

Information Security Policy

Contents:

1.0	Introduction	Page 2
2.0	Management Intentions	Page 4
3.0	The Security Environment	Page 5
4.0	Roles and Responsibilities	Page 6
5.0	Security Monitoring, Review and Escalation	Page 9
6.0	Policy Statements	Page 11

Document Control

Version	V10
Date	15th June 2010
Author	A. Cole
Owner	Cambridgeshire Constabulary

1.0 Introduction

General policy

The Constabulary has a legal and moral duty to protect any information it holds, and for computerised systems, to secure the hardware, software and network which stores and distributes the information within the Constabulary.

This document is endorsed by the Chief Constable as a high-level security statement. The implementation of this policy demonstrates the commitment of the Force in complying with the requirements of the ACPO Community Security Policy (CSP) and the guidance given by the National Police Improvement Agency on Identity Access Management, thus enabling secure information sharing within the police community and our partner organisations.

Purpose of security

The purpose of Information Security is to:

Ensure operational continuity and to minimise damage or financial loss to the Constabulary by preventing and reducing the impact of security incidents.

Promote public confidence that the Constabulary is complying with all the legal requirements for the collection, maintenance and disposal of information handled by Constabulary IT systems in the course of operational duties.

Who must read this Policy?

The Information Security Policy concerns all Constabulary Officers, Special Constables and Police Staff employees, including temporary staff, volunteers, contractors and suppliers.

Contents

The Main part of the Information Security Policy comprises the following sections:

Management Intentions. A statement of objectives, benefits and compliance.

The Security Environment. An overview of IT services and access points covered by the Information Security Policy.

Security Monitoring, Review and Escalation. The policy for monitoring and reviewing security, and for escalating security issues.

Policy Statements. A series of brief definitive statements covering all aspects of Information Security. Where the reader is required to follow a specific procedure, a reference will be made to a Procedure (see below).

NOT PROTECTIVELY MARKED

Procedures

To accompany the Main Policy there are a series of Procedures which set out guidelines for how the policy is to be applied to different areas of IT services used within the Constabulary. The Information Security Procedures currently in force are:

- Information Security
- User Access
- Remote Access (3rd Party)
- Home Working
- Data Disposal
- Email Usage
- Internet Access
- Portable Computers
- Blackberry Terminals
- Clear Desk
- PNC Compliance
- Remote Service Portal (RSP)
- Software Acquisition
- Clear Desk
- Information Sharing

2.0 Management intentions

Objectives

This Policy is designed to encourage a professional approach to the handling and disclosure of information throughout the Constabulary. The key objectives of the protective measures set out in this Policy document and its Procedures are the maintenance of:

Confidentiality. Ensuring that information is not disclosed to unauthorised persons, or used in an unauthorised manner.

Integrity. Ensuring accurate entry and maintenance of the information stored in the IT systems - that is preventing unauthorised modification of the information.

Availability. Ensuring that information is available when required by authorised Constabulary users, and that data is not corrupted or lost.

Benefits of compliance

A high degree of compliance with the Information Security Policy benefits the Constabulary and the public by:

Avoiding inappropriate disclosure of information.

Minimising operational problems due to data loss or corruption.

Reducing public anxiety about how the Constabulary stores, uses and disposes of sensitive information.

Clarifying the roles and responsibilities of all staff in maintaining effective Information Security.

Demonstrating compliance with legislation and contractual requirements.

Compliance

In order to meet the above goals and realise the benefits, the Constabulary intends that this Policy and its Procedures are adhered to at all times. All employees, contractors, permanent or temporary, are responsible for complying with the Information Security Policy within the scope of their own work area. Information Security will be regularly monitored and reviewed and an escalation procedure will be implemented to deal with detected security violations. Failure to comply with the Information Security Policy will be treated as misconduct and may be considered gross misconduct under the Constabulary disciplinary procedures.

Employees have a right to be informed of all relevant policies, procedures and legislation so they can comply with the Information Security Policy. Employees should contact the Human Resources Department if they require further information.

NOT PROTECTIVELY MARKED

Implementation

Department Heads and Divisional Commanders are responsible for implementation and compliance with the policy in their areas.

