NICR ICT & PHYSICAL SECURITY POLICY

Version 1.4

VERSION CONTROL

No	*Version*	*Description*	*Date*	*Author*
1	1.0	Draft version	Dec 2004	Colin Fox
2	1.1	Added backup procedure to memory stick for laptops	21/03/05	Colin Fox
3	1.2	General review and update	24/07/07	Colin Fox
4	1.3	Title and appendix on physical security updated and the document agreed by IT Manager	12/08/07	Colin R Fox
5	1.4	Mention of TrueCrypt full disk encryption, use of encrypted memory sticks and other minor changes	15/03/10	Colin Fox

ACKNOWLEDGEMENT

The material in this document defines Security Policy in Information and Communications Technology (ICT) security for use throughout the Northern Ireland Cancer Registry, Belfast.

The structure of this document derives from the HPSS ICT Security policy document, which in turn has adopted the structure of British Standard BS 7799 and ISO/IEC 17799:2000 Information Security Management – Part 1: Code of Practice for Information Security Management.

CONTENTS

SUBJECT **PAGE**

1.INTRODUCTION, PURPOSE, SCOPE AND CONFORMANCE

1.1 INTRODUCTION

The 1998 Data Protection Act, which became law on 1 March 2000, makes clear the need for organisations to take steps to ensure that personal data is adequately protected by placing a legal obligation on them to do so.

This security of information can be achieved through technical means, together with appropriate management, procedures and education. Information security management needs, as a minimum, participation by all employees in the organisation.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that the specific security objectives of the NICR are met and that the information NICR systems contain, with particular regard to patient data, is seen only by those entitled to see it.

A number of controls can be considered as guiding principles providing a good starting point for implementing information security.

Controls considered to be essential to an organisation from a legislative point of view include:

a) data protection and privacy of personal information (see 12.1.4).
b) safeguarding of organisational records (see 12.1.3);
c) intellectual property rights (see 12.1.2);

Controls considered to be common best practice for information security include:

a) information security policy document (see 3.1), which is this document;
b) allocation of information security responsibilities (see 4.1.3);
c) information security education and training (see 6.2.1);
d) reporting security incidents (see 6.3.1);
e) business continuity management (see 11.1).

1.2 PURPOSE

The purpose of setting down this policy is to ensure a consistent and high standard of security in the NICR.

The guidance in this document aims to ensure that:-

- information systems used in the NICR are properly assessed for security;
- appropriate levels of security are employed in order to maintain the confidentiality, integrity and availability of information and information systems;
- all staff are aware of the limits of their authority and their accountability;
- a means is established to communicate appropriate and continuing guidance on these issues.

This NICR ICT Security Policy establishes the security principles, procedures and guidelines to be followed.

1.3 SCOPE

This policy applies to the Northern Ireland Cancer Registry but is limited to:

1. The equipment used to store and/or process personal identifiable data
2. The network used for the transmission of personal identifiable data
3. The premises in which the above mentioned equipment and network are installed or used

The network as in point 2. above is the stand-alone network, connecting only the equipment as in point 1. and nothing else.

This policy does not apply to internet connectivity, email usage and security, nor to the equipment/network infrastructure used for such activities; those activities are managed by the Queen's University of Belfast Computer Services.

2 TERMS AND DEFINITIONS

2.1 INFORMATION SECURITY

The purpose of the NICR ICT Security Policy is to preserve:-

- **Confidentiality**: data access is confined to those with specified authority to view the data;
- **Integrity**: all system assets are operating correctly according to specification and in the manner that the current user believes them to be operating;
- **Availability**: information is delivered to the right person as and when needed;

2.2 RISK ASSESSMENT

Risk Assessment may be broken down into four main functions:-

(a) identification of the assets. The assets within the scope of the risk assessment should be checked against an Asset Register;

(b) evaluation of the impact of an adverse event (threat) on the assets. An event does not necessarily have to be a disaster in the normally understood sense, such as a fire. It can also be an event which simply prevents the system from operating for a period of time. This could be machine failure, operator error, malicious interference, or even a quarantining of the computer room during an investigation for Legionnaire's Disease;

(c) assessment of the likelihood of the adverse event occurring. There can be a tendency to underestimate the likelihood of an event occurring. Fire and

malicious infiltration, such as hacking or burglary, could be likely, irrespective of the location of the assets;

(d) identification of appropriate countermeasures to protect the asset and/or limit the damage caused by an event;

2.3 RISK MANAGEMENT

Having assessed the levels of risk, risk management identifies the protective measures that could be applied to reduce the risks to acceptable levels. CRAMM is the Risk Analysis and Management Methodology preferred by OGC for use in the UK public sector method for assessing and managing such risks.

3 SECURITY POLICY

3.1 INFORMATION SECURITY POLICY

The purpose of an information security policy is to provide management direction and support for information security. Management must set a clear policy direction and demonstrate support for, and commitment to information security through the issue and maintenance of an information security policy across the organisation.

