marked up to and including a specific level, normally RESTRICTED, without being encrypted.

An 'approved circuit' is a landline, either fibre-optic or wire, and associated terminal equipment, to which certain electro-magnetic and physical safeguards have been applied in order to prevent unauthorised interception. Because such circuits are usually under close control, the risks are reduced and higher protective markings can be conveyed without encryption.

The incorporation of controls to restrict the connection capability of the users may be required by the access control criteria for shared networks, especially those extending across organizational boundaries.

G.2.2 Operating systems access control

Automatic terminal identification

Relevant information asset owners should consider automatic terminal identification to authenticate connections to specific locations and to portable equipment depending on the criticality or confidentiality of the system. This risk assessment shall be documented and reviewed periodically.

Terminal log-on procedures

Access must only be permitted through a secure log-on procedure. The following controls are recommended:

- System or application identifiers should not be displayed until the log-on has been successfully completed.
- Display a general notice warning users that authorised users must only access the system.
- Not provide help messages that would assist an unauthorised user to gain access.
- Limit the number of failed log-on attempts to a maximum of three then disconnect and provide no assistance. Where possible user accounts should be locked after three unsuccessful attempts to log-on. If this is not possible a minimum ten-minute time delay should be introduced prior to any further attempts to log-on being permitted. Record all failed attempts in an audit log.
- Where possible the minimum time limit for log-on should be at least one minute and the maximum time permitted should be three minutes. Outside these time limits the log-on procedure should be terminated.

Where possible the following information should be displayed upon a successful log-on:

- The last time and date of a successful log-on.
- Details of any unsuccessful attempts to log-on since the last successful log-on.

User must report, through their normal management channels, any unusual or suspicious successful or failed log-on attempts.

User identification and authentication

The user naming standards for User ID’s will be based on Warrant card numbers for Officers and the payroll numbers for other members of staff. Single sign-on is recommended, this will reduce the opportunity, by the presentation of further sign-on screens, for unauthorised users to attempt to access other systems for which the authorised user has no permissions.

Password management system

See Appendix A - Secure use of Passwords.

Utilities

Control must be kept of utility programs so that they cannot be used to deliberately or inadvertently corrupt data, systems or software. System users must not load or use utility programs. Staff responsible for diagnostic across the enterprise will document procedures to ensure that only necessary utilities are maintained and that only authorised persons can access and use them for specific purposes. Utility programs should be removed when not in use. An audit log of use must be maintained and may be required in any subsequent investigation where digital Forensic Evidence is required.

Terminal time-out

Force terminals must be configured to time-out after a set period. The period of time should be adjustable depending on the confidentiality or criticality of the system. As a maximum threshold, screens should revert to the log-on screen after ten minutes.

Limitation of connection time

Where available system access will be limited to connection times to the work pattern of individual users – providing additional security for high-risk applications. Attempts to log-on outside the specified period should be logged and create an alert.

G.2.3 Application and information access control

Information access restriction

The relevant information asset owner will ensure that access to information is in accordance with the access control criteria for that information. Users will only be accorded the minimum rights necessary to perform their role.

Sensitive system isolation

Systems processing information protectively marked at CONFIDENTIAL or above, or other critical systems, will where possible, have a dedicated environment and only share resources with trusted applications. Sharing must be agreed in advance with the Head of Technology and the Force Information Security Manager and extra security controls considered commensurate with HMG standards. Relevant advice can be obtained from the Force Information Security Manager.

H Asset Management

H.1 General Procedures

H.1.1 Accountability and inventory of assets

Accountability

The following are examples of the assets of the force which require protection:

- Personal data relating to the user of any force service must be protected against loss, damage, or unwarranted disclosure in line with the relevant data protection and privacy legislation;
- Corporate information base of the force in general must be protected against loss, unwarranted disclosure, or introduction of erroneous content;
- Force information infrastructure (comprising the applications and delivery platforms) must be protected against threats to its availability and integrity of the service offered;
- Authentication credentials must be protected against forgery or unwarranted use;
- Objects that represent monetary or other value must be protected against fraud. Some of the force transactions are likely to result in cashable orders that must be properly controlled, some may relate to the delivery of goods that can be misappropriated.

Inventory of assets

All assets should be clearly identified and an inventory of all-important assets drawn up and maintained.

The information asset owner will draw up inventories for all relevant information assets.

Inventories will include:

- Information Assets – databases, system documentation, user manuals, business continuity plans, etc.
- Software Assets – application software, system software etc.
- Physical Assets – computer and communications equipment, specialist equipment (power supplies, air conditioning units etc.)
- Information asset owners should conduct an audit every two years

The process of compiling an inventory of assets is an important prerequisite of risk management.

H.1.2 Information Classification

Classification guidelines

Information and related IT assets have a value. Information asset owners should know what assets they hold in order to make best use of them, to manage them effectively and securely, and to conform to legal requirements. The value of assets plays a part in determining the associated security requirements.

Classifications and associated protective controls for information should take account of force needs for sharing or restricting information and the impacts associated with such needs.

The value of information is based on its protective marking. However, even information having no protective marking will have value, expressed in terms of the time, cost or effort of replacing it if lost or corrupted, and it will merit inclusion in an asset valuation exercise.

The costs of losing and replacing such assets need to be considered by information asset owners when developing security policies and carrying out risk assessments.

Protectively Marking Information

‘Protective Marking’ is the method by which the originator of an asset, indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage and movement both within and outside the originator’s own department or force and its ultimate method of disposal.

Security controls are required where there is a risk that the deliberate or accidental compromise of assets will interfere with the effective conduct of the Force’s business.

An effective system of control is essential for the protection of protectively marked and other valuable documents against compromise. Such a system must allow information asset owners and their contractors to know:

- What protectively marked documents they hold;
- What level of protection it must be given;
- Where it is held;
- Who is authorised to see or use it and, at the higher levels of protection;
- Who has had access to it or has used it in the past.

Protectively marked or other valuable assets are at risk during transit from accidental or deliberate compromise. To protect such assets when in transit the means of carriage must be reliable, the packaging robust, and the attractiveness, identity and source of the assets concealed under plain cover. Where higher levels of protectively marked assets are involved, a system of audit must be built in to track such assets and to reveal any actual or attempted tampering.

For further detailed information see Protective Marking & Handling in this procedure.

I Communications and Operations Management

I.1 General procedures

I.1.1 Documented operating procedures

All information systems must be subject to security operating procedures (SyOPs). Such a procedure will comply with this framework, the relevant system security policy (SSP) and exert whatever additional security controls a local risk assessment deems necessary. Careful consideration must be given to the recommendations of this framework and the results of any risk assessment. All decisions must be justified and documented.

The security operating procedures will be owned, managed, and maintained by the relevant information asset owner. The SyOPs must be readily available to all users at all times for reference. The relevant information asset owner will undertake responsibility for auditing the system to ensure compliance with this procedure, relevant system security policies and their own security operating procedures.

Auditing policy, practice, procedure and results will be fully documented and subject to quality assurance checks by the Force Information Security Manager. The policy will be reviewed annually. The Force Information Security Manager must approve all security operating procedures.

I.1.2 Security of system documentation

System documentation can provide valuable information to unauthorised persons attempting to access systems. Relevant information asset owners must ensure that distribution of such material is minimised. System documentation must be kept securely locked away when not in use. Sensitive system documentation held on computer must have additional access controls applied. Effective audit procedures must be established. These procedures must be regularly reviewed and tested by the relevant information asset owner and commensurate with the requirements of the Government Protective Marking Scheme.

I.1.3 Operational Change control

In order to minimise the corruption of applications there must be strict control over the implementation of changes. The relevant information asset owner authorises and oversees the implementation of locally owned system changes. Changes to centrally owned resources will be implemented and controlled by the Technology Department.

Change Control procedures should ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system that are necessary for their work, and that formal interdisciplinary agreement and approval for any changes are obtained. Changes to facilities and systems should be controlled. The responsibility for controlling changes to the facilities lies with the relevant information asset owner.

The following items should be covered:

- Identification and recording of any changes to the system.
- Planning and testing of changes.
- Analysis of the potential impact of such changes.
- Approval procedure for proposed changes.
- Communication of change details to all relevant persons.
- Procedures and responsibilities for aborting and recovering from unsuccessful changes.

I.1.4 Segregation of duties

Relevant information asset owners will ensure duties and areas of responsibility are segregated in order to reduce opportunities for negligent or unauthorised modification or misuse of information or services. This segregation of duties will be documented as part of security operating procedures.

Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent. The possibility of collusion should not be forgotten when designing the controls.

I.1.5 Separation of development and operational facilities

Developmental activity must, where practicable, be kept separate from the live system. Any changes to the operational system will be subject to documented change control procedures, as described above.

I.1.6 Third party service delivery management

The relevant information asset owner must identify any risks and adopt appropriate control measures prior to any external service management being utilised. The contract with the external provider will specify the necessary measures needed to ensure that the relevant information system retains its confidentiality, integrity and availability.

The force should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disasters.

I.1.7 Protection against malicious software

No unauthorised software is permitted on any device connected to the City of London Police Network.

All access to email resources must be undertaken via an approved force gateway, as accredited by the force information security manager, using only those email programs supplied by the IT department.

All access to Internet resources must be undertaken via an approved force gateway, as accredited by the force information security manager, using only those email programs supplied by the IT department.

Any external force connection is subject to monitoring.

The IT department will maintain anti-virus software across the force. No device is permitted to connect to the force network without appropriate anti-virus controls.

I.2 Exchanges of information and software

Any exchange of information with external organisations must be subject to a formal protocol. Such a protocol will address responsibilities and liabilities, exchange procedures, data protection act considerations, audit, information classification and handling, and information security in general.

I.2.1 Security of media in transit

Security of information assets in physical transit must be consistent with the protective marking of the information.

I.2.2 Electronic commerce security

Electronic commerce will not be entered into without the prior express approval of the Technology Programme Board.

Should any such activity be approved, in the future, it must first be supported by a security policy designed to protect the confidentiality, integrity and availability of force information. Consideration must also be given to protecting the force from fraud, contractual disputes and unauthorised disclosure or modification of information.

I.2.3 Publicly available systems

Information must not be made publicly available on force information systems unless expressly approved by the relevant information owner. Published information must be protected from modification. (see Intranet Policy)

Due to various technical changes to the UK public telecommunications networks over the last few years, including the phased switch to new and digital networks, the National Technical authority for Information Assurance (CESG) can no longer guarantee the protection of RESTRICTED data sent over these networks (e.g. PSTN, which includes GTN). This is largely due to the fact that the specified routes of calls cannot be guaranteed, and in some cases can be re-routed outside of the UK.

As a result there is an inherent increase to the risk of vulnerability and therefore potential compromise.

This is NOT an outright limit on RESTRICTED telecommunications on existing systems, but rather departments are now required to conduct a risk assessment to ascertain whether they can accept the risk.

Digital mobile phone services based on pan-European standards, DCS 1800 and GSM offer some degree of protection to calls made on them. Radio transmissions between the handset and the base-station are encrypted; however when a call is passed onto another base-station within the cellular network or to the PSTN it is in clear.

I.2.4 Internet usage and protective marking

Information protectively marked CONFIDENTIAL or above must not be transmitted over the Internet, or similar networks. Information protectively marked RESTRICTED may be transmitted over the Internet, or similar networks, provided that an appropriate grade of encryption is used.

Information asset owners making use of Internet or similar services are reminded that this is an area of rapid technological change, attracting considerable public attention, with the prospect of appreciable embarrassment should mishaps occur. There are no 'fit-and-forget' solutions to security in this area; new technical threats to security appear frequently, and some may defeat current protective controls. The continued effectiveness of any local protective controls must be monitored regularly. For the common good, security incidents must be reported promptly, and any corrective action recommended should be promptly applied.

I.2.5 Other forms of information exchange

Information is exchanged in a variety of ways such as telephone, fax, video, etc. Great care must be taken to ensure that information exchange and disclosure takes place only in accordance with Force instructions. Prior to disclosure personnel should ensure the identity of the recipient and that they are entitled to receive such information. Disclosure of personal information must adhere to the provisions of the Data Protection Act. Any information exchange with an outside agency must be subject to a protocol as described above.

Voicemail systems are inherently vulnerable to hacking and therefore should never be used for protectively marked messages.

I.3 Technical procedures

I.3.1 System planning and maintenance

Capacity planning

Relevant information asset owners will ensure that adequate processing power and storage are available to meet projected demand. The Head of Technology is responsible for capacity planning in respect of centrally owned IT resources.

System acceptance

System or project managers will document the acceptance criteria for new information systems, upgrades or new versions. Any new system, upgrade or version must be tested prior to acceptance or installation.

I.3.2 Housekeeping

Information back –up

The relevant information asset owner is responsible for agreeing with the IT department the appropriate settings for the backup of information. Frequency will depend on the criticality or confidentiality of the data.

The relevant information asset owner should ensure that the IT department test the integrity of the backup by performing the restore operation on an agreed basis – at least once a year.

All backups and statutory data must be stored in a manner consistent with its criticality or confidentiality. Wherever practical, storage of backup media should always be in a building other than that where the original data is located.

The IT department is responsible for the management and maintenance of the backup solution including the engagement with third party suppliers where backup of data is managed under contract.

Relevant information asset owners must determine and document a policy of data retention, weeding and archiving consistent with the requirements of the Management of Police Information.

Fault logging

All faults to force systems shall be reported to the Technology help desk. Faults to other systems will be reported to the relevant information asset owner. All faults will be logged and corrective action documented. Fault logs will be reviewed regularly to ensure all faults are dealt with and that security has not been compromised. Reviews will be documented; frequency will be determined and documented, based on the criticality or confidentiality of the system.

I.3.3 Network management

Network controls

The IT department will be responsible for the operation of the network and will ensure data security controls are established to prevent unauthorised access. Particular care must be taken with regard to protecting data passed over public networks.

The IT department will establish effective procedures to counter any breaches of security. All breaches or suspected breaches of security must be reported to the Force Information Security Manager.

I.3.4 Media handling and security

Management of removable computer media

Relevant information asset owners will document procedures regarding removable computer media such as disks, tapes and printouts. Media should not be removed without express permission. Security measures consistent with the criticality and sensitivity of the data should be applied.

Information handling procedures

Relevant information asset owners should determine a media handling and storage policy commensurate with the relevant protective marking baseline standards. Media includes not only removable computer disks, but also, mail, telephone and fax services, photocopiers, post (internal and external), video, voice mail, paper and any other means of recording information, electronically or mechanically.

The policy should determine the handling, labelling and secure disposal of all types of media, and establish a documented audit trail and local audit regime. The purpose of these procedures will be to ensure that information assets are not lost or damaged.

Security of system documentation

System documentation should be stored securely with appropriate access controls limited to authorised users only.

I.3.5 Monitoring system access and use.

Event logging

Once an information system is in use, it is essential for security management personnel to be able to track the way in which the system is used and to ensure that security controls are effective in practice. Specific events and details relating to the operation of the system and its security controls must be recorded for subsequent inspection and analysis. More than other forms of security, information security measures are liable to be influenced by technology developments and re-configuration, and regular audit review is essential.