3.0 The security environment

Services

The following are examples of the wide range of ICT services delivered to users:

Office automation applications such as Lotus Notes for electronic mail and database services, Microsoft Word processing facilities and Excel spreadsheets.

Intranet and Internet services.

Administrative applications such as the Administration of Justice System (AJU), the Custody System and HOLMES.

Command and Control System.

Centrally controlled information systems such as the Police National Computer (PNC), ViSOR and MEMEX.

The above is not an exhaustive list of the currently available services - a complete description of all services can be obtained from the Service Delivery Manager, Information Communication Technology (ICT Services).

Access points

Workstations

ICT Services are delivered to Constabulary users via the following types of workstations:

Desktop Workstations connected to the Cambridgeshire Constabulary Digital Network (CCDN).

Stand-alone PCs not connected to any network.

Portable computers and remote connected PCs, which may have authorised on-line access to Constabulary ICT systems via the remote access service.

Hand held Blackberry terminals.

Printers

Most printers are connected to the CCDN and are therefore accessible from nearby and remote desktop workstations. Users should remember that printed output is covered by this Information Security Policy, and should follow the guidelines in the Information Security Procedure.

NOT PROTECTIVELY MARKED

External systems

The security environment also covers any Constabulary computers connected to external systems belonging to third parties, such as software maintenance companies.

Physical security

Users (or potential users) should be aware that the primary risk to Information Security is the point at which services are accessed. Divisional Business Managers, HQ and Safer Communities Managers are responsible for the physical security of the terminals and the building in which the terminals are located, and should refer to the Buildings Security Policy for guidance.

The use of Constabulary ICT equipment or services for personal use or private gain is not allowed. The misuse of personal computers, telephones, fax machines and communications equipment, will be subject to disciplinary action. Users should check with their line manager or the Information Security Manager if they are unsure what is construed as misuse

4.0 Roles and responsibilities

This section outlines the roles and responsibilities of those involved in the compliance and enforcement of the Information Security Policy. It is not intended to be a complete definition of all the responsibilities that the role holder may have.

Users

Any person who accesses a Constabulary ICT service is a User. Users are responsible for the security of the data they are processing or accessing, and must have read this Information Security Policy and its associated Procedures.

When users are first provided with access to ICT services they will be provided with training on the impact of the Information Security Policy on their job. Users must be made aware that all systems will be regularly monitored for security incidents.

If a user is in any doubt about how the Information Security Policy applies to their job, they must always contact the User Manager or the Information Security Manager. Questions regarding the confidentiality of the content of information must be directed to the Force Data Protection Officer.

Local managers and Divisional Business Managers, even if they are not themselves users, are responsible for the physical security of premises containing ICT equipment and associated restricted information.

User Managers

Each Constabulary ICT system or application is allocated a User Manager who is responsible for:

NOT PROTECTIVELY MARKED

Acting as the first line of support for users.

Controlling user access to the system or applications, within boundaries set by the Information Security Manager.

Training users in the meaning and practice of the Information Security Policy

Ensuring their system and its users comply with the Information Security Policy.

Monitoring use of the system for security breaches and reporting problems or exceptions to the Information Security Manager or in the case of Data Protection breaches, to the Data Protection Officer.

Submitting monitoring reports to the Information Security Officer for review.

Assisting with PSD investigations into system usage when required.

Note that User Managers may delegate some or all of these responsibilities to key users, subject to the approval of the Information Security Manager. While the Information Security Policy allows for delegation in this way, the responsibilities listed above still reside with the User Manager.

Information Communication Technology Services Department

Within the ICT Services Department, the following roles have specific responsibilities under the Information Security Policy:

Service Delivery Manager. Overall responsibility for the security of the Constabulary Core Applications and Communications Systems. Responsible for the routine provision of Information Services to the user community, and ensuring that such services are delivered in a manner that enables the user community to protect the information handled by them.

Network Services Manager. Overall responsibility for the security of the Constabulary Digital Network. The Network Services Manager also acts as the User Manager for Lotus Notes and other centrally managed LAN-based services, and controls the issuing of user IDs for such services.

ICT Systems Team Leader. Responsible for the issuing of all UNIX User ID's centrally and the day to day administration of all Constabulary Core Applications and Systems. Responsible for all user access to RDBMS systems, and ensuring the integrity and availability of the data, tables and structures contained in the database. The Team Leader may delegate some of these responsibilities to User Managers where appropriate.