3.1.1 ICT security policy document

This is the ICT security policy document that you are reading. An integral copy of this document is communicated, as appropriate, to all employees in the NICR with ICT duties. A shortened version of this document, in a form that is relevant, accessible and understandable to the intended readers, is communicated to all other members of NICR staff and temporary users of NICR equipment. The integral copy is always available for consultation to all members of staff.

At its highest level, the NICR ICT Security Policy contained in this document is set out below:-

> The NICR Director must direct and make certain that effective information systems security procedures are implemented which ensure that access to information is restricted to those staff who have a legitimate need for it, and that the information itself is appropriately stored and safeguarded.
>
> In discharging these duties, the NICR must:
>
> - nominate an officer to have day-to-day responsibility for ICT security (the ICTSO);
> - develop an ICT Security programme based on a realistic assessment of risk and impact;
> - implement effective mechanisms for regularly monitoring and reviewing ICT security and the ICT security programme;
> - ensure that staff receive appropriate ICT security training in order that all actions by individuals when interacting with information systems conform to this policy, to NICR ICT security standards and to legal requirements;
> - maintain an up-to-date Asset Register to hold details of all the items of hardware and software that make up the organisation's information systems;
> - develop, test and maintain a contingency plan or plans to allow continued business operation in the event of a disaster;
> - take care to ensure that no information, especially personal information, is disclosed to persons not authorised to see it;
> - ensure that the organisation uses no illegal software;
> - implement and follow procedures to ensure that all computers, including laptops and handheld devices such as P.D.A.s, are protected from malicious code such as viruses;
> - ensure that the security of the network is not put at risk through the establishment of non-authorised external connections to individuals, organisations or networks;

- ensure that all ICT equipment is properly maintained with specific reference to the application of security patches issued by suppliers to counter identified vulnerabilities;
- report ICT security breaches in accordance with standard procedures.

4 ORGANISATIONAL SECURITY

4.1 INFORMATION SECURITY INFRASTRUCTURE

4.1.1 Management information security forum

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

4.1.2 Information security co-ordination

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

4.1.3 Allocation of information security responsibilities

The *NICR ICT Security Policy* sets out the responsibilities for ICT security in the NICR as follows:-

- The ICT Manager (ICTM) has overall responsibility for ICT security within the NICR;
- Day-to-day responsibility for ICT security is delegated to the ICT Security Officer (ICTSO). This role must be filled by someone with sufficient authority, and with direct open support from senior management, to ensure that appropriate security-related measures are adopted and enforced throughout the organisation.
- All managers and staff developing, introducing, managing or using information systems also have a responsibility for the security of those systems.

4.1.3.1 Director

This post is ultimately responsible for:-

- nominating an ICT Security Officer to have responsibility for implementing and monitoring ICT Security Policy and to carry out the day-to-day tasks of promoting and monitoring ICT security;
- ensuring that all information systems in use are appropriately assessed for security and are protected in accordance with the ICT Security Policy;

4.1.3.2 ICT Security Officer (ICTSO)

This post is intended to provide a focus for all ICT security issues and the day-to-day monitoring of the ICT Security programme to implement, monitor and maintain the ICT Security Policy.

- The ICTSO is consulted as soon as possible following a suspected security incident.

ICTSO is responsible to the Director

for:-

- providing a focus within the NICR on all ICT security matters;
- co-ordinating ICT security matters across departmental and system boundaries within the NICR;
- playing a proactive role in establishing and implementing an ICT Security programme;
- taking the lead in monitoring the effectiveness of ICT security policy, standards, procedures and guidelines within the NICR;
- ensuring compliance with legislation, including the Data Protection Act (1998);
- receiving and considering reports of ICT security incidents;
- ensuring that agreed recommendations emerging from risk analyses are implemented;
- ensuring that follow-up security reviews are carried out regularly or when there are system or installation changes;
- promoting ICT security awareness throughout the NICR;
- helping to identify appropriate ICT security training for staff within the NICR;
- responsible for ensuring that appropriate Contingency arrangements are in place for the local network.

4.1.4 Authorisation process for information processing facilities

During development and procurement of information processing facilities, ICT Security must be considered, with particular reference to network requirements especially remote support services.

There is a requirement for the establishment of an authorisation process for new information processing facilities. Before authorisation of new information processing facilities:-

- New facilities should have appropriate user management approval authorising their purpose and use. Approval should also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;
- Where necessary, hardware and software should be checked to ensure that they are compatible with other system components.
- The installation of new hardware and software should be documented.

4.1.5 Specialist information security advice

The ICT Security Officer co-ordinates in-house knowledge and experiences to ensure consistency and provide help in security
decision making. Where applicable they should have access to suitable external advisors to provide specialist advice outside their own experience. In the majority of cases this role will be carried out by the relevant ICT Security Officer (see 4.1.3.2)

4.1.6 Co-operation between organisations

Appropriate contacts with law enforcement authorities, regulatory bodies, information

service providers and telecommunications operators should be maintained to ensure that appropriate action can be taken quickly and advice obtained in the event of a security incident.

Exchanges of security information should be restricted to ensure that confidential information is not passed to unauthorised persons.