The following events should be logged and retained for at least one year:

- Changes to user or group management.
- Log-on and log-off (except for successful log-ins).
- Changes to security policy.
- The use of privileges and restart or shutdown of the system.
- Archiving and deletion of audit logs.

Information logged should include; User ID's, date, time, type of event, files and records accessed, programs, utilities, devices used and terminal identity and location.

Operating systems generally record both successful and unsuccessful events. However, it is the case that the details of unsuccessful events can be more revealing Operating systems are capable of recording vast amounts of detailed information about a wide range of system events. However, most operating systems have facilities to allow the system manager to define and select which events are to be recorded in the audit log as security audit messages. Generally, for the purposes of system security, it is the recording of exceptional events that is required and will be of greatest interest in determining compliance with the System Security Policy.

Monitoring system use

The level of monitoring will depend on the confidentiality or criticality of the system and the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations.

Relevant information asset owners must inform users that their activities are being monitored.

It is important to establish what are the normal and acceptable patterns of use of your system before you can recognise potential security problems. Once this is done procedures should be established to regularly review the audit log. Consideration should be given to monitoring the following:

- The number of unsuccessful log-ons.
- Accounts with privileged facilities.
- Access failures.
- Trends in unsuccessful log-ons.
- Out of hours usage
- Usage trends of specific accounts.
- Tracing of selected transactions.
- Trends in reports printed.

The audit log should periodically be analysed. The size, number of users and amount of system use will help determine how often this should be done. The most common type of report is a brief daily listing of selected events that is created from running a batch job every evening before midnight. It is important that such reports are reviewed as soon as possible in order to gain early warning of any system security breaches.

The relevant information asset owner must establish and document an effective monitoring regime. The Force Information Security Manager who will conduct quality assurance checks of the audit records supplied by the relevant information asset owners, and report the findings to the Head of the Professional Standards Unit must approve this regime.

Clock synchronisation

Computer clocks must be synchronised to ensure the accurate recording of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Computer and communication devices that have the capability to operate a real time clock must be set to local standard time.

There must be procedures to check and correct time variations including change over to and from summer time.

J Protective Marking and Handling

The originator of a document (whether in hard copy or electronic form) should consider whether it needs a protective marking. Applying a protective marking to a sensitive information asset indicates to others the appropriate level of protection and security controls required to protect it against compromise.

When applying protective markings the originator should bear in mind that security controls can be costly; the higher the level of protective marking, the greater the cost of protective controls it attracts. Consequently, it is important to take into account the level of access required and the implied cost of the protective controls that should be given when applying a specific protective marking.

Applying too high a protective marking to an asset can inhibit access, lead to unnecessary protective controls and impair the efficiency of Force business. Conversely, applying too low a protective marking can put assets at risk of compromise, since the appropriate controls may not be in place.

J.1 Staff Responsibilities

Line managers are responsible for ensuring that individuals correctly mark sensitive assets.

Only the originator can protectively mark an asset or change its protective marking, though holders of copies may challenge the level of protective marking applied. Where agreement cannot be reached, the information asset owner will determine the protective marking. Final arbitration rests with the Force Information Security Manager. All challenges to a protective marking and decisions taken must be recorded and retained with the information to be protectively marked.

Where the originator is no longer available, his/her successor becomes responsible. Where a successor cannot be traced, the holder of a copy document may change its marking only after consultation with all other addressees.

When assessing the value of an asset it will be necessary to consider the direct and indirect consequences of compromise in relation to a breach or loss of:

- Confidentiality – the restriction of information and assets to authorised individuals.
- Integrity – the maintenance of information systems and physical assets in their complete and proper form.
- Availability – the continuous or timely access to information systems or physical assets by authorised individuals.

J.2 Protective Marking Identifiers[6]

A comprehensive list of the criteria covered by the system is at Appendix B, but the following extract covers most situations relevant to police work:

J.2.1 NOT PROTECTIVELY MARKED

The compromise of this material would not be likely to have the impact warranting the security measures mandated for protectively marked material, but the absence of a protective marking does not necessarily mean that the material may be made freely available.

J.2.2 PROTECT

Impact level 1

The compromise of this material would be likely to cause:

- No impact on life and safety;
- Minor disruption to emergency service activities that require reprioritisation at local (station) level to meet expected levels of service;
- No impact on crime fighting;
- No impact on judicial proceedings;

[6] The Government Protective Marking Scheme (GPMS) is being replaced by the Government Security Classification. Although the Government have gone live with GSC in April 2014 the Police service have yet to adopt it.

Impact level 2

- Inconvenience or cause discomfort to an individual;
- Minor disruption to emergency service activities that requires reprioritisation at area / divisional level to meet expected levels of service;
- Minor failure in local Magistrates Courts.

NOTE: Not to be used for operational issues; Must be accompanied by a "Descriptor" (e.g. PROTECT – STAFF)

J.2.3 RESTRICTED

The compromise of this material would be likely to:

- Cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness or security of the UK or allied forces;
- Prejudice the investigation or facilitate the commission of crime;
- Impede the effective development or operation of government policy;
- Breach proper undertakings to maintain the confidence of material provided by third parties;
- Breach statutory restrictions on disclosure of material (e.g. unauthorised disclosure of personal data contrary to the Data Protection Act);
- Disadvantage government or the Force in commercial or policy negotiations with others.

J.2.4 CONFIDENTIAL

The compromise of this material would be likely to:

- Prejudice individual security or liberty;
- Cause damage to the effectiveness of valuable security or intelligence operations; or
- Impede the investigation or facilitate the commission of serious crime.

- Seriously impede the government policies
- Shut down or otherwise substantially disrupt significant national operations.

J.2.5 SECRET

The compromise of this material would be likely to:

- Threaten life directly, or seriously prejudice public order, or individual security or liberty or
- Cause serious damage to the continuing effectiveness of high valuable security or intelligence operations.

J.2.6 TOP SECRET

The compromise of this material would be likely to:

- Lead directly to widespread loss of life; or
- Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

J.3 Handling

See Appendix B for a full description.

J.3.1 RESTRICTED AND CONFIDENTIAL

Baseline security measures are sufficient.

J.3.2 SECRET

All material protectively marked SECRET must be recorded on movement sheets when it is received, despatched, destroyed, or moved to other locations or branches.

As an added measure, originators must number each copy and record them in a register.

J.3.3 TOP SECRET

All TOP SECRET material must be recorded on movement sheets when it is received, despatched, destroyed, or moved to other locations. You must keep copies of material to the minimum necessary. As an added measure, originators must number each copy and record them in a register.

A register for recording the movement of SECRET and TOP SECRET material must be maintained by all units. As a minimum this register must record the date out/returned, addressee, seal number and the name of person conveying the material.

J.4 Physical Storage

J.4.1 Storage Rules

Protectively marked material should be stored in a secure environment, which is defined as a barrier, or combination of barriers, providing protection commensurate with the risk of compromise.

RESTRICTED material should be protected by one barrier internal to the building e.g. a locked container.

CONFIDENTIAL material should be protected by two barriers internal to the building e.g. a locked container within a locked room.

SECRET or TOP SECRET material should be stored in approved security containers.

Effective key control systems must be in use to ensure access is limited to those who need to access the particular material and to provide a record of keys issued, where appropriate.

J.4.2 Destruction

Whilst the current “Blue Bins” are commonly referred to as confidential waste bins this should not be confused with the Protective marking of CONFIDENTIAL. The Blue Bins have been security assessed as being acceptable for information to PROTECT.

PROTECT documents must be torn by hand into a number of pieces before being placed into the “Blue Bin”

RESTRICTED documents must be shredded prior to being placed within the “Blue Bin”.

CONFIDENTIAL documents must be shredded using a crosscut shredder. The Force Information Security Manager can provide advice on the purchase of shredders.

SECRET documents may be destroyed using a cross cut shredder configured to the government standard (60 sq. mm).

For advice on the destruction of TOP SECRET documents and guidance on all aspects of physical protection contact the Force Information Security Manager.

J.5 Movement of Protectively Marked Material

J.5.1 CoLP Personnel

If protectively marked material is being carried in a public place, it must be kept under cover with no outward indication of the contents. The material must not be left unattended and outside the immediate direct control of the carrier at any time.

When carrying protectively marked material, all items must be treated according to the highest marking.

TOP SECRET documents must only be carried by a person having a security clearance appropriate for unsupervised access to them. A receipt must be obtained each time a TOP SECRET document changes hands unless it is within an area where other measures have been specifically agreed.

J.5.2 Internal Despatch Service

When sending protectively marked documents within the CoLP via the internal despatch service the following rules apply:

RESTRICTED: Use a sealed envelope, with the protective marking shown on the envelope. Transit envelope may be used for internal mail, but the flap must be sealed with the appropriate label.

CONFIDENTIAL: Use a new sealed envelope, with the protective marking shown on the envelope then place this within another envelope with no protective marking shown. Transit envelopes must not be used for CONFIDENTIAL documents.

SECRET and TOP SECRET documents must NOT be sent via the internal despatch service.

J.5.3 Royal Mail/Courier Services

When sending any external mail a return address or ‘PO Box’ number must be shown on the reverse of the envelope.

When sending protectively marked material within Great Britain by Royal Mail or courier the following rules apply:

- RESTRICTED material may be sent by ordinary post. It must be sent in a sealed envelope with no protective marking visible (except PERSONAL, when appropriate).
- CONFIDENTIAL material must be sealed in an envelope showing the protective marking and addressed to a named individual, or specific appointment. This envelope should be sealed within a second envelope, suitably addressed and with a return address or PO Box number on the reverse, but with no indication of the protective marking.

- SECRET and TOP SECRET documents must not be sent via the Royal Mail or courier service.

More detailed rules on the movement of protectively marked material are shown in the table at appendix B.

K Data Breach and Incident Management

K.1 Definition of an Information Security Incident

An information security incident is defined as any event that has, or could have, resulted in the loss of, or damage to, or unauthorised disclosure of, any City of London Police information asset.

The Force Information Security Manager (ISO) is responsible recording, examining and making recommendations to prevent such incidents reoccurring.

Information System Owners are responsible for collating details, taking immediate appropriate action to prevent a reoccurrence, immediately reporting the incident to the Force Information Security Manager (ISO) and if relevant the Technology section. A report outlining any information security issues must be sent to the Head of Professional Standards (HoPS) and the Head of Technology (HoT) for consideration of appropriate countermeasures.

Information system assets include, but are not limited to:

- Information assets - Databases, system documentation, user manuals, business continuity plans fall back arrangements etc.
- Software assets – application software, system software
- Physical assets – computer and communication equipment, specialist equipment (power supplies, air conditioning units etc.)

A security breach could result in a variety of different consequences, which may include:

- jeopardising national security;
- frustrating the apprehension or prosecution of offenders;
- impeding the prevention or investigation of offences;
- facilitating the commission of crime;
- distress, injury or death to individuals;
- disruption of operations or other activities;

- loss, destruction or unauthorised disclosure of information;
- invasion of privacy;
- legal obligation or penalty;
- financial loss;
- damage to the reputation or integrity of the City of London Police; or
- embarrassment to the Service.

Reportable incidents under the Information Security Incident Reporting Scheme (ISIRS) include compromise or potential compromise to the confidentiality, integrity and availability of City of London Police assets, such as:

- accidental or deliberate unauthorised destruction, loss, modification or disclosure of information;
- deliberate, unauthorised or catastrophic (in terms of business impact) unavailability of systems;
- unauthorised access to information, IT, radio and telephone equipment/systems or protectively marked equipment;
- misuse or unauthorised use of information, IT, radio and telephone equipment/systems or protectively marked equipment;
- malicious damage to IT and radio equipment/systems or protectively marked equipment;
- malicious software (virus);
- theft of information (plans, files, papers, floppy disks, etc.), IT equipment or protectively marked equipment;
- any other event which affects security.

K.2 Reporting Security Incidents

Information security incidents must be immediately reported to the ISO. All malicious software (virus) incidents must also be reported to the IT Helpdesk immediately.

Where appropriate, information security incidents involving an unrecoverable fault or failure of IT equipment must be reported to the IT Helpdesk.

When a virus is detected on an information system, the information asset owner / administrator will report the infection in accordance with the relevant System Security Policy (SSP), and their own Security Operating Procedures (SyOPs). If the virus is discovered by the Technology Unit they will contact the relevant systems owner / administrator and the ISO.

All personnel must be encouraged to report any perceived information security weaknesses through their line management to the ISO.

It is not normally necessary to report one-off minor incidents, e.g. where a user has trouble keying in a password. What is a minor incident in one set of circumstances may be a major incident in another and judgement must be exercised when deciding whether a report should be made. For example, if a user accidentally switches off the power to a computer, it is unlikely to cause serious disruption to business unless the computer is used as a file server for a network. If, however, the power supply to the Command & Control system was similarly interrupted it would be likely to constitute a major incident.

Some information security incidents are handled through other mechanisms and the following provisions apply:

- Police Property & Equipment: theft and criminal damage are reported as crimes. However, the theft or damage, or unauthorised disclosure of information, of IT equipment or protectively marked equipment are additionally reportable under the ISIRS.

- Physical Security incidents: Reported to the Heads of Departments and Divisions are also reportable under the ISIRS. For example, burglary or trespass on City of London Police premises containing information assets.
- Equipment Security (Information Systems): unavailability of force systems are normally dealt with under serviceability arrangements between the information asset owner and the relevant service provider. However, deliberate or catastrophic (in terms of business impact) unavailability are additionally reportable under the ISIRS.
- Personnel Security (Warrant Cards, Civilian Support Staff Passes and other Security Passes): rules covering the loss or theft of these are detailed in Force Orders and are not therefore, reportable under the ISIRS.
- Personnel Security: corruption, dishonesty and unethical behaviour is dealt with through Police or Civil staff disciplinary procedures. However, if this is connected with the use of information system equipment such instances are additionally reportable under the ISIRS.

Unauthorised attempts to investigate any suspected security weakness could be interpreted as a disciplinary and/or criminal offence.

K.3 Incident Handling

On being notified of an information security incident the ISO will initiate incident handling procedures. These procedures ensure a uniform and consistent response to incidents by incident management, escalation where necessary and the identification of countermeasures to avoid recurrence.

The major concern during an information security incident evaluation is not to attach blame to an individual, but to improve and maintain security and to rectify any shortcoming.

The ISO will offer advice, guidance and instructions to the reporting officer who will ensure local compliance. If you breach any instructions you may be committing a serious disciplinary and/or possibly a criminal offence.