Information Security Manager

General responsibilities

The Information Security Manager is a full time role within the Professional Standards Department, and reports directly to the Head of PSD.

The Information Security Manager is responsible for:

NOT PROTECTIVELY MARKED

Ensuring the referential integrity and security of data across different ICT systems.

Monitoring the changes to user access rights (for example new users, changed ids etc.).

Reviewing security monitoring reports submitted by User Managers.

Investigating any reported security breaches, and executing the escalation procedure.

Routine liaison with Data Protection Officer.

Manage the implementation and day to day application of the Information Security Policy throughout the force.

Act as a focal point on all matters relating to Information Security and disseminate regular information and advice when necessary to management and users.

Submitting regular reports on security administration to the Service Delivery Manager.

PNC responsibilities

In addition to the above general responsibilities, the Information Security Manager has the following responsibilities with respect to the Police National Computer (PNC).

Liaising with the PNC Security Manager

Ensuring that security measures are implemented on PNC facilities in accordance with the PNC IS Security Policy.

Acting as stage manager in the project to implement PNC Security Review recommendations.

The Data Protection Officer

The Force Data Protection Officer's main purpose is to provide management guidance to ensure that Cambridgeshire Constabulary complies with all aspects of legislation, Home Office, ACPO and Force policies relating to personal data in whatever form it is held.

It is important to note that Principle 7 of the Data Protection Act, 1998 relates to Information Security.

The duties of the Force Data Protection Officer pertinent to Information Security are as follows;

Registration of all types of systems containing personal data to the Information Commissioner.

Provision of the right of access to the subject of data held by the Constabulary.

Provision of specific advice to system managers and users of force systems, relating to the practicalities of ensuring compliance with the regulations.

NOT PROTECTIVELY MARKED

Auditing to assess both the compliance of the data held and the use made of the data.

Investigation of all Data Protection breaches.

Liaison with Information Security Manager on Data Protection matters.

The Assistant Chief Constable (ACC)

The ACC has ultimate responsibility within Cambridgeshire Constabulary for the security of the data and Information Technology Systems. Assisted by the Director of ICT Services, the ACC will have the final decision on matters raised under the Information Security Policy Escalation procedure. The ACC also acts as the Force Senior Information Risk Officer (SIRO).

4.7 Department Heads & Divisional Commanders.

Department Heads and Divisional Commanders are responsible for the implementation of the policy in their areas and for the compliance to it by their staff. They will report any actual or suspected breach to the policy and provide resources to assist the Information Security Manager in investigating the suspected breach.

4.8 Divisional Information Security Co-ordinators.

Divisional Information Security Co-ordinators are responsible for the day to day work of monitoring of the Information Security Policy within their division. They are appointed as a part time role within a division by the Divisional Commander, (normally attached to an existing job) and will report and liaise on matters of Information Security with the Information Security Manager and Data Protection Officer.

5.0 Security Monitoring, Review and Escalation

Why Security Monitoring?

The objective of security monitoring is to discover potential security problems and encourage good practice throughout the Constabulary. The intention is to promote an awareness of Information Security. In general the monitoring and reporting process will usually result in advice and/or training so that good Information Security practices becomes part of everyday procedures.

Monitoring and reporting

Much of the security monitoring is delegated by the Information Security Manager to User Managers, local Divisional Information Security Co-ordinators and to the users themselves. Each User Manager is responsible for monitoring how their systems are being used with a view to identifying security breaches, or potential threats to the ICT

NOT PROTECTIVELY MARKED

systems and data. In particular the User Manager must periodically submit a monitoring report to the Information Security Officer detailing:

The number of failed access attempts if this information is available from the system.

Unusual logon patterns.

Summary of user access modifications (additions, changes, deletions), including any allocation of special administrator privileges.

Summary of any detected security violations.

Breaches of security

Any person detecting a breach of the Information Security Policy must report it immediately to the Information Security Manager, who will take immediate action as laid down in the Escalation Procedures within the policy.

Where disciplinary action may result from a reported incident, strict confidentiality will be maintained at all times. The Constabulary want to encourage and enable staff to raise their concerns at an early stage and to do so in the right way without fear of adverse consequences. If we know about a risk or danger in terms of Information Security and do nothing about it we are also accountable for the consequences. For further information refer to the Reporting Wrong Doing Policy.