4.1.7 Review of information security

This ICT Security Policy sets out the policy and responsibilities for information security. Its implementation should be reviewed to provide assurance that NICR working practices properly reflect the policy and that the policy is feasible and effective. Such a review may be carried out by the internal audit function or a third party organisation specializing in such reviews, using this document as a review template.

4.2 THIRD PARTY ACCESS

No third party network connection to the NICR Information System is allowed.

4.2.1 Identification of risks from third party access

Third party access should be permitted only via the infrastructure managed by NICR. Researchers wishing to access the NICR Information System should contact the NICR ICTM so that discussions on the feasibility in obtaining such access can be started as soon as possible.

4.2.2 Security requirements for third party access

Third party individuals will be required to comply with the principles established within this ICT Security Policy.

5 ASSET CLASSIFICATION AND CONTROL

5.1 ACCOUNTABILITY OF ASSETS

5.1.1 Inventory of assets

An inventory of the major assets associated with the NICR information System is stored on a regularly backed up QUB networked folder and maintained by administrative staff.

The inventory identifies each asset and its ownership. Assets include:-

- information;
- software;
- physical assets.

5.2 INFORMATION CLASSIFICATION

5.2.1 Classification guidelines

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

5.2.2 Information labelling and handling

Sensitive information should be labelled appropriately and output from systems handling such data should carry an appropriate classification label (in the output). The marking should reflect the classification of the most sensitive data in the output. Output includes printed reports, removable media, electronic messages and file transfers.

See also 7.2.6 and 8.6.2 which deal with the disposal of equipment and media that have been used to store sensitive information.

6 PERSONNEL SECURITY

The essence of this section is the duty of the NICR, within reasonable parameters, to reduce the risks of human error, theft, fraud or misuse of facilities.

6.1 SECURITY IN JOB DEFINITION AND RESOURCING

6.1.1 Including security in job responsibilities

Staff job definitions should include any responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of ICT assets or for particular security processes or activities. Management should ensure that for definitions of job responsibilities and working practices, the following apply:-

- Each member of staff is personally accountable for the function he/she performs. If accountability is shared, it may be impossible to enforce disciplinary action.
- Where work is critical to the organisation, it is essential that it can be taken over by someone else in the event of unavailability. Documentation reduces the risk of reliance on key staff.
- Each individual should know the extent of his/her own authority. This will range from responsible tasks they may perform to budgetary responsibilities.
- Security privileges and access rights must be allocated based on the requirements of the user's job rather than on a status basis. For example, the Director may have no requirement to enter the computer room, so should not necessarily be given those access rights.
- It may be necessary to require employees to declare personal interest. For instance, an individual working in ICT procurement should make it known if he/she or any close relative has direct interest in a potential supplier.
- Contract staff at any level should be subject to the same disciplines relating to security as full time members of staff. Where their work relates directly to sensitive security issues, for example, computer maintenance staff, extra conditions may have to be imposed according to the risk exposure.
- Where necessary, requests for recruitment references for ICT users (technical or end users) may need to make particular reference to ICT security.

6.1.2 Personnel screening and policy

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

6.1.3 Confidentiality agreements

Personal data held in NICR information systems are safeguarded by the Data Protection Act 1998 which places obligations on those who record or use such information. In addition, health professionals have ethical duties to maintain the confidentiality of data relating to their patients or clients.

6.1.4 Terms and conditions of employment

Conformance to this ICT Security Policy is

part of the NICR's terms and conditions of employment including those that apply to part-time, temporary, contract or agency staff or any others who may have access to the organisation's information, applications, systems or networks.

6.2 USER TRAINING

6.2.1 Information security education and training

ICT security is largely dependent on personnel. For this reason, staff awareness and training are crucial if ICT security is to be effective. The NICR must ensure that:-

(a) staff with access to information systems are adequately trained in their security related roles and responsibilities and in the correct use of those systems;

(b) staff with access to information systems are kept aware of the ICT Security Policy and of relevant standards and procedures.

In addition, all NICR staff must be given appropriate ICT security training in order to ensure that all actions by individuals when interacting with information systems conform to the policy, to NICR ICT security standards and to legal requirements.

Management should ensure that for induction training the following apply:-

- ICT users are, according to their responsibilities, briefed on:-
  - The NICR ICT Security Policy (this document);
  - the Computer Misuse Act;
  - the Data Protection Act;
  - conduct and disciplinary procedures which may be invoked should a breach of security arise.

- For critical systems training should be given to at least two people so that if one is absent the activity can be performed by the other.
- Contract staff should receive equivalent induction training and sign an agreement to abide by the same codes of conduct and discipline as permanent staff. Where contract staff are taken on through a private firm or agency, this condition should form part of the contract of engagement.

6.3 RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS

6.3.1 Reporting security incidents

While the reason for having ICT security is to prevent, as far as possible, security breaches from occurring, it must be recognised that breaches do occur from time to time.

Details of real or suspected ICT security incidents should be reported immediately, by using the *Security incident form* in Appendix, to the ICT Security Officer who will take whatever action is.