The ISO collates information from security incidents. This information forms the basis of a report for the analysis of trends, security weaknesses and appropriate countermeasures

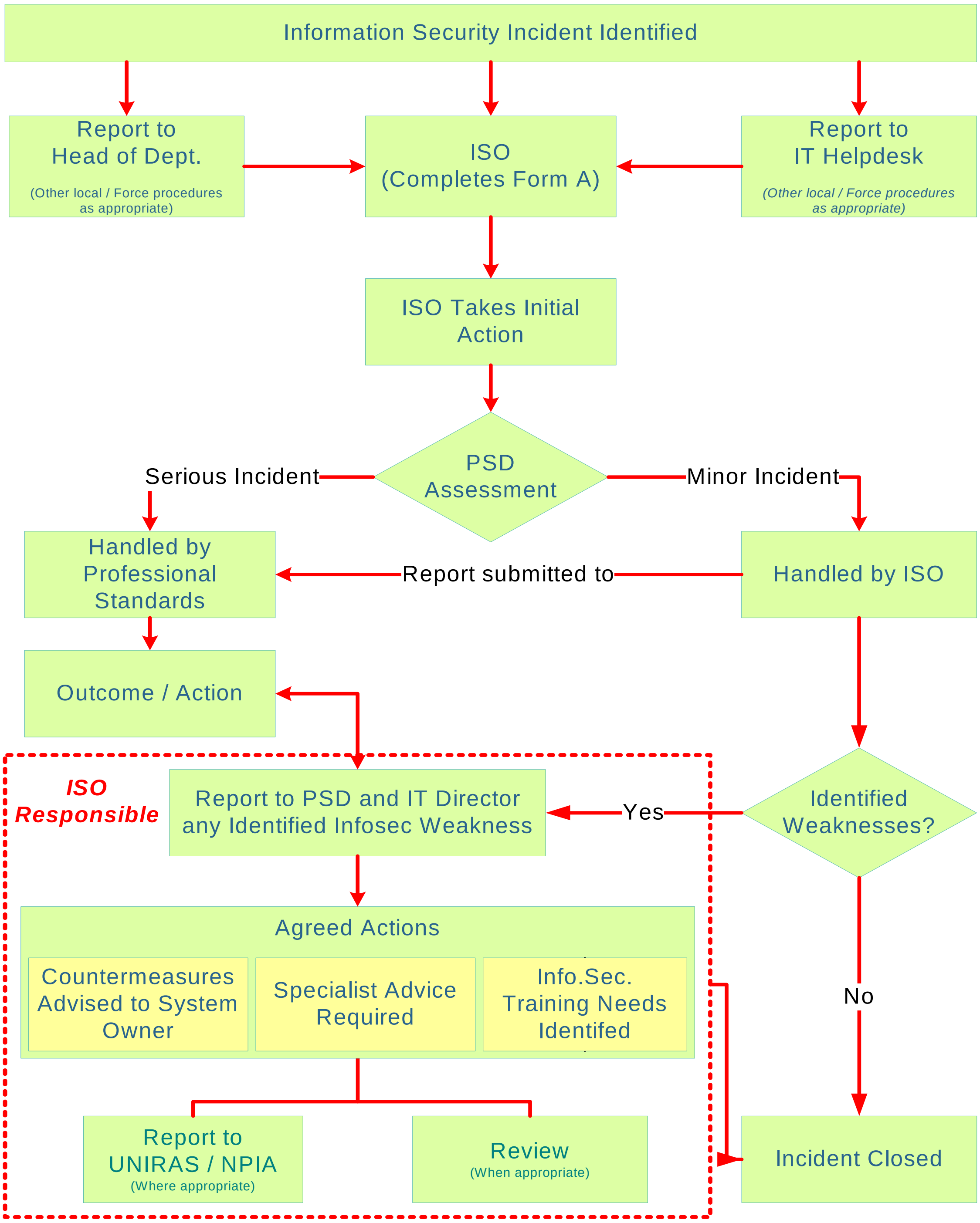
Where appropriate, if the ISO identifies training needs that have arisen as a result of an incident the ISO can offer specialist guidance to divisions and departments in dealing with this requirement.

The ISO will forward details of all relevant security incidents to the National Police Information Risk Management Team via PoLWARP for inclusion in the government's Unified Incident Reporting and Alert Scheme (UNIRAS).

The ISO receives Security Alerts and Briefing Notes from Centre for The Protection of National Infrastructure (CPNI). These are then forwarded to appropriate individuals.

In accordance with the PNC System Security Policy, Code of Connection Volume 1, the ISO shall forward details of any security incident involving PNC data to the Home Office Force Information Security Manager.

Information Security Incident Management Scheme Flowchart



Information Security Incident Identified
Report to Head of Dept.
(Other local / Force procedures as appropriate)
ISO (Completes Form A)
Report to IT Helpdesk
(Other local / Force procedures as appropriate)
ISO Takes Initial Action
PSD Assessment
Serious Incident
Minor Incident
Handled by Professional Standards
Report submitted to
Handled by ISO
Outcome / Action
ISO Responsible
Report to PSD and IT Director any Identified Infosec Weakness
Yes
Identified Weaknesses?
Agreed Actions
Countermeasures Advised to System Owner
Specialist Advice Required
Info.Sec. Training Needs Identifed
No
Report to UNIRAS / NPIA
(Where appropriate)
Review
(When appropriate)
Incident Closed

L Internet and Email

L.1 Purpose

This procedure informs all users (Police Officers, Civilian Staff, members of the Special Constabulary, contractors, staff employed on a temporary basis and delivery partners staff) of their responsibilities in using all Force e-mail and internet facilities and the procedures to be adopted to ensure that good practice is upheld thereby ensuring the confidentiality, integrity and availability of the Force's computer systems and the data held thereon, and to contribute to the efficient running of these systems and all the associated applications and other systems dependent upon them.

The Force wants to encourage the use of electronic and technological media in the conduct of its business. The Force expects you to access points of contact (e.g. e-mail Inboxes and Broadcast) during each shift, to use these facilities sensibly and act professionally as you would in the normal course of work. For example, when sending e-mail messages, you should use the same safeguards and precautions as you would when sending a fax or letter. Similarly, you should exercise proper judgement as to which Internet sites you visit.

L.1.1 Justification

Providing a direct internet connection substantially increases the chances of importing security risks onto the force network and the main security concerns are:

- The risk of importing malicious or defective software;
- The risk to the force network from external and internal hackers exploiting the connection.
- The risk of sensitive information being released onto the Internet through the actions, accidental or otherwise, of force personnel.
- The risk of sensitive information being disclosed in transit.

In addition the City of London Police has a responsibility to ensure the highest level of public confidence by developing the necessary strategies to prevent corruption, dishonesty, unprofessional and unethical behaviour and to investigate any such incidents that may be brought to attention. In particular, it is the responsibility of the Head of the Professional Standards Unit to create systems to ensure that all information and intelligence is handled, securely stored and disseminated appropriately, and ensure that the City of London Police appropriately apply the legislation governing data protection.

L.1.2 Monitoring

For the purposes of network security, efficiency and maintenance, and compliance with this procedure, the force uses a variety of automated electronic systems to monitor internet and e-mail traffic data[7]. These also provide records to support appropriate incident reporting, response, investigation and system accreditation.

The Force reserves the right to, access, retrieve, review and delete the following without notifying the individual concerned: -

- All e-mail sent, received or in the course of composition.
- Mail boxes and private directories.
- All use of the internet and all other communication techniques deployed by you using the systems; and
- Any third party screen savers, software, materials, etc. on the systems.

The force network and its applications do not provide for the sending, receiving or otherwise storing private, personal, or 'in-confidence' electronic communications. The systems have been designed and should be used for business purposes and for carrying out activities consistent with your responsibilities.

[7] "traffic data" means the data used to facilitate communications **but not** the content of that communication.

L.1.3 Compliance

It is important that you read each section that affects you or your work since you will, forthwith, be deemed to be aware of its contents in the event that there is any breach of Force policy.

This procedure must be followed at all times and it applies to all the Force's computer equipment and facilities, whether or not they are part of the Force network.

Just as with other modes of communication, in all your dealings on the Internet and through the use of e-mail, you are required to observe all legal requirements and the requirements of the APP Code of Ethics, Police Code of Conduct, Corporation Code of Conduct (stated in the Staff Handbook), Force Orders and the Force Information Security Policy.

You will be liable to disciplinary action if you abuse or misuse the systems.

L.2 General Requirements

L.2.1 Mandatory Standards

You will not engage in any activity, which is illegal, offensive or likely to have negative repercussions for the Force. Particularly, you must not access, upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- Are or might be considered to be indecent or obscene; or
- Are or might be offensive or abusive, in that its content is or can be considered to be a personal attack, rude, sexist, racist, or generally distasteful; or
- Tend to disparage or harass others; or
- Encourage or promote activities which make unproductive use of your time; or
- Encourage or promote activities which would, if conducted, be illegal or unlawful; or

- Involve business activities outside the scope of your responsibilities – for example, unauthorised selling/advertising of goods and services; or
- Might affect or have the potential to affect, the performance of, damage to or overload of the Force systems, network and/or external communications in any way; or
- Might be defamatory or incur liability on the part of the Force, or adversely impact upon the image of the Force.

Any police action or instruction which requires, or may require, supporting evidence of that action must be confirmed in writing and signed by an authorised signatory in accordance with Force Orders.

You are responsible for the security of your password(s) and any action taken under those account details issued to you[8].

L.2.2 Intellectual Property

Broadly speaking, intellectual property refers to copyright material, designs, patents, trademarks, inventions, ideas, know-how and business information. Most images, texts and materials are protected by copyright; others are protected by trademarks.

All intellectual property created in the course of employment belongs to the Force. All computer equipment, software and facilities used by you are also proprietary to the Force, including all documents, materials and e-mails created.

The downloading, possession, distribution or copying of a copyright work is an infringement of copyright unless the person is properly authorised to do so by the copyright owner.

You cannot agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of your line manager/business manager and the Head of Technological Services.

[8] The Password management information can be found in within the Access Control Standard Operating Procedure.

L.2.3 Contractual Processes

All purchases of equipment and services must be conducted in accordance with the Corporation of London Purchasing Rules.

L.2.4 Cryptography

The use of any products for the encryption or scrambling of any e-mail or other document are forbidden, unless authorised by the Head of Professional Standards after submission of a business case via the Force Information Security Manager. If so authorised you must ensure that the force Crypto-custodian is given:

- a complete and up-to-date copy of any private, public, or other decryption key, and
- all other information required for the efficient decryption of the original data.

L.2.5 Anti-Virus Precautions

You must not download any programmes, applications, binary or bitmap files. If such is required in the course of your duties contact the Technology Operations Manager who can arrange for verification of the source and virus checking of the material that is downloaded. If virus infection is suspected do not take any action but inform the Technology Help Desk (ext. 2275) immediately and notify the Force Information Security Manager (ext. 2704).

L.2.6 The Law and Electronic Communications

See Appendix C

L.3 Use of eMail

L.3.1 General

Care should be taken when using e-mail because e-mail messages are perceived to be less formal than paper based communication and there is a tendency to be lax about their content.

All expressions of fact, intention and opinion via e-mail can be held against you and/or the Force in the same way as verbal and written statements. Do not include anything in an e-mail that you cannot or are not prepared to account for. E-mails, both in hard copy and electronic form, are admissible in a court of law.

All members of the Force will be allocated a mailbox in which all mail, including external e-mail can be received. You are allocated an e-mail address for receiving external e-mail; this should only be disclosed, as necessary, in the course of your duties. It should not be used as a contact for commercial purposes i.e. Supermarket shopping, clothes shopping etc.

All email communication must be conducted though the provided force email system. The use of any other email provider, e.g. hotmail/ google mail, is expressly prohibited.

You must not falsify e-mails to make them appear to originate from someone else, nor use anonymous mailing services to conceal your identity when using e-mail services, except for approved purposes (e.g. covert operations).

Never send passwords or any other security codes by e-mail.

Do not send, or forward junk/SPAM e-mail.

Restrict messages to the appropriate recipients and **take care** when addressing e-mails.

Regularly delete messages from your Inbox and Sent Items areas.

The email system must not be used as a records management storage area and emails must be stored within the force network The system will automatically remove any messages that reach 12 months old and information will not be retrievable.

L.3.2 Additional Anti-Virus Precautions

The force employs a range of technical anti-virus measures, but the increasing number and variety of viruses being released means that these measures can never be 100% effective.

Viruses are normally contained in e-mail attachments so if a user is careful in the handling of attachments, the risks of virus infection can be reduced significantly. You are therefore expected to consider the following when opening an e-mail with attachments:

- Is this someone I normally receive attachments from?
- Was this attachment expected?
- Are they asking/tempting me to open it? (Normal business practice tells us that the sender doesn't tell you open the attachment).
- Is there something in the e-mail that doesn't seem right?

NEVER open an attachment that you are **NOT** expecting. If you are unsure contact the Force Information Security Manager immediately.

E-mail does not have to contain an attached file to trigger a virus, some are activated by simply opening the e-mail. You are therefore advised to turn off the **Inbox Preview Pane** in MS Outlook (select **View** in the menu bar then click on **Preview Pane** to remove the preview facility).

Virus warnings will only be distributed by the Information Management Department or the IT Helpdesk. If you receive any virus warnings (many are hoaxes) forward them to either of the above units for verification[9].

[9] Separate arrangements exist for UNIRAS alerts received by the Control Room.

L.3.3 Document Handling

When the content of a document is to be transmitted electronically, the document should be **attached** to an e-mail. The ‘cut and paste’ facility offered by MS Word should be avoided as it may compromise document security.

Recipients of e-mail are responsible for the security and integrity of any attachments they receive. Attachments should be saved as separate documents and then deleted from e-mail boxes.

When utilising any ‘auto forward’ facility check the conditions to be applied are secure before activating and ensure that the recipient(s) are appropriate for any mail that will be passed to them. **Auto forwarding to external email addresses is expressly prohibited**. Check with the Force ISO if unsure or for further guidance.

If you receive an e-mail and/or attachment, which contains illegal or offensive material, immediately inform a line manager and the Force Information Security Manager (ext. 2704). Do not delete or forward the e-mail/attachment.

L.3.4 Classification of Documents

E-mail containing information classified up to **RESTRICTED**[10] may be passed freely throughout the Force and Criminal Justice (CJX) networks. **CONFIDENTIAL** information may be passed within the force network if absolutely necessary, suitably password protected and with the permission of the Head of Division/Department (this does not permit the storage/processing of **CONFIDENTIAL** information on the force network).

Information classified at **RESTRICTED,** or higher, must not be transmitted over the Internet, i.e. non pnn, gsi, mod, nhs.net and cjsm addresses.

If your e-mail content is **NOT PROTECTIVELY MARKED** it may still be confidential in nature and you should ensure that the recipient is comfortable

[10] HMG Protective Marking Scheme Standard. All such references will be shown in bold capitals.

with this means of communication, be aware that other persons may have access to the recipients messages[11].

L.3.5 E-Mail and the Force Records Management System

E-mail is an effective method of written communication and is increasingly replacing the use of letters and memoranda. Wherever practical staff should place City-I identifiers (previously registry file reference) on e-mails in just the same way that they would for other forms of documentation. Emails that record organisational decision-making must be saved to the force network alongside the relevant supporting material. **The email system will automatically delete any information over 12 months old, so users are advised to apply sensible housekeeping rules to their email records.**

It is vital that gaps in force policy, knowledge and records do not appear whilst the force operates both manual and electronic administrative systems.