Escalation Procedure

When a breach to the Information Security Policy is identified the following procedures will be followed in an order considered appropriate by the Information Security Manager until the matter is resolved:

The Information Security Manager will investigate the cause of security breach.

If the breach is deemed to be of a minor nature, the Information Security Manager will issue written guidelines to the user(s) involved. The guidelines will advise the user(s) on how the Information Security Policy was breached, and will draw attention to how the policy should be applied in the future. No further action will be taken providing the breach does not re-occur within three months.

If the Information Security Manager considers that the suspected breach has potentially significant security implications, user access to the system may be suspended immediately and the appropriate User Manager will be informed. Suspension of user access will remain in force until the matter is resolved.

If the security breach is found to have a serious impact on delivery of ICT services, or is a reoccurrence of a minor breach, or results from a previously suspended user access, the matter will be reported to the Service Delivery Manager who will discuss it with the relevant system managers.

If the breach is likely to lead to disciplinary action, or if user access needs to be revoked, the matter will be reported to the Head of PSD, who will discuss it with the appropriate Divisional Commander or Head of Department. Where appropriate, the Director of ICT Services should be consulted especially where technical issues are involved.

NOT PROTECTIVELY MARKED

Where the breach to the policy is by a User Manager, a senior ICT Department member of staff or in other exceptional circumstances, access to the system may be suspended for that person by the Information Security Manager if considered necessary, and be reported to the Head of PSD and Director of ICT Services.

If the breach to the policy is by the Information Security Manager, the Head of PSD will have the responsibility of investigating the breach and where necessary suspending the computer access rights of the officer.

If the breach is deemed to impact the ability of the Constabulary to meet its obligations for the use of IT, the matter will be reported to the ACC by the Director of ICT Services.

In the absence of the above mentioned officers, the matter may be reported directly to the ACC or in his absence, the Director of ICT Services, representing FEB.

6.0 Policy statements

Introduction

Each of the following statements sets out the Constabulary's policy in a particular area of Information Security. The statement may be backed up by one or more Procedures which provide guidelines to Users and User Managers for how to apply the Information Security Policy at the workplace. Alternatively the policy statements may cross-refer to other relevant Constabulary policies.

Security of information

Where is information held?

Information is stored and used in Constabulary ICT systems in a variety of forms. For the purpose of this Policy, information may include any of the following:

Data stored in servers and distributed around the Constabulary network to users with PCs connected to local area networks (LANs).

Data stored in UNIX computers.

Data extracted from centralised computers such as the Police National Computer and displayed on computer terminals and PCs.

Printed reports and screen dumps.

Data stored on magnetic media.

What is RESTRICTED information?

The following are typical examples of RESTRICTED information as defined in the Government Protected Marking Scheme and covered by this Policy.

All personal data held by the Constabulary under the terms of the Data Protection Act 1998.

NOT PROTECTIVELY MARKED

Personal data relating to victims, their families and acquaintances.

Information regulated by law (such as intelligence information).

Restricted information as defined in contractual agreements between the Constabulary and its suppliers.

Financial information which, if not protected, could expose the Constabulary to fraud.

[Access to RESTRICTED information](#)

Access to RESTRICTED information is limited to:

Persons who have a genuine and proven need to know.

The person who is the subject of the information, following an official application through the Data Protection Officer.

Inadvertent disclosure of RESTRICTED information must be avoided by all persons handling the information. See Legal Obligations for a summary of the implications of the Data Protection Act. See the Information Security Procedure for guidance on keeping information secure.

[Physical security](#)

Physical security of Constabulary ICT systems (and therefore the information those systems maintain) is the responsibility of all staff. It is important that all staff guard against:

Unauthorised access to Constabulary premises.

'Hi-jacking' of open ICT accounts.

Theft of computer equipment, magnetic media and hard copy.

Malicious damage to computer equipment or the Constabulary network.

Environmental hazards such as fire.

Users should contact the Estates Manager or the local administration office for policies concerning physical access.