6.3.2 Reporting security weaknesses

Users of information services are required to report any observed security weaknesses in, or threats to, information systems. The weaknesses should be reported, through management and using the *Security incident form* in Appendix, to the ICT Security Officer. Users should not, in any circumstances, attempt to prove a suspected weakness as this could be interpreted as potential misuse of the system.

6.3.3 Reporting software/hardware malfunctions

Users of information services are required to report any observed software and hardware malfunctions in, or threats to, information systems. The weaknesses should be reported, through management and using the *Hardware Fault Form* or the *Software Error Form* in Appendix, to the ICT Security Officer. Users should not, in any circumstances, attempt to prove a suspected software malfunction as this could be interpreted as potential misuse of the system.

6.3.4 Learning from incidents

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

6.3.5 Disciplinary process

[This element of ISO 17799 is deliberately left blank since it falls in the scope of the Queen's University Belfast ICT Security Policy.]

7 PHYSICAL AND ENVIRONMENTAL SECURITY

7.1 SECURE AREAS

7.1.1 Physical security perimeter

Physical security protection should be based on defined perimeters and achieved through a series of strategically located barriers throughout the organisation. Critical installations must be protected by, at least, lock and key.

The requirements and siting of each physical barrier should depend on the value of the assets and services to be protected, whilst considering the associated security risks.

Important or particularly sensitive computer areas need to be protected by locks with codes which can be changed periodically.

7.1.2 Physical entry controls

Where an area is designated as a secure area appropriate entry controls should be employed in order to ensure that access is restricted to authorised personnel only:-

- visitors should be supervised, they should be granted access for specific, authorised purposes only;
- staff with visitors should, if appropriate, ensure that they are accompanied throughout the visit;

Except in places of public access, staff should be instructed to challenge strangers. Staff should be aware of visitors who are unaccompanied, such people should be approached politely, to determine their business.

Only those staff whose jobs require it should be allowed to enter areas where computer systems are located. In addition to the risk of theft, damage or unauthorised use, data security could be compromised and passwords may become known.

7.1.3 Securing offices rooms and facilities

For the purposes of information security this refers to secure computer rooms and rooms containing communication equipment. The selection, design and position of such areas should take account of the possibility of damage from fire, flood, explosion, civil unrest and other forms of natural and man-made disaster. Such areas should also comply with relevant health and safety regulations and standards.

In general, key computer rooms and communications rooms should be sited to avoid unauthorised public access. Such rooms should be unobtrusive and give minimum indication of their purpose with no obvious signs identifying the presence of information processing activities. Doors and windows should be locked when unattended.

Contingency equipment and back-up media should be sited at a safe distance to avoid damage from a disaster at a main computer or communications site.

7.1.4 Working in secure areas

Additional controls and guidelines are required to enhance the security of secure areas as defined in the previous section. This includes controls for the personnel and third party personnel working in the secure area in addition to third party activities being undertaken there.

Unsupervised working in secure areas should be monitored for safety reasons and to prevent opportunities for malicious activities. Vacant secure areas should be locked and periodically checked. Third party support services personnel should be granted restricted access to secure areas only as required. Such access should be authorised and monitored.

7.1.5 Isolated delivery and loading areas

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

7.2 EQUIPMENT SECURITY

7.2.1 Equipment siting and protection

In order to prevent loss, damage or compromise of assets and interruption of core activities, equipment should be physically protected from security threats and environmental hazards and also protected against unauthorised access to data.

Computer environments, including temperature, humidity and power supply quality, should be monitored where necessary. Monitoring will identify conditions which might adversely affect the operation of the computer equipment to enable any corrective action to be taken. It should always be carried out in accordance with manufacturers' recommendations.

Eating and drinking are discouraged in areas housing computer equipment.

7.2.2 Power supplies

Critical equipment should be protected from power failures or other electrical anomalies. A suitable electrical supply, conforming to the equipment manufacturer's specifications should be supplied. Consideration should be given to using a standby power supply. An uninterruptible power supply (UPS) is required for equipment supporting critical business operations. As a minimum, a device protecting against power supply fluctuations should be fitted. Emergency lighting should be provided in case of main power failure.

7.2.3 Cabling and Wireless LANs Security

7.2.3.1 Cabling Security

Power and telecommunications cabling carrying data or supporting ICT services should be protected from interception or damage. Power and telecommunications lines into ICT facilities should be underground where possible, or subject to adequate alternative protection. Network cabling should be protected from unauthorised interception or damage by using conduits, or by avoiding routes through public areas. Power cabling should be segregated from communications cabling to prevent interference.

7.2.3.2 Wireless LANs Security

Wireless LANs are not allowed in the NICR.

7.2.4 Equipment maintenance

On-going maintenance arrangements (defining level of maintenance and minimum levels of performance) should be the subject of contractual agreement. If any equipment need not be maintained (as it may be cheaper to replace it) the decision process should include an impact analysis of the loss of availability.

A record of faults or suspected faults should be maintained.