L.3.6 Broadcast

It is intended that the force broadcast facility should be used only for policing purposes and welfare related issues. It will not be considered appropriate for the broadcast to be used for matters of a trivial nature; classified advertising; to pass information to a small identifiable audience when a direct e-mail may be more appropriate; nor for the dissemination of sensitive or classified information. An alternative public folder, Notices, has been made available for non-operational matters to accommodate the demand for other services.

Information Management Services will monitor use of the broadcast in order to maintain standards in line with this procedure and other force policies.

L.3.7 Access to Mailboxes

In addition to the monitoring provisions of this procedure or a formal investigation, other third party access to mail boxes will be subject to permission from the Professional Standards Director upon application through

[11] The conditions of use of many commercial ISP mail services assume ownership of the information stored on them. The use of external e-mail addresses should not be obviously attributable to the force and authorised by the relevant division/department head.

the relevant Head of Division/Department. This permission will only be for operational reasons and because of the absence of the box holder. All such requests and the decisions made will be recorded.

L.3.8 Global Address List and External Addresses

The global address list is a useful tool for the dissemination and reuse of email addresses across the organisation. However, a naming convention **MUST** be followed when recording external recipients in the Global Address List. This will take the format of a prefix "EXT_" before any descriptive information is provided, therefore the email address of "Smith, Gary Gary.Smith@Example.com" will be recorded as "EXT_Smith, Gary Gary.Smith@Example.com". In addition, where an external address is included within a distribution list then this list **MUST** take the format of a prefix "EXT_" so that all users are aware of the external distribution. These steps are necessary to prevent the accidental sending of any information to an external recipient. The ICT Department are responsible for the daily management of the Global Address List and are the responsible owner of this system and its administration.

L.4 Use of the Internet

L.4.1 General

The Internet is provided for business purposes. Users are reminded that when visiting an Internet site the forces identity (IP address) may be logged; therefore any activity engaged in, undertaking given or transaction made might impact upon the force.

When entering an Internet site, always read and comply with the terms and conditions governing its use.

If you arrive unwittingly at a website that contains illegal or offensive material you must disconnect from the site immediately and inform a line supervisor and the Force Information Security Manager (ext. 2704).

Particular care should be exercised when gathering evidence from the Internet to ensure that it has been done in accordance with PACE and other relevant legislation. It must be remembered that prior to any action being taken as the result of information received from the Internet the information must be validated, so far as is possible, to ensure the reliability of the information. Access for **investigative purposes** must be undertaken on a **standalone** Internet enabled machine.

Publication of information onto the Internet must be co-ordinated by the Corporate Communication department. Personal views regarding policing matters should not be published unless previously authorised by the relevant Head of Division/Department.

The following activities are expressly prohibited:

- The introduction of packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- Seeking to gain access to restricted areas of the network;
- Using Internet based email systems, i.e. Hotmail, googlemail, etc
- Knowingly seeking to access data which you know, or ought to know, to be confidential unless authorised to do so;
- Introducing any form of computer viruses; and
- Carrying out any other hacking activities.

L.5 Personal Use

L.5.1 General

In exceptional circumstances the system and/or the facilities may be used for your own purposes, this use will be within the rules and caveats stated in this standard operating procedure. Any personal communication or Internet interaction must not be excessive in duration, size or content; users should distinguish personal e-mails from business-related e-mails by marking them as NOT PROTECTIVELY MARKED – PERSONAL or PRIVATE - in the subject line.

In addition, you will ensure that your personal use of the system does not:

- take priority over your work responsibilities;
- overload the communications system you are using;
- interfere with the performance of your duties;
- incur unwarranted expense on the Force; and
- have a negative impact upon the Force in anyway.

Personal use of email and Internet systems is not exempt from usage monitoring or auditing.

Personal use does not include onward transmission of written or picture “jokes”, personal photographs, video and audio clips – all of which, if not for business purposes, should not even be on the network.

M Physical and Environmental Security

M.1 Overview

In order to comply with elements of law, HMG and industry best practice, and mandated security frameworks such as the Criminal Justice Community Code of Connection, access to City of London Police's equipment and physical environment as well as information must be protected.

The aim of this policy is to prevent unauthorised access to both physical and electronic information. In summary, the policy requires the following to be protected:

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect City of London Police's IT data. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access, loss or other compromise. Information Asset Owners are responsible for assessing the level of protection required.

M.2 Policy Statement

The purpose of this policy is to establish standards in regard to the physical and environmental security of City of London Police's information. All City of London Police employees, partners, contractors and other users with access to City of London Police's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of City of London Police's equipment and the information that they use, store or manipulate.

M.3 Scope of the procedure

This procedure applies to all users of City of London Police's owned, leased or hired facilities and equipment. The policy defines what paper and electronic information belonging to City of London Police should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of Police information.

M.4 Secure areas

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

M.4.1 Physical security controls

Physical security controls are intended to protect the organisation and its staff, including visitors from violence and protectively marked and other valuable assets from attack by individuals or organisations that are not authorised to have access to them. Such controls often combine some degree of controlled entry through a secure perimeter, with one or more layer of other physical security controls closer to the assets. They should also take account of the security status of individuals who work or visit such areas and meet any requirement for contingency.

The areas of physical security that need to be considered include:

- Document handling - including transfer, accounting, copying and carriage;
- Buildings;
- Rooms, including strong rooms;
- Security containers;
- Locks;
- Entry and Access Control Systems;
- Guards;
- Intruder detection;
- Perimeter security - including the use of CCTV and perimeter intruder detection;
- Destruction of protectively marked waste and other valuables;

- Working on protectively marked assets away from official premises – for example, at home or when travelling and planning for:
- Accommodation moves;
- Conference security;

A balance of physical security controls is needed to meet a system's security requirement. This is likely to be struck between effective perimeter security and protection of the assets involved through, for example, the use of strong rooms and security containers. The type and mix of controls required will depend on the nature of the threats, the cost-effectiveness of the controls, the site and its surrounding environment, sole or shared occupation of the site and if public right of entry is an issue. information asset owners and their contractors are required to ensure that effective arrangements are in place for the appropriate protection of the protectively marked and other valuable assets they hold. Good security can only be achieved with the co-operation of all

M.4.2 Physical security perimeter

The security of the perimeter should be consistent with the value of the assets or services under protection. Secure areas in relation to information security; generally fall into two categories, namely sensitive and secure zones.

Sensitive zones may be defined as areas where the value or confidentiality of the information is high. For example, personnel information, financial management information and Police National Computer terminals.

Secure zones are communication and computer rooms that support business critical activities.

M.4.3 Physical entry controls

The Chief Force Information Security Manager (Director of Information) has overall responsibility for force physical security.

The minimum standards that should be applied are detailed below.

In reception areas, City of London Police staff, to control entrance. Alternatively, other responsible persons or organisations approved by the responsible person.

Entrance to all buildings must be protected by appropriate entry controls. All visitors must register their details at the Front Desk where a Visitors Pass will be issued and entry/departure times from the building of the visitor logged.

Any external staff requiring regular entry to force premises will be issued with an identity card on successful clearance from vetting. No external staff, including the Corporation of London, is to be permitted unaccompanied access to force premises.

Staffs that do not possess swipe cards must validate their identity with a member of the Front Office staff prior to entering a building and be issued with a temporary pass.

Identity cards should be displayed at all times by non- uniformed staff.

Users are to ensure that workstation monitors, printers and any output are not overlooked by unauthorised persons.

Staff passes and Warrant cards will be recovered from staff leavers in accordance with Force Orders and HR policy.

M.4.4 Securing offices, rooms and facilities

Secure or sensitive areas should be subjected to a risk analysis by the relevant information asset owner and appropriate higher levels of protection afforded.

As a minimum the following measures will apply:

- Authorised personnel only.
- Access restricted to necessity basis with visitors or contractors supervised at all times.

- Areas locked and checked out of hours,
- Support equipment (photocopiers, fax, printers, etc.) sited to minimise risk of compromise of sensitive information.
- Prevent photography or other means of recording.

Recommended confidential area measures – Include those recommended above plus entry audit facility, alarm facility, fire control system, regular cleaning by specialist personnel, environmental controls and alarms.

M.4.5 Working in secure areas

Personnel working in secure or sensitive areas must exercise greater vigilance. Any security incidents or weaknesses must be reported immediately to a line manager.

M.4.6 Isolated delivery and loading areas

Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access or compromise.

M.5 Equipment security

M.5.1 Equipment siting and protection, Power supplies, Cabling security, Equipment maintenance

Any defective or redundant hardware should be disposed of in accordance with the current advice received from the Force Information Security Manager.

Apart from the exchange of specific parts, hardware should not be altered, modified, added or removed without the authorisation of the relevant information asset owner.

No remote diagnostic links are to be installed without the permission of the Information Technology Director and the Force Information Security Manager. Any connections must comply with HMG standards.

Any defective equipment should be suitably isolated from the system before any maintenance work can proceed.

Equipment should be sited or protected to reduce the risks of damage, interference and unauthorised access.

Equipment should be protected from power failure or other electrical anomalies.

Equipment should be adequately maintained and each piece of equipment should have a maintenance record. Maintenance should be carried out in accordance with the manufacturer's instructions. This will ensure continued availability and integrity.

Power and telecommunication cabling should be protected from interception or damage.

Portable IT systems (laptops etc.) used on the force network must not be linked to any other IT system or network without prior approval of the Force Information Security Manager.

M.6 Security of equipment off-premise

M.6.1 General

Information systems equipment may only be removed with the express permission of the relevant information asset owner. No information systems equipment may be used for unauthorised or private purposes. Private equipment may not be used for City of London Police business, unless authorised by the information owner and such use is in accordance with the requirements of the Force Information Security Policy. Thereafter the authorised person will be responsible for ensuring any necessary security controls are implemented and maintained. For example, Force laptops may not be used for personal affairs such as games or home finance. And personal home computers may not be used to perform force tasks, such as the preparation of files, unless authorised. To gain authorisation a member of staff may have to implement physical and technical security requirements at their own expense.

IT equipment may only be removed from the Force local secure environment in accordance with the security guidelines, and all equipment used for such information processing will be subject to regular recall and audit.

N Protective Monitoring

N.1 Aims and Objectives

The City of London Police, by virtue of Section 6, Human Rights Act 1998, is a public authority and is required to act in a manner that is compatible with the rights outlined in the Convention.

The Regulation of Investigatory Powers Act 2000 (RIPA) enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept or monitor communications for the purposes of carrying on a business. These regulations apply equally to public authorities.

Various legislation and codes of practice including the Data Protection Act 1998, ISO 27001/2 Information Security Management Systems and ACPO Community Security Policy impose a positive duty on the Force to protect its information assets and provide the assurances that appropriate controls are in place.

The monitoring of staff activity is an established concept which includes the routine supervision of performance and staff behaviour. RIPA extends the principle of supervision to the use by staff of communications equipment provided by the organisation for business purposes.

The procedure applies to City of London Police Officers, Police Staff, Partners, agents and approved persons working for or with the Police

Protective Monitoring is a lawful and ethical tool used to assist the Force in the protection of its staff, information and to assist in the investigation of misconduct or criminal activity. Auditing systems monitor and record all computer based actions conducted using any City of London Police computer equipment.

This procedure defines the monitoring and auditing of staff activity as a means of ensuring all staff comply with Force policy and procedures and with the standards of behavior expected by the City of London Police.

This procedure does not over-ride any existing policies or negate any existing guidance regarding information security, data protection or acceptable use. It is intended that it will supplement such policies but with a specific focus on the protective monitoring of the force computer network and access to the data held within or transported by it.

Main aims and objectives are:

- To ensure the data integrity of the information held by the City of London Police and enhance operational security of criminal investigations. This will be achieved by way of a single force-wide network based facility that will audit computer and peripheral device usage independent of any specific application. The system will ensure that City of London Police complies with the ACPO Community Security Policy (CSP) requirement to carry out "Protective Monitoring".
- To identify misuse, monitor exceptional usage and support intelligence led investigations. All users of City of London Police LAN accounts must note that the monitoring system will include any personal use staff make of Force equipment, even if undertaken in their own time and with Management agreement. Standard use of all City of London Police systems and information is identified to all users as for 'Business Use Only'.
- To provide a forensic capability to the auditing process to ensure its evidential credibility.
- To protect the Force by providing the Counter-Corruption Unit (CCU) with the means by which they can effectively seek out those who abuse their position within the force for personal gain or benefit of others.
- To instil within the communities of City of London the confidence that those employed by City of London Police maintain the highest levels of honesty and integrity by enforcing the relevant Codes of Conduct in relation to unethical behaviour or gross misconduct.
- To protect the information and intelligence assets of the Force from malicious or accidental disclosure.

N.2 Definitions

Protective Monitoring – The term given to an auditing capability that is network based as opposed to being application specific.

Application – Refers to the software installed on force computers/servers, virtual or otherwise, that will facilitate the logging of actions conducted by the user logged on to a specific terminal or access point.

Console – The administrative and querying interface of the application used to interrogate and manage the system.

Intercept – The "live" monitoring of communications which may involve recording of any activity witnessed.

Monitor – The review of "historic" data recorded and stored within the auditing database.

Communications Equipment – Any equipment that facilitates the creation, transmission or receipt of data provided by the Force and intended for the business use of the City of London Police.

N.3 Administration

The Protective Monitoring data will be stored and controlled in accordance with the controls commensurate with a RESTRICTED system.

The auditing systems will be administered by nominated MV/SC vetted staff.

Routine reviews of the audit data will be conducted to ensure compliance with relevant legislation.

N.4 Access

Data stored within the Protective Monitoring system will only be accessible to suitably trained members of CCU; access to pre-defined Management Information reports will be available to other Professional Standards staff members as appropriate.

Requests for quantitative/system data must be submitted to the DCI - CCU and each case will be considered on its own merits. Such requests must be made with the authorisation of an officer of the rank of Chief Inspector or above or police staff equivalent.

No personal data will be disseminated outside the department without the explicit instructions of the Department head.

N.5 Security

Data stored within the database is afforded the physical and protective security measures required for RESTRICTED material.

Passwords entered by force network users are not exposed to audit and remain known only to the user.

All system users and administrators are audited including those with access to the software terminal console.

N.6 Publication / System Warnings

A suitably worded logon script is shown at the point each individual user logs onto a force computer. The text explains in plain language that access to the force network is for authorised users only and is monitored. Users are advised that they should have no expectation of privacy if they choose to use the Force computers for personal use. They are also reminded that personal use must be only be conducted following recorded agreement with Line Management.

Attempts to disable/prevent installation or otherwise deliberately interfere with the functionality of auditing software will be considered a misconduct matter and investigated appropriately. Interference with the system may also constitute an offence under the Computer Misuse Act 1990 and would be treated as a criminal matter.

Information generated by the Protective Monitoring audit systems may be used as grounds for further enquiries and form the basis for further investigation.

The results of audit log interrogation may be used as evidence in misconduct and criminal proceedings.