Specific measures should be taken by Department Heads and Divisional Commanders to identify and secure rooms containing sensitive information whether stored within Computers or not. Consideration must be given to the visibility of information to visitors and from the outside, and measures be put in place to prevent inadvertent disclosure of personal or sensitive data.

The Security and restricted access to ICT equipment rooms must be given a high priority by Department Heads and Divisional Commanders and every reasonable step should be taken to ensure the absolute minimum risk of unauthorised entry or

NOT PROTECTIVELY MARKED

damage. Work identified as being necessary within these rooms, such as building or electrical work must be co-ordinated and agreed with the ICT Department Service Delivery Manager.

Accuracy and integrity of data

Information collected and processed by the Constabulary must be checked for accuracy and kept up to date at all times. User Managers and Line Managers are jointly responsible for implementing quality checks on all data entered onto Constabulary IT systems. Quality checks must be carried out by a person other than the user who first keyed in the data.

The Data Protection Officer has specific responsibility to ensure these checks are being made regularly and to investigate any resulting problems.

User access

Requests for access

Constabulary ICT systems are accessible only to those persons who have a genuine need to use the system in order to carry out their work. It is the User Managers' responsibility to manage and control access to their systems.

Monitoring and Audit

Constabulary employees should have no **expectation of privacy** in respect of their use of communication methods and computer systems which are provided by the Force.

User IDs

User ID's should ensure that all activities including read/write/amend/delete can be traced to individuals. Each user of a particular ICT system or application must have a unique user ID for his/her sole use. Shared user IDs are not permitted except in exceptional circumstances as determined by the Information Security Manager. In these cases the Information Security Manager will be required to assess the business benefits against the risks of inadvertent information disclosure, data corruption or data loss.

Password management

All Constabulary owned ICT systems must be password protected and all user IDs must have passwords. Where technically possible the system must force users to change passwords at least every 40 days, although the Force Single Sign On mechanism will activate for most systems so that only initial password entry / change is required. Exceptions to this policy may exist at the discretion of the Information Security Manager. Passwords must be generated in a manner that makes them difficult to guess. Passwords must be distributed in such a manner that

NOT PROTECTIVELY MARKED

confidentiality of passwords is maintained. i.e. if via email, don't include an explanation of what the password is for in the same text.

User ID Expiry

Where a User ID has not been used in over 3 months, the User Manager should consider suspending or deleting the account, dependant on the circumstances involved. There are potentially a number of reasons that may cause a User to not activate their account for a lengthy period; this could include extended Sick Leave, Secondment, change of duties etc. This should be taken into account when considering the most appropriate action to take. In any event, the account should be deleted if it has not been used in 6 months.

If the User subsequently requests access to the system in the next six months they will in effect be a new User and the User Manager must be satisfied that a suitable level of competency exists before granting their access. This will normally involve either a 'Refresher' or full training course and /or a competency test.

Where a competency test is elected, it can be administered by the local Line Manager who should then advise the User Manager of the outcome by email. The Line manager must be aware that they are responsible for ensuring competent use of the system by their staff member. Competency checks may be obtained from the User Manager.

Where a User ID has not been used in over 12 months, or where they fail a competency test, then re-training must be taken before access can be granted. Disputed access requests should be registered with and recorded by the Information Security Manager.

See the *User Access Procedure* for specific access control guidelines.

Logon Dialogue & Identification

The log on dialogue should not assist unauthorised users in any attempt to gain unauthorised access.

The workstation identifier should be used to restrict users to specific workstations or assist in investigation of any specific security related incident.

Unauthorised Software

Any software shall be considered unauthorised if it does not feature in the Force Approved Software List (see IT Systems Porfolio). Use of unauthorised software on Constabulary equipment is expressly forbidden and may result in disciplinary action.

Police National Computer.

The Police National Computer is used widely throughout the force and is an integral part of policing. As such a national policy exists for all forces connecting to it and each user is responsible for adhering to those policies. The force has therefore adopted in whole the PNC Code of Connection Policy as issued by the NPIA group within the Home Office. All users of PNC must therefore make themselves aware of the policy and ensure they comply with its requirements. Failure to do so may lead to disciplinary action being taken.

NOT PROTECTIVELY MARKED

Internet.