Only approved systems engineers should be allowed access to hardware or software. Where possible systems engineers should be escorted and supervised while on site. The systems engineer should, if possible, be escorted in and out of the building and the user, or a representative of the user, should be present during the maintenance or repair operation.

Where possible, diagnostic tools for use by a supplier's staff should be obtained from the supplier and kept on site for use by systems engineers as necessary. As these disks may contain powerful access or monitoring software such disks should be kept securely for use only by authorised staff.

The system security policy (10.1.1) should state whether, and if so which, disks must not be moved from official premises for maintenance or repair. Equipment with accessible data on a hard disk should only be sent for maintenance elsewhere after careful consideration. The sensitivity of the data and the consequences of its disclosure must be weighed against the need for the equipment to be repaired, rather than disposed of and replaced. Whether or not a hard disk containing data may be moved from official premises for repair should always be documented in the system security policy and the system secure operating procedures (8.1.1)

Where a disk is to be removed from the premises for repair, where possible, the data should be over-written. Simply deleting data from disks is not adequate and is therefore unsuitable for removing sensitive information. Computer hard disks may be over-written with random data an the use of specialised software, such as 'Eraser', is recommended. "Delete", "erase" and "formatting" are all processes that can be reversed and are therefore not suitable mechanisms for removing data.

7.2.5 Security of equipment off-premises

Equipment, data or software should not be taken off-site without documented (signed)

management authorisation.

No sensitive data (as defined under the Data Protection Act (1998)) may be stored on portable computers unless protected by encryption. Full disk encryption and individual encrypted folders, placed on the account's desktop, should be used to protect all sensitive data (see *Appendix F - Sensitive Information Labelling and Handling Procedures*). Even with password-protected screensavers and boot-up passwords it is not possible to wholly guard against information on local hard disks being accessed by unauthorised users.
Portable computers should not be left unattended in public places. Portable computers are very vulnerable to theft, loss or unauthorised access when travelling. The high incidence of car theft makes it inadvisable to leave equipment or media in a car - even in a locked boot.

The user must be responsible for ensuring that no unauthorised person has access to the computer while it is outside official areas (this includes access by family members or others if the computer is used at home) and that the computer is never connected to any network other than the NICR internal network (this includes home networks and dial-up internet connections). Built-in wireless network adapters and modem devices should be disabled by an administrator.

More information about other aspects of protecting mobile equipment can be found in 9.8.1 and in the Appendices.

7.2.6 Secure disposal or re-use of equipment

If a machine has ever been used to process personal data as defined under the Data Protection Act (1998) or confidential data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal must be documented. The whole disk should be over-written with randomly generated characters using software designed for this purpose (see 7.2.4).

If a hard disk cannot be over-written it should be destroyed.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk. Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software.

See also 8.6.2 which deals with the disposal of media.

7.3 GENERAL CONTROLS

General controls exist to prevent compromise or theft of information and information processing facilities. Information and information processing facilities should be protected from disclosure to, modification of, or theft by unauthorised persons. Controls should also be in place to minimise loss or damage.

7.3.1 Clear desk and clear screen policy

ICT users should observe a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorised access, loss of, and damage to information during and outside normal working hours.

Information left out on desks is also likely to be damaged or destroyed in a disaster such as a fire, flood or explosion.

The following controls should be considered.

(a) Where appropriate, paper and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.

(b) Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.

(c) Computers and printers should not be left logged on when unattended and should be protected by key locks, passwords or other controls when not in use.

(d) Incoming and outgoing mail points and unattended fax and telex machines should be protected.

(e) Photocopiers should be locked (or protected from unauthorised use in some other way) outside normal working hours.

(f) Sensitive information, when printed, should be cleared from printers immediately.

7.3.2 Removal of Property

Equipment, information or software should not be taken off site without proper authorisation. Where necessary and appropriate, equipment should be logged out and logged back in when returned.

8. COMMUNICATIONS AND OPERATIONS MANAGEMENT

8.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

The establishment of operational procedures and responsibilities ensure the correct and secure operation of information processing facilities. This includes the development of appropriate operating instructions and incident response procedures.

8.1.1 Documented operating procedures

Documented secure operating procedures should be produced for each significant new or replacement application system. The purpose of such documentation is to specify the rules necessary to meet security requirements. For example, it may be that the system security policy might specify that the computer needs to be kept in a room that is locked during silent hours and the secure operating procedures will state who will be responsible for locking and opening the room, where the key is to be held and the times the room is open.

The secure operating procedures should contain at least the following:-

(a) Introduction and description of system;

(b) Responsibilities - outline statements of responsibilities for at least:-

- system security and accountability;
- staff conduct and discipline;
- system management and administration;
- security administration;
- ICT Security Officer role;
- system user authority.

Other aspects may include:-

- third party maintenance of the system (both hardware and software);
- external visitors (including rules for disclosure of data).

(c) Timings of security operations - the timing and frequency of security operations which are appropriate to each user or supporter of the system. For example a file containing volatile records requiring high availability may require back-ups to be taken daily, whereas it may be deemed sufficient to test a contingency plan once a year.