N.7 Data Protection

The Data Protection Act 1998 provides for the regulation of the processing of information relating to individuals, including the obtaining, holding, use and disclosure of such information.

Any information relating to an individual or their actions generated by the audit system will be subject to relevant legislation and protected accordingly.

It is the responsibility of the system owner to ensure that all aspects of the Data Protection Act are complied with.

The requirements for data review, retention and disposal will be applied in accordance with the provisions of the Data Protection Act 1998 and the Management of Police Information (MoPI) Codes of Practice 2010.

O Remote Access to Force Systems

O.1 Overview

The purpose of this procedure is to detail the standards for connecting to the CoLP network from devices that are outside the network perimeter. These standards are designed to minimise the potential exposure of CoLP from damage that may result from unauthorised access to their information assets, or computing resources. Potential damages include the loss of confidentiality, integrity or availability of force confidential data or intellectual property, damage to public image, or damage to CoLP internal systems.

CoLP will comply with CESG Infosec Memo 35 – Remote Access to Public Sector IT Systems. This Remote Access procedure is intended to provide specific information relating to CoLP use of remote access.

O.2 Objectives

The objectives of this SOP are to:

- Protect the systems and infrastructure of the CoLP network, and the information held thereon from damage, degradation or unauthorised access;
- Protect CoLP information from risks that could arise from remote access;
- Meet the requirements of all applicable legislation.

O.2.1 Security Principles

The connection by remote access of any device, by any individual, is subject to the same policies, standards and controls that are applied for access within the CoLP network.

- Before remote access is granted, it must be confirmed that there is a valid operational or business reason for that access.
- Remote access facilities will only be available for the purpose and duration for which they are granted. In the event that the requirement for any individual changes, the change will be subject to the approval process.

- Access may only be permitted from approved known devices, in the possession of known individuals who have been vetted to a level that is appropriate for the sensitivity of the information to which they will have access.
- Strong authentication will be used to avoid the risk of unauthorised remote access. This authentication will comply with the current Unified Police Secure Architecture.
- Encryption will be used to protect information in transit across communications links.
- All accesses will be recorded and proactively monitored, and the activities performed will be logged. The logs will be reviewed regularly, and any suspicious activity will be investigated.
- All devices that are approved for remote connection to the CoLP network will be free of unauthorised code, such as viruses, and will be configured to ensure that they remain so.

O.3 Scope of this Procedure

This policy applies to all users of City of London Police facilities and equipment including staff and any third party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

O.4 Responsibilities

O.4.1 Users of remote access facilities

Employees of CoLP or its agents must ensure that their remote access connection is given the same consideration as their on-site connection to the network.

Users will not connect any system to the CoLP network without prior approval of its configuration by the CoLP Technology Unit.

Users will ensure that all systems that connect to the CoLP network use the most up-to-date version of anti-virus software and virus definitions.

Employees of third parties, including service organisations must comply with the CoLP Security Policies, and with the Third Party Connection Agreement (Appendix E).

Employees of other organizations, forces or agencies are expected to comply with the Force Information Security Policy and be explicitly identified within relevant procedural document and/or contract.

Users must not reconfigure systems that have been set up or approved by the CoLP Technology Unit without direct instructions from the Technology Unit.

Users must not divulge their password to anyone and will take care to ensure that others do not overlook the access process. If they suspect that their password is known to anyone else, they will change it immediately, and if they suspect that someone else has used their password, they will change it immediately and report it using the CoLP Incident Reporting and Management Procedure.

Users will not share any material or token for authenticating remote access.

Users will only use the connection to perform the activities for which the access was approved.

Printouts may only be produced remotely by exception and requires a detailed business case, approved by the SIRO. This is due to the normal lack of assurance of remote locations where the material is to be produced.

Users must ensure that systems in non-secure areas are not left unattended while logged on, and are logged off and disconnected from the CoLP network at the end of the session.

O.4.2 Managers

Managers are responsible for requesting remote access for their users. This involves the following activities:

- Define the business case.

- Ensure that the individual has been appropriately vetted for the access required.
- Where applicable, ensure that a Third Party Access Agreement is in place and all appropriate checks are made prior to requesting approval from the Information Management Board.
- Identify the specific activities required for remote access – these may not be as comprehensive as those required within the network, and special consideration should be given to the sensitivity of the information to be accessed, the location from which it will be accessed and the Impact Level.
- Arrange, and obtain approval for loan equipment if required.
- Periodically (at least 6 monthly) review the requirements for remote access.
- Advise the Technology Unit when the requirement for remote access no longer exists.
- Ensure that the individuals are fully aware of their responsibilities.

O.4.3 Technology Unit

The technology unit are responsible for ensuring compliance with technical aspects of this policy by:

- Securely configuring loan equipment in accordance with the document entitled “Security Conditions to be met before working outside of CoLP premises with a CoLP computer system” before and after use.
- Issuing tokens and administering the RSA Secure-ID token system.
- Reporting security incidents, whether actual, suspected or potential to the Force Information Security Manager.
- Keeping asset records for loan equipment.
- Reviewing access and event logs.

O.4.4 Information Management

Information Management are responsible for providing assurance to the SIRO in respect of appropriate security measures and will be responsible for:

- Ensuring that remote access to CoLP I.T systems complies with CESG Memo 35 and HMG Infosec Standard No 4.
- Providing advice to remote access users on the security requirements of their own systems.
- Periodically (at least 6 monthly) review access logs and inspect all connections to the RESTRICTED Network.
- Overseeing and assisting with the risk assessment on users, communications methods and locations based upon the Impact Level of the information to be accessed.

O.5 Monitoring and Inspection

O.5.1 Monitoring

All external connections to the CoLP network will be logged, and the user, location and times of access recorded. All access to CoLP systems will also be logged.

These logs will be reviewed. If any unauthorised access is identified the CoLP will remove access from the individual(s) concerned.

O.5.2 Inspection

The CoLP will inspect the security arrangements of those with external access on a regular basis, and reserves the right to conduct such inspections without warning. The purpose of any inspection will be to ensure that the requirements of this SOP are being met.

O.6 Security of Third Party Access

O.6.1 General

Access by third parties poses a risk to City of London Police information systems. Before any connection is undertaken the information asset owner will conduct an analysis of the risks. Appropriate security controls will be adopted. Any connection must be subject to a contract, which must specify the security requirements. No connection may be made without the express permission of the Information Technology Director and the Chief Information Security Officer.

O.6.2 Outsourcing

Outsourcing the management or control of information systems poses a risk to the City of London Police. Before any outsourcing is undertaken the information asset owner will conduct a risk analysis. Any risk must be managed to ensure the confidentiality, integrity and availability of information. Any outsourcing must be subject to a contract, which must specify the security requirements. No outsourcing may be made without the express permission of the Information Management Board.

For information asset owners managing protectively marked assets, security is the central issue in any procurement or outsourcing project. It is recognised that, at the outset, the detail of the security requirement may not be known. However, strategic requirements for CONFIDENTIALITY, INTEGRITY and AVAILABILITY should be specified in the invitation to tender and the award of contract must be subject to assurance that the contractor is capable of meeting detailed security requirements.

O.6.3 Legal Compliance

General

Arrangements involving third party access force IT facilities, information, or personal data should be based upon a formal contract containing, or referring to, all of the necessary security conditions to ensure compliance with this procedure. This contract should be in place before the access is provided.

Data Protection Act

The Data Protection Act 1998 requires that where the processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle:

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- take reasonable steps to ensure compliance with those measures.

Where the processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless:

- the processing is carried out under a contract:
- Which is made and evidenced in writing; and
- under which the data processor is to act only on instructions from the data controller.
- the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

The most common situations involving the handling of such assets by individuals and organisations outside the force are:

- Contractors working on force premises
- Contractors working on their own premises
- Consultants

P Business Continuity

P.1 Overview

The City of London Police has a legal responsibility under the Civil Contingencies Act 2004 to deliver their core functions to the community as a whole.

Information Technology services are paramount in supporting the provision of key departments and sections. It is vital that information asset owners build resilience into the provision of their system(s) to support the force.

P.1.1 Aspects of business continuity management process

A managed process should be developed and maintained, including identifying sufficient financial, organizational, technical and environmental resources for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.

Information asset owners must ensure that contingency plans are in place to cover the continuity of essential business operations and services. These include but are not limited to IT services. Plans should be exercised regularly.

Contingency Planning involves identifying the most likely failures and defining effective plans of response should those failures occur. Where appropriate, plans should address not just long-term recovery from failure, but also interim measures to assure a minimum level of service while recovery is in progress.

Contingency Plans should cover such issues as (but not limited to):

- system failure
- network and telecommunications failure
- effects of fire and flood
- effects of terrorist attack, and
- recovery procedures.

P.1.2 Business continuity management process

Plans covering procedures to follow in the event of a contingency are laid out in the Force IT Contingency Plan. The plan provides an alternative means of continuing processing in the event of any damage to or failure of the force network. Owners of other systems should adopt similar procedures.

A formal method of change control is needed to ensure that the implications of change are identified and disseminated prior to updating and redistribution of the Plan.

P.1.3 Business continuity and impact analysis

Information management continuity plans will be based on an appropriate risk analysis and shall be consistent with the force's overall approach to business continuity, as defined within the Business Continuity Policy.

P.1.4 Writing and implementing continuity plans

The relevant information asset owner will develop plans to restore business operations following interruption to, or failure of, critical business processes. Consideration must be given to all aspects of the restoration process not merely the IT services.

P.1.5 Business continuity planning framework

Emergency procedures to address major incidents or interruptions to Force core functions and critical activities are contained within the Force Business Continuity and Emergency Plans and associated Force IT contingency plan. City of London Police information asset owners must develop procedures consistent with established frameworks. The plans shall also identify priorities for regular testing and maintenance. Responsibilities will be clearly identified and agreed.

P.1.6 Testing, maintaining and re-assessing business continuity plans

The relevant information asset owner is responsible for identifying and applying changes to the plan. The need for individual changes should be reviewed at least annually. This process should be reinforced by a brief annual review of the complete plan.

Q Human Resources Requirements for Information Security

Q.1 Overview

City of London Police holds large amounts of personal and confidential information. It has a variety of statutory, regulatory and internal obligations to process this information in a way that assures its confidentiality, quality and availability at all times. Security cannot be achieved by technical means alone. It must be supported by effective processes and people. This procedure addresses security issues related to people.

Q.2 Procedure Statement

City of London Police understands that to reduce the risk of loss, theft, fraud, inappropriate or criminal use of its information systems, anyone that is given access to Police information systems must be fully identified to national standards, and be suitable for their roles. They must fully understand their responsibilities for ensuring the security of the information, and that they must only have access to the information they need, and that this access must be removed as soon as it is no longer required.

Access to Police information systems will not be permitted until the requirements of this policy have been met.

Q.3 Scope of the Procedure

This procedure applies to any person that requires access to City of London Police information systems of any type or format (paper or electronic).

The policy applies to all Police employees through their contract of employment and its enforcement is the responsibility of HR and Departmental managers.

Where access is to be granted to any third party (eg temporary staff, contractors, service providers, voluntary agencies, partners etc) compliance with this procedure must be ensured. Responsibility lies with the City of

London Police sponsor that initiates this third party access, in co-ordination with HR.

This procedure addresses 3 key stages of a user's access:

1. **Joiners**: Prior to granting access
   National ACPO identification and vetting checks must be made to ensure that the individual is suitable for access to Police and other criminal justice information systems. The manager is responsible for co-ordinating system access requirements with HR, based on the user's job role.
2. **Movers**: Period during access

   Users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure that it remains appropriate. The current manager is responsible for co-ordinating system access with HR, based on the user's job role.
3. **Leavers**: Termination of access

   Where the user's requirement for access ends and needs to be removed in a controlled manner.

This procedure also addresses third party access to City of London Police information systems (eg temporary staff, contractors, service providers, Local Authorities, Quangos, voluntary agencies and other Criminal Justice partners).

R Secure Disposal of Assets

R.1 Purpose

The purpose of this procedure is to establish and define standards, methods, and restrictions for the disposal of CoLP IT equipment in a legal, cost-effective manner. City of London Police's obsolete IT assets resources (i.e. desktop computers, laptops, notebooks, printers and servers) must be discarded according to legal requirements and environmental regulations. Therefore, all disposal procedures for retired IT assets (legacy) must adhere to this procedure

R.2 Scope

This procedure applies to the proper disposal of City of London Police IT hardware, including PCs, laptops, notebooks, printers and servers. City of London Police obsolete machines (legacy), and any equipment beyond reasonable repair or reuse are covered by this procedure. All COLP departments are included in this procedure. Leased equipment must also be cleansed before being returned to the leaser.

R.3 Definitions

- "Non-leased" refers to any and all IT assets that are the sole property of City of London Police
- CoLP Owned; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.
- "Disposal" refers to the removing of the asset from operating use with the intent of retiring the asset according to the surplus property disposal policy.
- "Obsolete" refers to any and all equipment that no longer meets requisite functionality.
- "Surplus" refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

- “Beyond reasonable repair” refers to any and all equipment whose condition requires fixing or refurbishing if the cost is equal to or more than total replacement.

R.4 Secure purchase, maintenance, disposal or re-use of equipment

This procedure describes the high level guidance for when information system equipment containing City of London Police information is being disposed of, reallocated within the City of London Police, or removed from a City of London Police site for maintenance or repair. Specific instructions can be obtained from the Force Information Security Manager or Information Technology Department.

When information system equipment becomes surplus to requirement, care must be taken to ensure that its disposal does not expose any City of London Police data that it has processed or stored to an unacceptable risk of compromise. Of primary concern are data bearing components of the equipment, e.g. disks (fixed and removable).

Disposal of equipment by reallocation or sale requires deletion of sensitive material. If the information is actually held on fixed disks, these components must either be removed or be subjected to an approved process whereby the data resident on these devices is obliterated.

R.4.1 Software

Most software, be it end-user, package or system software, is widely available but if not obtained through the normal procurement channels it may be illegal and unsupported. The Force Information Security Manager will provide details of suitable software for the removal of data from force systems.

Software acquired or used illegally renders both the force and individuals open to criminal charges. Software from an unaccredited source, such as a bulletin board or the Internet, may be illegal and is more likely to be of poor quality or malicious (e.g. it may include a virus, covert channel or Trojan code). Because end-user software is easily acquired and relatively inexpensive, it is more likely to be chosen without proper consideration of its fitness for purpose or its future support and maintenance.

The disposal of software, once it has ceased to be of operational use, may well just involve straight deletion. However in some cases there may be additional contractual obligations to be fulfilled, raising the possibility of a supplier gaining access to proprietary information, either from data originally needed for support purposes or from any returned or reclaimed software. Also the support by a supplier may be reduced during the notice period and external links (for diagnostic purposes) being left connected to the supplier.

Most software cannot be re-sold, under the terms of its licence. Therefore care must be taken to ensure that executable code is not left on any device that is disposed of from the Force.

Consideration also needs to be given to any data that is to be kept. These may need to be converted to another format before they can be used with any new or replacement software, or it may be necessary to retain the software itself until there is no further business need to access the data.