Each User has an Internet account which may be used for business purposes and limited personal use. The force has published a dedicated Internet Policy. This internet policy has been combined with the overall Information Security Policy and as such all users of the internet must make themselves aware of its requirements and ensure they comply with them.

Telephone (&FAX) Usage

Telephone (&FAX) services are available to all Constabulary employees to use for normal business purposes. Both internal and external connections are provided.

On a routine basis, communications will be treated as private (except in the Force Control Room and CMU's where emergency calls are recorded as a matter of procedure). The Constabulary reserves the right, however, to monitor or record any communications system for the purpose of detecting and preventing crime or for detecting the unauthorised use of telecom systems. The interception of any communications system without consent may be employed for purposes of; preventing or detecting crime; detecting the unauthorised use of an electronic communications system; protecting a network against virus or hackers; and combating or investigating fraud or corruption.

Email Usage Policy

Electronic Mail or Email is a range of computer based services that at a basic level facilitate the exchange of typed messages between system users. In addition to the basic message, an Email may also have attached to it other computer files. These attachments may be documents, images or executable computer programmes, (which includes computer viruses).

In Cambridgeshire an internal and external Email service are provided for all employees.

This policy sets out the general rules for the use of Email and identifies a number of constraints and consideration for using Email as a communication medium.

It is important to recognise that Email is subject to the same legal considerations as traditional written material. Particularly in relation to external Email communications, Cambridgeshire Constabulary as well as the provider of the information may be held liable for any breach of the law; particularly regarding breach of confidence, libel, defamation, obscenity, racial or sexual discrimination, copyright and data protection. Users of the Email systems must exercise the same level of discretion in drafting Emails as they would in the creation of any other written document.

The analogy with written documents may also be extended to security. The content of internal Emails is not accessible on a routine basis, however, users must be aware that in exceptional circumstances and following the appropriate authorisations from FEB, mechanisms are available to access Email accounts. Therefore, Email content should not be regarded as completely private, managerial access may be granted if circumstances warrant the disclosure. An individual may voluntarily grant access if they so wish.

Remote access

NOT PROTECTIVELY MARKED

The remote service portal

Access to services on the Constabulary network is usually restricted to users working on workstations at fixed network access points. However in certain circumstances access from remote sites (such as a person's home, or a temporary operational unit) can be provided via a PC, Token and Broadband connection using the Remote Service Portal (RSP)

Who can use the remote access service?

For reasons of cost and security, the remote access service is not generally available to all users. Use is restricted to those staff who demonstrate a clear business need which cannot otherwise be met using the normal access methods.

See the *Remote Access Procedure* for special security rules when using the remote access service.

Home working

For the purposes of this Policy, a *home worker* is any person who undertakes official Constabulary business at home, and who may or may not have remote access to Constabulary IT services via a communications link. See *Remote Access*.

All home workers must be registered with the Information Security Manager

The Constabulary expressly forbids the use of non-Constabulary computers and or networks for official Constabulary business (with the exception of RSP connections), except when authorised by the Information Security Manager.

For further guidance on home working see the *Home Working Procedure*.

Data transfer (virus protection)

All Constabulary ICT systems must be protected against corruption and possible viruses. Data in any format can only be introduced onto the Constabulary network at specific locations and at the discretion of the Network Services Manager.

Third party access

The Constabulary allows access by third parties to its IT network and systems in order that remote diagnostics and emergency fault fixing can take place. Access will be granted only when the third party agrees to work within the limits of the Information Security Policy, and is contractually obliged to do so. It is also a condition of such access being granted that no data files or information relating to policing methods, practices or systems of any kind are downloaded or transferred outside the boundaries of the Constabulary IT network. Any such occurrence may lead to prosecution.

NOT PROTECTIVELY MARKED

For guidance on obtaining permission for third party access, and the controls that need to be in place to protect the Constabulary network, see the *Remote Access (3rd Party) Procedure*.

Disposal of redundant IT equipment and data storage devices

RESTRICTED (or above) information that is no longer required for operational purposes must be disposed of in a manner that precludes any other person recovering the information in a readable format. All redundant IT equipment and media must be disposed of according to the *Data Disposal Procedure*.

It is a disciplinary offence to dispose of information classified as 'RESTRICTED' or above in normal waste bins.