(d) Procedures for:-

- The confidentiality of the system to be protected to the correct level, i.e. the information it contains should be seen only by those people authorised to see it;
- building access control;
- computer area/office access control;

- physical and logical access control to the system, software and data. The type of access to data and software (i.e. read-only, update, delete) should be based on business requirements. There is often a tendency to assume that a hierarchy of staff implies a hierarchy of user access permissions, with the more senior people having more powerful access rights. This will only be the case where the system demands a hierarchical system of user profiles/access rights. Senior staff will often require a broader scope of access, but at a much less detailed level than most junior staff;
- protecting integrity. The integrity of the system should be protected to the correct level, i.e. the accuracy of the data should be safeguarded against accidental or deliberate corruption. Where personal information is involved it is a legal requirement under the Data Protection Act (1998) that the data "shall be accurate and, where necessary, kept up to date";
- protecting availability. The availability of the system should be protected to the correct level, i.e. the data should be available for access by authorised people whenever required. Where service level agreements are in place they will dictate the necessary minimum and desirable service levels. The measures taken will depend on the criticality of the system, but certain baseline precautions should always be implemented;
- incident reporting. The procedures for notifying any security breaches should be specified here. There is no need to include procedures for investigating and rectifying any reported breach as these are likely to be different in each case. However, this section should specify who is to be responsible for such action;
- compliance monitoring. Where the criticality or sensitivity of the system requires it, formal regular, documented monitoring of each procedure defined in this section should be undertaken.

The secure operating procedures should be reviewed and maintained regularly. The document should be kept up-to-date. Significant changes to the system will always warrant a review. In the absence of these, it should be reviewed annually. Staff should be encouraged to report any weaknesses they see in security procedures to the ICT Security Officer.

Clear documented operating procedures should be prepared for the operation of all application systems to ensure their correct, secure operation.

The procedures should specify the correct instructions for the detailed execution of each job including, as appropriate, the following items:-

- the correct handling of data files;
- instructions for handling errors or other exceptional conditions which might arise during job execution, including restrictions on the use of system utilities and secure disposal of output from failed jobs;
- support contacts in the event of unexpected operational or technical difficulties;
- special output handling instructions such as the use of special stationery;
- system restart and recovery procedures for use in the event of system failure.

Documented procedures should be prepared for system housekeeping activities associated with computer and network management, such as computer start-up and close down procedures, data back-up, equipment maintenance, computer room management and safety.

Operating procedures should be treated as formal documents, changes to which should only be made after approval by authorised management.

8.1.2 Operational change control

Changes to information processing facilities and systems should be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. System security can be compromised by changes which are made before or after the system has gone live. The ICT Manager is responsible for ensuring that changes do not alter, degrade or compromise:-

- security controls;
- access rights;
- audit and security software.

8.1.3 Incident management procedures

Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents (see also 6.3.1). The following controls should be considered.

(a) Procedures should be established to cover all potential types of security incident, including:

(1) information system failures and loss of service;
(2) denial of service;
(3) errors resulting from incomplete or inaccurate business data;
(4) breaches of confidentiality.

(b) In addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures should also cover (see also 6.3.4):

(1) analysis and identification of the cause of the incident;
(2) planning and implementation of remedies to prevent recurrence, if necessary;
(3) collection of audit trails and similar evidence;
(4) communication with those affected by or involved with recovery from the incident;
(5) reporting the action to the appropriate authority.

(c) Audit trails and similar evidence should be collected (see 12.1.7) and secured, as appropriate, for:

(1) internal problem analysis;
(2) use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
(3) negotiating for compensation from software and service suppliers.

(d) Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures should ensure that:

(1) only clearly identified and authorised staff are allowed access to live systems and data (see also 4.2.2 for third party access);
(2) all emergency actions taken are documented in detail;
(3) emergency action is reported to management and reviewed in an orderly manner;
(4) the integrity of business systems and controls is confirmed with minimal delay.

8.1.4 Segregation of duties

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.1.5 Separation of development and operational facilities

In cases where software is developed in-house, to reduce the risk of accidental changes or unauthorised access to operational software and business data, development and operational facilities should be separated. Otherwise development and testing activities may cause unintended changes to software and data sharing the same computing environment.

The following controls should be considered:-

- development and operational software should, where possible, run on different processors, or in different domains or directories;
- development and test work should be separated from each other as far as possible;
- compilers, editors and other system utilities should not be stored alongside operational systems, when not required.

8.1.6 External facilities management

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.2 SYSTEM PLANNING AND ACCEPTANCE

8.2.1 Capacity planning

Capacity demands should be monitored and, where applicable, procurement procedures should, if appropriate, provide for an acceptable level of spare capacity.

Spare capacity should be measured in terms of sufficient additional equipment to back up failed equipment, or sufficient equipment to allow a system adequate spare time to recover from processing delays. Projections of future capacity requirements for both new and existing systems should be made to ensure that adequate processing power and storage remain available.