R.4.2 Hardware

The main risks when acquiring hardware are that the equipment may not be properly installed and maintained, may not be sufficiently powerful and reliable for the task and viruses can also be introduced with new hardware. The more critical the system and the more confidential the data stored on the hardware, the greater the risk.

Hardware (e.g. disk drives and memory modules) and consumables (e.g. diskettes and CD ROM’s) are discarded because they are damaged, cannot be reused, or have become redundant. With the disposal of hardware and consumables, other than the danger of inadvertent reuse of damaged equipment, the main risk lies with the information and data, which may have been stored on these media. With the appropriate technology most media, even when damaged, can be read.

Equipment needs to be correctly maintained to ensure its continued availability and integrity. The Force, via the City of London Corporation, has a comprehensive maintenance agreement, and insurance for all hardware recorded in the Force asset register. Hardware purchased in accordance with this order will be covered by these existing arrangements.

All hardware must be disposed of in accordance with the Law and Corporate procedures.

All purchasing, maintenance and disposal of IT software, hardware and removable media used for the processing of force data, will be in accordance with this procedure. Any current contractual agreements for such services, which are contrary to the requirements of this procedure, may be continued until the expiry of such, but they must be registered with the Information Technology department. Thereafter this procedure must be complied with.

R.5 Procedure

There are two scenarios that must be considered for disposal.

R.5.1 CoLP owned asset disposal

The current method for the disposal of assets is to physically destroy the device via an IS5 out sourced provider. This is a zero cost solution managed by the Security Team within Information Management Services.

In every instance the Data Cleansing Form (Appendix D) must be completed.

For each computer to be taken out of service, the hard disk drive component will be removed by a qualified IT technician and then transferred to the Security Team within Information Management Services who manage the onward disposal with an IS5 approved company**.** The computer chassis will then be disposed of via the Corporation of London equipment disposal provider, at this time Maxi-tech

R.5.2 Leased asset disposal

Any equipment that is leased remains the property of the lease company and is not therefore subject to physical disposal, unless explicitly agreed with the lease company.

Before returning any leased equipment capable of holding data all of the data stored must be removed from storage area.

The IT department is responsible for sourcing appropriate technical software to cleanse devices to the necessary IS5 standard.

The cleansing technician (IT staff member) is responsible for ensuring any CoLP data, on a device to be returned is properly backed-up and that it is so noted on the Data Cleansing Audit Form, found in **Appendix D**.

Upon completion of the cleaning and sanitizing, the IT technician will complete and sign the Data Cleansing Audit Form, see Appendix D, and submit it to the Force Information Security Manager for future audit purposes. The device can then be returned to the owning company.

S Security Standards for Acquisition, Development and Maintenance of Information Systems

S.1 Security requirements of systems

S.1.1 General

All security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

S.1.2 Security requirements analysis and specification

A risk analysis should be carried out to determine the security threats and vulnerabilities of any new systems, or enhancements to an existing system. All systems processing protectively marked information must undergo a technical risk assessment to HMG Infosec 1 Standard. The Information Security Officer can provide the necessary guidance on this standard. Risk assessment is to be commensurate with the force approach to risk assessment.

Any business requirement must specify the security controls required to safeguard the confidentiality, integrity and availability of the information contained within the system.

To achieve this, consideration should be given to access controls, privileges, audit and accounting controls, disaster recovery and statutory requirements.

Data protection standards must be maintained.

Security measures must take into account the physical, operational and technical operating environment.

S.2 Security in application systems

S.2.1 General

Relevant system owners shall validate data input into application systems to ensure that it is correct and appropriate.

Relevant system owners will issue instructions to specify the detailed execution of each task. These instructions will include procedure for correct data handling and entry, error handling, help facilities, handling and secure disposal of output, restart and recovery, correct start-up and close down, back-up, hand-over, security of system documentation, and keeping of logs. Relevant system owners must establish procedures to respond to validation errors.

These procedures must be reviewed annually.

Users must enter and handle data accurately, appropriately and correctly. Failure to do so may lead to disciplinary action.

S.2.2 Input data validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

The following should be checked to detect errors:

- Out of range values.
- Invalid characters in data fields.
- Missing or incomplete data.
- Exceeding upper or lower data volume limits.
- Unauthorised or inconsistent control data.

These checks should be documented and available for inspection.

Automatic examination and validation of input data can be considered, where applicable, to reduce the risk of errors and to prevent standard attacks including buffer overflow and code injection.

S.2.3 Control of internal processing

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. These checks may be manual or automated. These checks should be documented and available for inspection.

S.2.4 Message authentication

Consideration should be given to message authentication where there is a security requirement to protect the integrity of the message content.

S.2.5 Output data validation

Relevant system owners should conduct validation checks to ensure that data output from stored information is correct. These checks should be documented and available for inspection.

S.3 Cryptographic Controls

S.3.1 Policy on the use of cryptographic controls

A risk analysis should be carried out to determine if encryption is appropriate. The subsequent risk assessment should identify the level of protection required.

S.3.2 Encryption

Relevant system owners will ensure that critical or sensitive information is protected by encryption during transmission or storage. Appropriate, encryption of information can reduce its attractiveness if the attacker is unable to break the encryption. On the other hand, encrypting information can highlight the fact that it is important thus making it more attractive. It is therefore vital to use the appropriate grade of encryption where it is used at all.

Many forms of encryption involve the setting-up of encryption devices ('crypto equipment') with keying material - paper tape, swipe cards etc. These consumables are collectively referred to as 'crypto material'. Just like physical keys, crypto material needs to be kept under close control. For detailed guidance on the handling and operation of crypto material contact the Force Crypto-Custodian or Force Information Security Officer.

The Information Technology Director, Force Crypto-Custodian and the Force Information Security Officer must approve all cryptosystems before being used for protection of protectively marked information.

Any proposed modification to crypto equipment must be approved through the Force Crypto-Custodian. Changes to commercial equipment will require re-evaluation and re-certification.

S.3.3 Appropriate grades of encryption

The grade of encryption used must assure adequate resistance to attacks. The highest grade of cryptographic protection is designed to resist the severest attacks for many years. Lower grades of encryption protect against lesser attacks for shorter periods.

Approved cryptography within the UK is divided into three grades known since 1996 as High, Enhanced and Baseline Grade.

S.3.4 Digital signatures

A digital signature is a technique that creates a unique and unforgettable identifier for the sender of a message. The digital signature can be checked by the recipient to verify authenticity, a guarantee of the INTEGRITY of the signed message and provides for non-repudiation. Such a signature is only open to forgery if the private key becomes compromised. Within a public key architecture, certificates are used to verify that public keys belong to named individuals and offer a safeguard against the use of false keys for masquerading purposes.

Consideration should be given to the application of digital signatures to protect the authenticity and integrity of electronic information.

S.3.5 Non-repudiation services

Non-repudiation is a process, which offers evidence that a message or transaction originated by an individual or entity was in fact originated by that individual or entity, or that a recipient of a message in fact received it. It thus frustrates attempts by originators or recipients to deny their involvement. This is particularly important in electronic commerce and any electronic transactions creating legal obligations, for example, contracts.

S.3.6 Authentication

Authentication is a process, which verifies the claimed identity of an originator, recipient or other entity. For example, it can be used to provide assurance that an order or other message transmitted electronically is genuine, or as an aspect of access control to sensitive data. Public Key Cryptography techniques, which provide security features without needing a secure distribution network for large user communities, are good illustrations of the value of authentication. Any user can encrypt using a public key, but only the holder of a private key can decrypt, and vice versa. This sort of authentication system depends on the owners of private keys being the only individuals who have access to their private keys, and mechanisms are often incorporated to verify the authenticity of the various keys that match them to the individuals.

S.3.7 Key certification

Under a public key architecture, it is necessary for the public key and its owner's identity to be encapsulated in a certificate, which is digitally signed by an approved certification authority. The certification authority guarantees the correctness of the information. Secure e-mail and Secure Electronic

Transaction (SET) protocols are examples of the sorts of applications which public key certification can underpin.

S.3.8 Time stamping

Time stamping is a means of allowing users to determine exactly when a document was last modified or created; in effect, a parallel service to authorship guarantees, that have been secured via use of digital signatures.

A digital signature mechanism can be used to provide a means of authenticating the originator of the data.

HMG recommends the use of the Digital Signature Algorithm (DSA).

The use of DSA will only provide assurance to the user if appropriate access controls have been applied to the system(s) they reside on.

The establishment of a non-repudiation mechanism must be the subject of an agreement between the data originator and recipient.

On an internal system where encryption is not required for CONFIDENTIALITY, but privacy is an issue, approved baseline grade cryptography may be used for data separation. The use of non-approved commercial software is not recommended for data separation, as it does not provide any level of assurance.

Consideration should be given to the use of non-repudiation services to resolve disputes about the occurrence or non-occurrence of events or actions.

S.3.9 Protection of crypto material (Key management)

Crypto Key material, may itself, be unencrypted or may itself be protected by encryption. The unencrypted form is obviously more vulnerable. The basic principle governing the protective marking of unencrypted keying material is that it must be given a marking equivalent to the information it is to protect. When filled or keyed, crypto equipment must be handled in accordance with the greater of its own protective marking or the protective marking of the keying material it contains.

Crypto material is to be secured according to its protective marking and in a way that allows access only by appropriately vetted and crypto authorised personnel. An additional marking - CRYPTO - indicates the need to limit access and apply extra controls.

Keying material for systems using Public Key Cryptography (PKC) techniques, such as BRENT, may not have a protective marking, but should be handled as valuable and accountable items.

Crypto equipment must be protected from unauthorised access to prevent loss and any possibility of tampering that might render the system inoperable or insecure. Access to operational crypto-equipment, and keyed equipment in particular, must be limited to employees:

Cleared to the level of the protective marking of the keying material in use and with an operational need to be in the vicinity of the equipment.

S.3.10 Disposal and destruction of cryptoequipment

CESG (Communications-Electronics Security Group, the Information Security arm of the Government Communications Headquarters) are the authority for the disposal and destruction of cryptoequipment.

S.4 Security of system files

Relevant system owners will ensure that IT projects and support activities are conducted in a secure manner.

S.4.1 Control of operational software

Relevant system owners will exercise strict control over the implementation of software on operational systems. Updates to operational software will be documented. Previous versions will be retained as a fallback.

S.4.2 Protection of system test data

Relevant system owners will protect and control test data in the same manner as operational data. Access must be restricted to persons who need the data to perform their function. Records of access will be maintained. Where possible test data should be de-personalised. The provisions of the Data Protection Act must be adhered to with regard to personal data on a test system. An audit trail must be maintained to monitor the use of live data on any test system. Live data on a test system must be destroyed when no longer required. Great care must be exercised to ensure that operational and test data are kept separate.

S.4.3 Access control to program source library

Relevant system owners will exercise strict control over access to program source libraries. All access will be authorised and documented.

S.5 Security in development and support processes

S.5.1 General

Relevant system owners will maintain the security of application system software and information.

Relevant system owners will ensure that the implementation of changes is strictly controlled. Formal change control procedures must be adopted to minimise the corruption of information systems. These procedures must be fully documented and include authorisation procedures, a review of the security implications, implementation of appropriate additional controls and audit logging of all actions taken to implement changes to applications.

S.5.2 Technical review of operating system changes

When change occurs relevant system owners must ensure that applications are reviewed and tested for security impacts. Testing and review will ensure that there is no way of bypassing security functions or provide means of obtaining unauthorised access.

S.5.3 Restriction on changes to software packages

Only software that is entered on the Approved Software Register, managed by the IT department, will be used. The installation of unauthorised software is prohibited. Software must not be modified without the consent of the owner of the software. Before any changes are made to software the risk to security must be assessed.

S.5.4 Covert channel and Trojan code

Covert channels or Trojan code (unauthorised functions allowing unauthorised access) are a risk to information security. All software shall be checked for such threats, prior to installation.

Prevention of unauthorised network access, as well as policies and procedures to discourage misuse of information services by personnel, will help to protect against covert channels.

S.5.5 Outsourced software development

Any external development work shall be subject of a risk analysis and appropriate security controls adopted to protect the confidentiality, integrity and availability of Force information.

S.6 Technical Vulnerability Management

S.6.1 Control of technical vulnerabilities

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities.

An effective management process for technical vulnerabilities should consider:

- The organisation should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;
- Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on a asset inventory list); these information resources should be updated based on changes in the inventory, or when other new or useful resources are founded;
- A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;
- Once a potential vulnerability has been identified, the organisation should identify the associated risks and the actions to be taken; such action could involve the patching of vulnerable systems and/or applying other controls;
- Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures;
- If a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);
- Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:
- turning off services or capabilities related to the vulnerability

- adapting or adding access controls, e.g. firewalls, at network borders;
- increased monitoring to detect or prevent actual attacks;
- raising awareness of the vulnerability;
- an audit log should be kept for all procedures undertaken;
- the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;
- systems at high risk should be addressed first.

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures.

~ APPENDICES ~

A The Secure Use of Passwords

Introduction

1. Proper access control is an essential part of computer security, and most other aspects of computer security depend on it. Password systems are commonly the sole means of controlling access to computer systems. It is important to realise that once the password system is bypassed, the rest of the system is potentially open to exploitation. Users should adequately design, implement and maintain their passwords in support of overall access control in order to safeguard the security of the entire system.

2. Computer systems often use passwords as a means of controlling access to both data and functions. Particularly with larger systems, and certainly within the City of London Police, entry will invariably be controlled by associating user identifications with specific functions. Thus systems are programmed to grant certain rights to particular authorised users - these are known as user rights. That user may be allowed to view all the records in a data base, or be limited to seeing only a subset of the records. He or she may or may not be allowed to create new records, to amend some or all of the information in a record, or to delete records. The user identification may be added to a computer held transaction log so that subsequent audits can discover which user was responsible for any particular transaction carried out.

3. Usually at least one individual, the Departmental Systems Manager, will be allowed to assign user rights to all, or any individual and will be responsible for password management. It is generally best for individuals using the system to have their own password.

4. The password is used to safeguard these rights. Once a system recognises a user identification, (entered as part of the log-on procedure), it will ask for a password. It will then compare this with a table of approved passwords and, if a match is achieved, will grant the specified access rights. Invariably these will remain in force until such time as the terminal is switched off. System

security will be endangered if a user leaves a terminal logged on and unattended.

5. The purpose of this Order is to provide guidance to assist users to prevent passwords being compromised. Passwords must always be kept secret if they are to achieve their purpose. In some cases unauthorised users could exploit the system to the extent of destroying the software and any data it holds.

The Need for Password Security:

6. Passwords are an effective IT security countermeasure only if they can be kept secret. A major problem is that passwords can be passed to, and used by, others without the knowledge of the original owner. It may not be apparent that this has happened and a password so obtained may be used for some considerable period without detection.

7. Unless staff appreciate the need for IT security, they are unlikely to take sufficient precautions to protect the integrity of their passwords. The need to remember and enter passwords detracts from the ease of use of a system, and it is all too common for users to compromise security in their attempts to simplify the use of passwords. All new users should therefore be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected.