Disaster Recovery Plan

Critical Constabulary business activities must be restored as quickly as possible following a major disaster or computer failure. The Constabulary Disaster Recovery Plan will include an analysis of the risks to the Constabulary, the effects of loss of sensitive information, and plans for recovering essential systems and data to meet requirements of all departments. For each IT service the plan specifies the hardware, network facilities, software and data required to support the Constabulary's business activities for specific periods following a disaster (e.g. after three days, after two weeks and after three months).

Backups

Back-up copies of essential business data and software must be taken in a manner that supports the Disaster Recovery Plan for the Constabulary.

In most cases this activity is carried out by the ICT Services department on the users' behalf. However, where users are required to make their own back-ups, the ICT Services Department will provide suitable training and support.

Systems documentation

All systems documentation which specifies Constabulary IT systems must be protected from unauthorised access.

Copies of the systems documentation must be archived off-site according to the Constabulary *Disaster Recovery Plan*.

Auditing

Auditing of legitimate events and violations must be in place for all systems allowing read/write/amend/delete transactions to be recorded. A range of facilities for analysing Logs must be provided and audit trails must be reviewed to ensure that users are only performing processes that have been explicitly authorised to them.

NOT PROTECTIVELY MARKED

Applications and Development

The development and implementation of applications and systems must be controlled by following development standards and ensuring new applications offer the necessary facilities to allow fully compliance with the policy. The project manager for any new system or application is responsible for all aspects of Information Security in the implementation. This, depending on the scale of the project will include carrying out risk analysis and producing Security Operating Procedures, in accordance with the Force Information Security policy for use in the operation of the system. The project manager will be required to provide progress reports and raise problems with the Information Security Manager. Where a development or implementation of a system, simply cannot meet the requirements of the force Information Security Policy, the project manager and the Information Security Manager, will raise this with the project board. The project board will then have the opportunity to stop the implementation or continue with it, accepting the risks to security involved. Where possible all applications and development work must follow the Applications and Development Procedure. Where possible Developers and Support roles must be kept separate.

Operations

Operator procedures must be formally documented and cover all operator actions. Personnel procedures must be in place to ensure that no undue reliance is placed on any individual. ICT Operators activity must be monitored to minimise accidental errors and malicious actions. The opportunity for misuse of the system by operational staff must be minimised.

Systems Administration Controls.

Formal management responsibilities and procedures are necessary to ensure satisfactory control of all changes to equipment, software, systems or procedures. When changes or updates to operating systems are made, security must be reviewed to ensure that it has not introduced any adverse affects. Access to System Administration accounts, the most powerful accounts on the system, must be tightly restricted on an absolute need to know basis and be consistent with maintenance of the operational service.

Disaster Recover Controls

Recovery plans, for networking, host servers, applications and servers must be in place and securely documented. Suitable backup technology must be used and procedures in place to test regularly these procedures. Business continuity plans must be drawn up by departments and sections and tested regularly.

Inventories

An electronic inventory of all ICT hardware and software (but not furniture or consumables) is held by the ICT Help Desk. All changes to the location and nature of the equipment must be notified to the ICT Help Desk.

NOT PROTECTIVELY MARKED

Media handling

Computer media (including tapes, CD's and printed hard copy) must be used and stored in a safe and secure environment. See the *Information Security Procedure* for further guidance.

Data Protection Act

All persons using Constabulary computer systems must comply with the appropriate registration under the Data Protection Act 1998.

Computer Misuse (Hacking)

Hacking is defined as the unauthorised access, actual or attempted, to a computer program or data.

All staff must note that it is both a disciplinary and a criminal offence to hack into any Constabulary computer system.

Illegal (pirated) software

The use of illegal or pirated software (such as games programs) presents a very high risk to ICT systems and the valuable information stored in them. It is therefore a disciplinary offence to bring unlicensed or illegally obtained software onto the site. It is also a disciplinary offence to copy software belonging to the Constabulary, or licensed by the Constabulary.

Education and training

All Line Managers are responsible for ensuring their staff, suppliers and contractors are aware of the Information Security Policy, and that they understand their responsibilities under the Policy. An Online training package (provided by NCalt), referred to as 'Information Awareness Training' can be found in CamNet on the Professional Standards microsite. All staff must complete the training modules (including Information Security) and note this on their PDR's.