8.2.2 System acceptance

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.3 PROTECTION FROM MALICIOUS SOFTWARE

8.3.1 Controls against malicious software

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software should be based on security awareness, appropriate system access and change management controls.

Some controls that should be considered are:

a) a formal policy requiring compliance with software licences and prohibiting the use of unauthorised software (see 12.1.2.2);
b) a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken (see also 10.5, especially 10.5.4 and 10.5.5);
c) installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis;
d) conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorised amendments should be formally investigated;
e) appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements (see clause 11);

8.4 HOUSEKEEPING

8.4.1 Information back-up

All data and system configuration of the main NICR servers is protected by clearly defined and controlled back-up procedures, which generate data for archiving and contingency recovery purposes. Back-up instructions and procedures are in Appendix E, where labelling, in-site and off-site storage and management of the backup tapes are specified

There are no automatic backup procedures in place for information stored locally on client computer hard disks. As a result, staff must make their own arrangements to secure locally-held data. See Appendix F for good practice data backup.

Archived and recovery data should be accorded the same security as live data and should be held separately at an off-site location. (Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes).

Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested to ensure that, in an emergency, the back-up data is sufficient and accurate. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

Recovery data should be used only as defined in the documented contingency plan for the system. If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

8.4.2 Operator logs

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.4.3 Fault Logging

All hardware and software faults, or suspected faults, should be logged. The log should contain at least:-

- software or hardware identification;
- date, time and description of the fault;
- remedial action;
- date and time repaired/replaced.

8.5 NETWORK MANAGEMENT

8.5.1 Network controls

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.6 MEDIA HANDLING AND SECURITY

8.6.1 Management of removable computer media

All essential media should be replaced in a safe secure environment after use. Any temporary storage media must also be protected if they may contain sensitive information. Sensitive or important files should be put back into protected storage as quickly as possible.

Files such as key back-up copies are only useful once they are in the fire-proof safe, or off-site. An unauthorised person should not be able to identify data from the label on the medium itself. A data storage system that avoids the use of descriptive labels on the physical media should be used.

8.6.2 Disposal of media

All hard disks should be reformatted prior to disposal. If a hard disk cannot be re-formatted and the data is innocuous (for example, publicly available) no action need be taken. If, however, there is any possibility that the data may contain sensitive or valuable information, then the disk should be erased as per section 7.2.6.

Prior to being discarded, all removable storage media which may contain sensitive or valuable information should where possible be erased or by other means rendered unusable. Media to be degaussed or otherwise destroyed should be held securely until collected. If no other secure method of disposal is available, it will be necessary to consider incineration of the media or indefinite keeping of the media within the secure area of the NICR.

See also Section 7.2.6 which deals with the secure disposal of equipment. See also Appendix F for relevant procedures.

8.6.3 Information handling procedures

Procedures should be drawn up for handling information consistent with its classification (see 5.2) in documents, computing systems, networks, mobile computing and any other sensitive items e.g. with regard to the latter, there should be documented procedures for controlling stationery having a potential value, such as payment stationery and order forms.

8.6.4 Security of system documentation

All systems should have associated documented procedures which must be kept up to date so that they match the state of the system at all times. In addition, classified systems should have individual system security policies. System documentation should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a location which will remain secure, even if the computer system and all other copies are destroyed. Distribution of system documentation should be formally authorised by the ICTM.

8.7 EXCHANGE OF INFORMATION AND SOFTWARE

8.7.1 Information and software exchange agreements

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.7.2 Security of media in transit

Reliable transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturers' specifications. A list of authorised couriers, and a procedure for their identification, should be established. Special measures should be adopted, where necessary, to protect sensitive information from unauthorised disclosure or modification, for example, locked containers.

8.7.3 Electronic commerce security

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

8.7.4 Security of electronic mail

Patient identifiable data must never be sent by email.

8.7.5 Security of electronic office systems

Electronic office systems provide opportunities for faster dissemination and sharing of business information. Clear policies and guidelines should control the business and security risks associated with them.

Requirements to be addressed include:-

- the possible need to exclude any sensitive business information, if the system security does not provide an appropriate level of protection;
- the possible need to restrict access to information relating to selected individuals;
- the categories of staff, and of contractors or other third parties, that are allowed to use the system, and the locations from which it may be accessed.

8.7.6 Publicly available systems

No material of a sensitive nature may be posted or transmitted via the Internet.

The Data Protection Act 1998 regulates what may be done with personal data. It reinforces other legal constraints on the use and disclosure of personal data; for example when data is held under an obligation of confidence, such as medical records.

The risk of contravening the Act or other legal constraints, such as libel, is likely to be increased if the Internet is used as a means of providing access to or communication of personal data. The business sensitivity too of data must always be recognised and staff must understand that publishing, or transmitting information on the Internet is akin to publishing it in a national newspaper.

8.7.7 Other forms of information exchange

Procedures and controls should be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.