8. Some of the ways in which passwords can be vulnerable are set out in the following paragraphs. Countermeasures for reducing or negating these vulnerabilities are also described. The degree to which these measures are implemented is always dependent on the sensitivity of the data and the requirement for confidentiality, integrity and availability. Passwords should always be treated as though classified at the level of the most sensitive data held on the system to which they allow access.

9. Passwords should not be confused with user identifications, (see para. 2), which specify areas and functions accessible to a particular user. The

password is the way in which the system verifies that a particular user is who they claim to be.

Sharing:

10. For the most effective security, staff should have individual passwords and should never reveal them to anyone.(but see para. 11). The simplest form of compromising a password is to tell others what it is. No one has the right to know another's password; not friends, colleagues or line managers. There may be various temptations to share passwords with others depending on working conditions, however a shared password is not good security.

Finding:

11. Obvious though it may seem, and with one exception, do not write passwords down anywhere. The exception is that the password may be written on a slip of paper and placed inside a sealed envelope, classified to the highest level of the data held on the system and protected to that level. The envelope should then be placed in the custody of the departmental officer nominated. Access may then be allowed in exceptional circumstances, e.g. extended sick leave. This course of action should always be adopted for pass worded standalone personal computers.

12. The simplest way in which a password may be revealed to unauthorised persons occurs when it is written down and left in the vicinity of a terminal.

Watching:

13. Another way in which an unauthorised user may "discover" a password is to watch closely while an authorised user logs-on. Whilst it is true that passwords are not displayed on screen as they are entered at the keyboard, it is fairly easy to watch the keys being pressed by a user, if necessary over a number of days, as he or she logs into the system. The shorter the password the easier it is!

14. While it may appear antisocial to ask people to avert their eyes whilst a password is being entered, the only effective countermeasure is to ensure that password entry is never viewed by anyone else.

Guessing:

15. Given a free choice most users will opt for passwords that they find particularly easy to remember. One of the reasons for this is that users do not feel obliged to write down their password in case they forget it. All too often, however, the password chosen has strong associations with either the system or the background of the user and may be guessed by potential intruders.

16. It is a well-documented fact that many users favour passwords that mean something to them personally, e.g. their own name, the name of someone close to them, the name of their house, the name of a pet, a favourite football team or a favourite food. A strong temptation when several people share an application is to also share a password, which may be the application name, e.g. PAYROLL. Potential intruders, particularly those who work in the same area and perhaps know some of the users well often find such passwords easy to guess.

17. Users must, therefore, try to devise passwords that are unique to them and are unlikely to appear on an intruder's test list. Some suggested means of achieving this are given in the next section. Unguessable passwords will never consist of a single dictionary word or name. They will always consist of at least 6 characters, at least one of which will be something other than one of the 26 letters of the alphabet.

18. Unauthorised users may compile a list of likely and commonly used passwords that they will then test against the system until they find a successful match. Such a list is likely to include words like 'USER', 'FRED', 'BATMAN', 'SPURS', 'QWERTY', 'X', 'GUEST', 'BOSS' and 'PASSWORD'.

Secure Passwords:

19. A secure password is one that is made up of at least 6 characters - or at least 8 characters if it is to be used on a system processing nationally classified data.

20. An ideal way of creating secure passwords is by making them alphanumeric i.e. containing letters and numbers. In order to make the password easier to remember a hidden meaning may be added:

"SASO6P"	Sing a song of six pence;
"967PIMB"	967 pages in my book;
"672FSITR"	672 files in the registry;
"26WITBO"	26 windows in the building opposite;
"TA9COHCR"	There are 9 chimneys on Hampton Court roof;

21. Secure passwords may also be created by linking two dictionary words together with a non-alpha character:

"HAPPY-DAYS"
"CAT*MOUSE"
"CAR_GAME"
"AND?OR"
"FULL.STOP"

22. Even names may be made secure if extra characters are added or simple changes made:

"?NDREW"	
"ENNAANNE"	(Backwards and forwards);
"GE0RGE"	(With a zero instead of an "O");
"SAM-AN-THA"	
"TARGAREM"	(First and last letters switched);
"(JOHN)"	
"WSTMNSTR"	(Vowels removed).

23. Users may also consider using dates that have a particular significance for them (other than obvious ones like birthdays, which might be known to others). For added security differing formats can be used:

"070777"
"7-7-77"
"7:7:1977"
"7/7/77"
"JUL7,77"
"7JULY1977"
"JUL7th,77"

24. Instead of trying to choose a password that is easy to remember, users can select a password where it is easy to remember how it was created:

"IWLAAC"	the initials of the first line of Wordsworth's poem "Daffodils".
"ADGJL:"	every other key on the middle line of the keyboard, but beware using every key on any particular line e.g. "QWERTY".
"UDTQCSSHND"	initials of the French words for the numbers 1 - 10.
"1992SPAIN"	A memorable holiday.
"2A6S0S7"	A mix of extension number and initials.

Changing:

25. The longer a password remains unchanged, the more opportunity a potential intruder will have to discover it. Once compromised a password will continue to give an intruder access to a system until such time as it is changed. An essential countermeasure is therefore to ensure that the password is changed regularly. In so doing it would be counter-productive if a previous password were to be used again. Thus staff should aim to invent a new and unique password each time a change is necessary.

26. Where a system automatically reminds users that a password is due to be changed, but does not enforce the change, (as some do), the change should be made as soon as possible. If the system allows the user to decide when

to change the password it should be so changed at least every 3 months unless the system manager decides that it should be made at other intervals. If the data on the system are sensitive it may be advisable to change the password more frequently.

[NOTE: It is not advisable to change a password on a Friday afternoon or just before a prolonged absence from work, (e.g. on annual leave) as there is a good chance that it will be forgotten].

27. Lastly, passwords should always be changed immediately there is the slightest suspicion that they or the system has been compromised in any way.

For further information relating to computer security matters please contact the Force Information Security Manager, telephone 2704.

B Protective Marking Guidance

The application of 'need-to-know' is fundamental to all aspects of security. Where it is necessary to reinforce 'need-to-know', special handling instructions may be applied.

If material is originated requiring a protective marking, a descriptor may be added to reinforce 'need-to-know' by indicating the nature of an information asset's sensitivity and the need to limit access to it. Its use indicates to others the nature of the threat and the interested groups that may be given access.

Where there is a statutory requirement for access or disclosure of information, the use of a protective marking, with or without a descriptor, on information will not exclude the required access to that information. Where the information is covered by an exemption to the access rights and consequently should not be made available, this should be signalled by marking the relevant documents: NOT FOR DISCLOSURE with a reference being made to the appropriate act and reason for exemption by the originator.

Information marked with a descriptor should in the first instance be handled and protected in accordance with its protective marking. The application of a descriptor is only intended to highlight a need to take additional common sense precautions to limit its access to individuals and interested groups authorised to see it.

Originators must not generate their own descriptors. Only the descriptors listed below may be used.

APPOINTMENTS

Concerning actual or potential appointments that have not yet been announced.

COMMERCIAL

Relating to a commercial establishment's processes or affairs.

CONTRACTS

Concerning tenders under consideration and the terms of any tenders.

CRIME

Concerning Crime.

HONOURS

Recognition given for exceptional achievements.

INFORMANTS

Regarding informants and their handling.

Any informant related information should be protectively marked as a baseline CONFIDENTIAL, with the appropriate handling procedures. Information that identifies an informant may require marking as SECRET.

INVESTIGATIONS

Concerning investigations into disciplinary or criminal matters.

MANAGEMENT

Policy and planning affecting the interests of groups of staff.

MEDICAL

Medical reports and records and material relating to them.

PERSONAL

Material intended for the person to whom it is addressed.

POLICY

Proposals for new or changed government or Force policy before publication.

PRIVATE

Information collected through electronic government services provided to the public and relating to the individual:

- Access to be limited to the individual concerned and those representatives of agencies with a requirement for access under the governing legislation.

Information collected through electronic government services provided to the public and relating to an organisation:

- Access to be limited to the appropriate officials of the organisation concerned and by those representatives of agencies with a requirement for access under the governing legislation.

STAFF

Concerning references to named or identifiable staff or personal confidences entrusted by staff to management.

VISITS

Concerning details of visits by, for example, royalty, ministers or very senior staff.

With the exception of PERSONAL and PRIVATE, which may be used by themselves, the above descriptors may only be used in conjunction with a protective marking.

B.1.1 Handling, Transmission and Storage of Information Assets

Paper Documents		
	RESTRICTED	**CONFIDENTIAL**
Marking of Information	Top and bottom of every page; pages numbered	Top and bottom of every page; pages numbered.
Storage of paper	Protected by one barrier, for example, a locked container.	Protected by two barriers, for example, a locked container in a locked room.
Disposal of papers	Secure waste sacks **Keep secure when left unattended.**	Tear by hand and place in secure waste sacks or use a cross cut shredder **Keep secure when left unattended**
Data		
	RESTRICTED	**CONFIDENTIAL**
Force Data Network	May be used	May be used in conjunction with in accordance with your

		accreditation status
Criminal Justice Extranet	May be used	Encryption must be considered in accordance with the recommendations from the Manual of Protective Security
Internet	Government approved encryption required. Contact Force Information Security Manager	Not to be used.
Fax	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.	Use a secure fax machine only.
Disposal of magnetic media	Return to Technology Unit	
Voice		
	RESTRICTED	**CONFIDENTIAL**
Mobile telephones	Digital cell phones may be used. This does not include cordless telephones.	Only if operationally urgent; use guarded speech and keep conversations brief.
Message Pager Systems	Not to be used due their inherent insecurity	Not to be used

If there is a requirement to use any of the above methods of communication to pass information at a higher level than it is recognised safe to do so, the operational urgency and the need for transmission must be weighed against the risk of a security breach, for which you and/or the Force may be held accountable. If it is decided that such transmissions are essential they should be kept short and guarded speech used. The use of some form of prearranged codes should be considered to avoid identifying officers, informants or locations

B.1.2 MOVEMENT OF PROTECTIVELY MARKED MATERIAL

RESTRICTED		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand; OR Via the internal despatch service in a sealed envelope, or other container, with the protective marking and descriptor visible. Transit envelopes may be used, but must be sealed with the appropriate security label.	By trusted hand in a closed envelope or container; OR By post, or courier service. If so sent, the envelope should show no protective marking or descriptor (other than PERSONAL, if appropriate). It should be addressed to an individual by name or appointment	By trusted hand in a sealed envelope or secured container; OR By post or courier service. If so sent, the envelope should show no protective marking or descriptor (other than PERSONAL, if appropriate) It should be addressed to an individual by name or appointment. Contact SB for details of countries of special sensitivity

CONFIDENTIAL		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand; OR Via the internal despatch service in a new sealed envelope, or other container, with the protective marking and descriptor visible Transit envelopes must not be used	By trusted hand in a sealed envelope or secured container **OR** By post, or courier service, using double envelopes as described below.	Secured Container or double envelopes (see below) Contact SB for details of countries or special sensitivity.

	OUTER ENVELOPES, or secure containers, should not show the protective marking or descriptor, but should show the name/appointment and address of the recipient and a return address. Inner ENVELOPES should be similarly addressed and marked CONFIDENTIAL (plus DESCRIPTOR, if any

NB: "By trusted hand" means always in the possession of an employee or contractor with a security clearance appropriate for uncontrolled access to the material; the internal despatch service does not meet this requirement.

SECRET		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand; OR The internal despatch service must not be used. Movement sheets required.	Secured container or double envelopes (see below) To be carried only by trusted hand. Receipts and movement sheets are required.	Double envelopes (a secured box, or bag, or pouch will count as outer envelope). If an approved tamper evident envelope is not used as outer envelope, the inner envelope should be security sealed. Diplomatic Protection required or (for bulky items carried in hold) escort to and from aircraft on direct flight. Receipts and movement sheets are required
OUTER ENVELOPES, including secure bags or pouches, should not show any protective marking or descriptor, but should show the name/appointment and address of the recipient and a return address. INNER ENVELOPES should be similarly addressed and marked SECRET (plus DESCRIPTOR, if any).		

TOP SECRET		
WITHIN THE CoLP	**WITHIN GREAT BRITAIN**	**OUTSIDE GREAT BRITAIN**
By trusted hand. The internal despatch service must not be used. Movement sheets are required	Double envelopes (a secured box or bag or pouch will count as outer envelope). If an approved tamper evident envelope is not used as outer cover, the inner envelope should be security sealed. To be carried only by trusted hand. Receipts and movement sheets are required	Double envelopes (a secured box, or bag, or pouch will count as outer envelope). If an approved tamper evident envelope is not used as outer envelope, the inner envelope should be security sealed. Diplomatic Protection required. Receipts and movement sheets are required.
OUTER ENVELOPES, including secure bags or pouches, should not show any protective marking or descriptor, but should show the name/appointment and address of the recipient and a return address. INNER ENVELOPES should be similarly addressed and marked TOP SECRET (plus DESCRIPTOR, if any) and include the inscription TO BE OPEND ONLY BY…(addressee or other designated person; or return to sender).		

NB: “By trusted hand” means always in the possession of an employee or contractor with a security clearance appropriate for uncontrolled access to the material; the internal despatch service does not meet this requirement.

C The Law and electronic communications

The Data Protection Act 1998

The Data Protection Act 1998 (DPA) requires departments and agencies to process personal data 'fairly' and 'lawfully'.

Personal data means information about identifiable living individuals and includes both facts and opinions about the individual. The DPA provides for individuals to be provided with a copy, on request, of the personal data an organisation holds on them.

The DPA does not just apply to data held on large databases. Any set of data held electronically, including material held on a personal computer, is potentially disclosable. This includes any references to an individual in any document, file, folder or e-mail, including e-mails still in the "deleted" folder.

Although there has been a tendency to consider e-mails as an informal or ephemeral way of communicating, the data they contain is subject to the same disclosure provisions as data elsewhere. Directories containing names, telephone numbers, e-mail addresses, etc also fall within the scope of the Act. The DPA also applies to certain collections of non-computerised personal information, such as printouts of e-mails held in structured filing systems. It is crucial to ensure that anything created is accurate, relevant and justifiable, and that data and e-mails no longer necessary for business are fully deleted.

You can obtain further information from the Data Protection Officer (ext. 2209). Further information can also be found on the Home Office site at: http://www.homeoffice.gov.uk/foi/foidpunit.htm or the Information Commissioner's web site at: www.dataprotection.gov.uk. You should note that policy responsibility for the Data Protection Act transferred from the Home Office to the Lord Chancellor's Department (LCD) in June 2001. The links above may also be expected to change.

C.1.1 Human Rights Act 1998

The Human Rights Act 1998 incorporated the European Convention on Human Rights into domestic law. Under this Act a UK citizen is be able to assert their Convention rights through the national courts without having to take their case to the European Court of Human Rights.

Further information on the Human Rights Act can be found on the Home Office site at: http://www.homeoffice.gov.uk/hract/hramenu.htm

C.1.2 Regulation of Investigatory Powers Act 2000

Part I of the Regulation of Investigatory Powers Act 2000 (RIPA) makes it unlawful for employers and others to intercept communications, in the course of their transmission on a private telecommunications system, unless certain conditions are met. Interception is allowed where: -

- the parties to the call, e-mail or other communication have both consented to the interception, or
- the interception is of communications taking place using the employer's business telecommunications system and is authorised under The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

The RIPA only restricts access to the contents of a communication. It does not address the collection and use of traffic data on a private network, for example, the information about telephone calls that would typically be produced by a call logger. This is subject only to the requirements of the Data Protection Act 1998.

A public sector employee invoked the European Convention on Human Rights after her employer intercepted her telephone calls (Halford v UK Government). The European Court of Human Rights found that the secret interception of calls made by Ms Halford from her office amounted to an unjustifiable interference with her right to respect for her privacy and correspondence, contrary to Article 8(1) of the European Convention on Human Rights.

Further information on RIPA can be found on the Home Office site at: http://www.homeoffice.gov.uk/ripa/ripact.htm

C.1.3 The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

The Lawful Business Practice Regulations authorise certain interceptions of communications that would otherwise be prohibited under the RIPA 2000. The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions), for purposes relevant to that person's business, and using that business's own telecommunication system.

Interceptions are authorised for:

- monitoring or recording communications -
  - to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training),
  - in the interests of national security (in which case only certain specified public officials may make the interception),
  - to prevent or detect crime,
  - to investigate or detect unauthorised use of telecommunication systems, or
  - to secure, or as an inherent part of, effective system operation;

- monitoring received communications to determine whether or not they are business communications;
- monitoring communications made to anonymous telephone help lines.

Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made. The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: they are not prohibited by the Act.

Further information on the Regulations can be found on the DTI web site at: http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/lawful_business_practice_regulations.shtml
The Regulations are available on the HMSO web site at: http://www.legislation.hmso.gov.uk/si/si2000/20002699.htm

C.1.4 The Freedom of Information Act 2000

The Freedom of Information Act (FOI Act) gives a general right of access to information held by the force. In due course it will replace the existing Code of Practice on Access to Government Information. The Act also amends certain provisions of the Public Records and Data Protection Acts. It provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to recorded information held by bodies across the public sector.

> *The legislation will apply to a wide range of public authorities, including Parliament, Government Departments and local authorities, health trusts, doctors' surgeries, publicly funded museums and thousands of other organisations.*

The Act gives a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions.

Together these Statutes place a duty on departments and agencies to manage records, including e-mails, in such a way that their provisions can be complied with.

Further information can also be found on the Home Office site at: http://www.homeoffice.gov.uk/foi/foidpunit.htm or the Information Commissioner's web site at: www.dataprotection.gov.uk.

C.1.5 Obscene Publications Act 1959

All computer material is subject to this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity. 'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to include the originator or poster of the item.

C.1.6 Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under s.43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

C.1.7 Protection of Children Act 1978; Criminal Justice Act 1988

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

C.1.8 Copyright, Design and Patents Act 1998

Copyright law applies equally to the Internet as it does to paper material. Many web sites contain a copyright notice detailing how the material they contain may be used. Often, this is in the form of a hyperlink from a short copyright notice to a more detailed statement of what is permitted. If no copyright notice is provided, it is not safe to assume anything. If you want to print out a Web page or attachment, or copy-and-paste anything from a Web page or attachment into a document of your own, you should obtain the permission of the copyright owner. For any use beyond everyday Web-browsing, permission should be obtained. A good starting point is to send an email to the web site operator. Where permission has not been granted, individuals and the Commissioner could be liable to civil proceedings by the author.

C.1.9 Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976

Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities has played a role.

C.1.10 Computer Misuse Act 1990.

This Act makes it an offence for an unauthorised person to access knowingly a program or data or for such a person to modify knowingly the contents of a computer.

This is not a comprehensive list of the law that could be relevant. Anyone requiring specific information on the effects or the effective implementation of these Acts should seek advice from an appropriate legal source.

D Data Cleansing Request Form

Device Information (to be completed by the source department)

Device location: ____________________

(include department, building and floor)

Device Type: □ Computer □ USB Drive □ Server HDD
□ Laptop □ Printer □ Photocopier HDD
□ Other (Please specifiy) ____________________

Manufacturer: ____________________ Model: ____________________

Serial Number: ____________________ Property Tag ID: ____________________

I authorise the above device to be decommissioned in accordance with the Force Asset Disposal procedure and can verify that any CoLP information has been removed from the device.

Name: ____________________ Position: ____________________

Signature: ____________________ Date: ____________________

Cleanse Verification (to be completed by Technology Unit)

Decommission date: ____________________ Date of Cleanse: ____________________

Method of Cleanse:
□ Software
□ Physical Destruction
□ Degaussing
□ External Service

Details of Cleanse:

(Include brief details of work undertaken including software or service provider)

Equipment location: ____________________

I confirm that the details entered on this form are a true and accurate record.

Name: ____________________ Position: ____________________

Signature: ____________________ Date: ____________________

A copy of this form must accompany the equipment when sent to IT for disposal. On finalisation the completed form must be sent to the Force ISO for audit purposes.
Last revision date 20/05/08

E Third Party Connection Agreement

EXAMPLE AGREEMENT FOR A THIRD PARTY USER FOR CONNECTION TO A FORCE IT SYSTEM

1 This agreement between the City of London Police and

Hereinafter referred to as the USER, relates to the USER's connection to the following system(s):

2 The connection is subject to the terms and conditions set out in Schedule 1 (attached).

3 The type or method of connection will be by:

4 The following list of specific items of user equipment and software are approved by the Force for connection to the system:

5 The USER is permitted connection for the following purposes:

6 The USER is permitted to access the following information:

7 The USER is permitted to disclose the following information:

#Third Party Company#

Signed: Date:

Position:

City of London Police (Information Asset Owner)

Signed: Date:

Position:

SCHEDULE 1

INTRODUCTION

1. This Schedule sets out the terms and conditions under which the City of London Police provides an authorised third party, hereafter called the User, with a connection to the specified computer system.

2. The system may contain protectively marked information which **must** not be disclosed to unauthorised individuals or organisations. It is therefore essential that it should be adequately protected from all security threats which may result in:

   - reductions in systems reliability and performance;
   - inaccurate or incomplete data; or
   - unauthorised disclosure of protectively marked data.

   It is therefore necessary that the security of the system should not be compromised as a result of the connection of independent organisations to any part of the system.

3. It is a condition of access to the system that the User should maintain at least the minimum system security controls as set out in this Schedule.

RIGHTS AND OBLIGATIONS

4. Whilst it is the responsibility of the User to implement the minimum security controls described in this Schedule, they should not necessarily regard them as sufficient to meet the User's own security requirements, e.g. under the Data Protection Act.

5. The City of London Police reserves the right either:

to audit the relevant security controls implemented by the User against the requirements set out in this schedule at reasonable and convenient times. Such audits may be arranged at short notice and may be carried out by the City of London Police or by other qualified organisations authorised by the City of London Police to act on its behalf;

or

to request that a suitable annual audit be carried out by the User at the User's expense.

The execution and findings of audits carried out by or on behalf of the City of London Police will be recorded. When corrective action is required the record will be made available to the User. The User will be required to submit a written annual statement to the City of London Police confirming that his security controls are in compliance with this Schedule.

6. If an audit reveals a security weakness which, in the opinion of the City of London Police, is not in compliance with this Schedule, or which in any other way unnecessarily exposes the system to a security risk, then the user will be asked by the City of London Police to implement appropriate improvements.

7. The City of London Police reserves the right to discontinue User access to the system if, in its opinion, User security procedures are inadequate. In these circumstances User access may be restored following a satisfactory formal audit of any security improvements that are required.

8. The City of London Police reserves the right at his sole discretion to permanently disconnect a User from the system for whatever reason and such disconnection shall not give rise to any claim for damages or compensation of any kind whatsoever by the User or by any third party claiming or purporting to claim through the User.

9. The User is responsible for protecting the confidentiality of information obtained from the system.

10. Information made available to the User under the Agreement has been compiled to satisfy the City of London Police's requirements. Although all reasonable efforts are made to ensure its accuracy and completeness, the City of London Police will accept no responsibility for any inconvenience or loss or damage resulting from the User's reliance upon this information for other purposes, or from any interruption in system service which may be necessary.

11. The User is responsible to the City of London Police for the consequences of any breach of system security which is occasioned by the User's staff.

MINIMUM SYSTEM SECURITY CONTROLS TO BE IMPLEMENTED BY USER

12. Throughout the following, the term 'User equipment' includes any computer equipment on the User's premises or under the User's control, which is or is intended to be connected to the system. The User equipment and associated software shall be as defined in Item 4 of the Agreement.

SECURITY ADMINISTRATION AND STAFFING

13. The City of London Police will appoint a person or persons ("the City of London Police's nominated representative") to oversee the implementation by the User of the provisions of this Schedule relating to security controls to be enforced, maintained and monitored by the User.

14. The User will appoint a suitably qualified and authorised member of staff (the "security administrator") to be formally responsible for enforcing, maintaining and monitoring the security controls set out below. The security administrator will be responsible for ensuring that all necessary records and documentation are current and complete, and for liaising with the City of London Polices' nominated representative on matters relating to the security of the connection to the system

and associated equipment and facilities. These responsibilities must be formally documented, with appropriate reference to the Agreement.

15. The User equipment will only be operated by suitably qualified and trained members of the User's staff. The City of London Police reserves the right to carry out such security vetting checks on the members of staff which they may, at their sole discretion, consider necessary to safeguard the security of systems.

16. The User must place a formal responsibility on members of staff to adhere to all system security controls and procedures. Members of the User's staff must be informed of this responsibility in writing.

SECURITY OF EQUIPMENT

17. Only the specific equipment identified in the Agreement may be connected to the system.

18. A register must be kept of all normal use made of the User equipment and must include:

a) the dates and times of the beginning and end of each period of physical connection;

b) the purpose of the use;

c) details of all User log-ons and log-offs; and

d) the name(s) of the staff involved.

19. The User must comply with system password and other access control procedures stipulated by the City of London Police.

20. No User equipment connected to the system may concurrently be connected to any other computer or communication system without the prior agreement of the City of London Police. Any connection between the User equipment and other

computers or networks which the User may make from time to time must be recorded in a log which must include:

a) the dates and times of the beginning and end of the physical connection period; and

b) the purpose of the connection.

21. All system and User logs stipulated in this Schedule must be made available for audit when required.

PHYSICAL ACCESS SECURITY

22. Physical access controls to User equipment must be in accordance with methods agreed with the City of London Police and be in operation at all times to ensure:

a) only authorised members of User staff operate the equipment; and

b) all unauthorised staff, such as equipment maintenance personnel and office cleaning personnel, who require occasional access to User equipment or its accommodation, are supervised, at all times, by an authorised member of staff.

OPERATIONS AND DATA SECURITY

23. User equipment will only be connected to the system at times and for periods agreed with the City of London Police's nominated representative. Specialised User equipment connected for technical support purposes will normally only be connected to the system at times and for periods necessary for the purpose, and in all cases with the explicit prior permission of the City of London Police's nominated representative.

24. Any data other than that permitted by the City of London Police for disclosure which is retrieved by User equipment from the system in permanent form (whether in printed or electronic form) must be retained within the same physical

environment and destroyed after use. Destruction shall be by non-recoverable means (e.g. shredding or incineration).

25. Computer terminals must be positioned to avoid the possibility of casual observation by unauthorised persons.

26. The User must take precautions to protect the confidentiality of any documentation relating to the system.

27. Information for which disclosure has not been permitted is subject to the provisions of the Official Secrets Act. The User shall produce a sign to remind the User's staff of the Act and its applicability, and erect copies in the appropriate areas.

F Security Incident Reporting

You can create a new security incident report by clicking here or navigating to SharePoint and selecting “Report Security Incident” from the home page.

Security Incidents are broken down into the following categories and should be reported in all instances here.

Email Misuse

- Emailing information to a non-secure address (via an insecure route) (E.g. Home PC’s)
- Sending inappropriate content in contravention of local policy
- Emailing information assets to unauthorised recipients

ID Cards – Keys – Warrants:

Lost - Missing – Stolen – Not Returned.

- Includes access control tokens
- Those that can be disabled
- Those where there is a continuing risk

Physical Security

Wide ranging but consider local policy and:

- Failed locks
- Doors wedged open – windows left open
- Door combination settings unofficially shared with unauthorised personnel
- Alarms not set

Airwave Incidents

- Radios Lost or Stolen
- Confirm stunning
- Breach of Procedures

Unplanned Outage

- Equipment failure
- Incidents where some action that was not expected to affect system availability did so
- System was taken out of service, but users were not told beforehand

Procedural

- Failure to comply with procedures through lack of awareness
- Deliberate attempts to circumvent security measures.

Unauthorised Disclosure

- Misconduct cases
- Data Protection Act breaches

- Information made available to people who are not authorised to have it
- Sensitive information on paper not securely disposed of

System Misuse

- Use of an ICT system other than for its intended authorised purpose such as an enquiry on PNC to satisfy private curiosity, rather than for a genuine investigation.

Malicious Software

- Successful and regular identification and quarantine of malware at or near a system boundary is **not** counted as an incident. Unusual or unexplained activity at a system boundary (e.g. potential denial of service attack) should be reported.

Unauthorised access to systems or data

- Access rights incorrectly granted
- Clear desk policy breaches
- Unattended equipment left logged on

Internet Misuse

- Breaches of Force policy
- Excessive personal use
- Disclosures on personal social networking sites

Unauthorised Person(s) on Premises

- Failure in Technical access controls
- Failure in physical access procedures

Account Sharing

- Password sharing, or an account signed on by one person and used by another / several.
- Non Standard Accounts

Loss or Theft of Technology Assets

- Laptop
- PDA
- Blackberry
- Mobile 'Phone
- USB Memory Sticks
- Portable peripherals
- Other Assets

Paper Documents

- Lost Including non-delivery by Royal Mail, courier, internal post
- Documents found where they should not have been
- Left insecure on desks, in cars, public transport etc.
- Breaches of GPMS

Crypto

- Any incident involving crypto.
- Breaches of IS4 requirements.
- Note that the loss or theft of any Crypto item should be reported using CINRAS.

Data Storage

- Where data – including backups - is not stored in accordance with its protective marking.

Vetting / Personnel

- New employee, contractor or volunteer, allowed access to premises or data without clearance.

Removable Media Related Incidents

- Use of private USB memory sticks to transfer data
- Unauthorised download / upload of data via USB ports
- Unauthorised download / upload via other media, e.g. CD's.

Social Engineering

- Masquerading as someone entitled to access to information or premises.

Unauthorised Equipment

- Use of equipment that has not been approved by the ICT department – generally items brought from home

Unauthorised Software

- Commercial software installed without authority / licence

Unauthorised System Connection

Insecure Disposal

- Breaches of IS5 requirements

Loss or Theft of Uniforms