9 ACCESS CONTROL

9.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL

9.1.1 Access control policy

9.1.1.1 Policy and business requirements

Business requirements for access to systems should be defined and documented. The documentation must clearly define the access rights of each user or group of users. The access rights should take account of:-

- the security requirements of the system;
- policies for information dissemination and entitlement, for example, the "need to know" principle.

9.1.1.2 Access control rules

In specifying the access control rules, care should be taken to consider the following:

a) differentiating between rules that must always be enforced and rules that are optional or conditional;
b) establishing rules based on the premise "What must be generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";
c) changes in information labels (see 5.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
e) rules which require administrator or other approval before enactment and those which do not.

9.2 USER ACCESS MANAGEMENT

9.2.1 User registration

A formal process to manage users' access rights should be established (see details in Appendix B). Any alterations to the process should still ensure that access rights are reviewed regularly and that authorisation for special privileged access rights is reviewed more frequently. The altered process should also:-

- check that each user has authorisation from the ICTM to use the service;
- check that the level of access is appropriate for the business purpose and is consistent with organisational security policy;
- ensure that service providers do not provide access until the authorisation process has been completed;
- maintain a formal record of all persons registered to use the service;
- immediately change or remove the access rights of users who have changed jobs or left the organisation;

- periodically check for, and remove, redundant user-ids and accounts that are no longer required;
- ensure that redundant user-ids are not re-issued to another person.

9.2.2 Privilege management

The use of privileges must be restricted and carefully controlled. For multi-user systems, the allocation of privileges should be controlled through a formal authorisation process, which should:-

- identify the privileges associated with each system product (for example, operating system, database management system) and the categories of staff to which they need to be allocated;
- allocate privileges to individuals on a "need to use" basis and on an "event by event" basis - i.e., the minimum requirement for their functional role and only when needed (with particular attention to permissions on when the user can logon to the system, from what workstations and to what operations he/she can perform on what data)
- maintain a record of all privileges granted. Privileges should not be granted until the authorisation procedure is complete;
- ensure that any user assigned special privileges for a particular purpose uses a different user identity from that used for normal business purposes and is allocated a "one-off" password, which is deleted after use.

"Privileges" are those such as are allowed to the system manager or systems programmers, allowing access to sensitive areas (for example, passwords). The unnecessary allocation and use of privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached.

Certain individuals such as those who provide support are frequently supplied with "administrative" privileges. Such privileges may enable those staff to have unfettered access to software and data. Consequentially, it must be brought to the attention of those individuals that being granted such privileges brings the need for them to be particularly vigilant in the exercise of their duties and their responsibility in protecting such software and data from unauthorised access. Owners of the data should also be made aware of the privileges afforded to such support staff so that they may take appropriate action.

9.2.3 User password management

The allocation of passwords should be controlled through a formal management process. All new users must be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected. Passwords are an effective ICT security countermeasure only if they can be kept secret. If compromised, passwords can be misused for a long period without detection. Passwords must always be treated as though they are classified at the level of the most sensitive data held on the system to which they allow access.

Where temporary passwords are known to the systems administrator or network manager (for example, on granting access to new users), the user should change the password immediately on receipt. Temporary passwords provided when users forget

their password should only be supplied following positive identification of the user. Where a temporary password is defined for an authorised user, for a trouble-shooting session for example, the password should be deleted at the end of the session. This deletion should, preferably, be automated, and should depend on the expiry of a pre-defined time period.

Passwords should never be stored on computer system in an unprotected form. Passwords must not be displayed on screens as they are entered and should be held on computer systems in one-way encrypted form.

9.2.4 Review of user access rights

To maintain effective control over access to data and information services, management should conduct a formal process at regular intervals to review users' access rights so that:

a) users' access rights are reviewed at regular intervals (a period of 6 months is recommended) and after any changes (see 9.2.1);
b) authorisations for special privileged access rights (see 9.2.2) should be reviewed at more frequent intervals; a period of 3 months is recommended;
c) privilege allocations are checked at regular intervals to ensure that unauthorised privileges have not been obtained.

9.3 USER RESPONSIBILITIES

9.3.1 Password use

Where passwords are in place, users should follow good security practices in the selection and use of passwords (see also Appendix C)

Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services. All users are advised to:

a) keep passwords confidential;
b) avoid keeping a paper record of passwords, unless this can be stored securely;
c) change passwords whenever there is any indication of possible system or password compromise;
d) select quality passwords with a minimum length of eight characters which are:
    1) easy to remember;
    2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
    3) free of consecutive identical characters or all-numeric or all-alphabetical groups.
e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;
f) change temporary passwords at the first log-on;
g) do not include passwords in any automated log-on process, e.g. stored in a macro or function key;
h) do not share individual user passwords;

i) do not logon on behalf of anybody else.

If users need to access multiple services or platforms and are required to maintain multiple passwords, they should be advised that they may use a single, quality password [see d) above] for all services that provide a reasonable level of protection for stored password.

Where fingerprint logon is in place, users are advised to

a) never logon on behalf of anybody else;
b) rub their finger on the sensor, once their logon has been successful, to destroy any latent image of their fingerprint on the surface of the device.

Additional instructions and procedures are in Appendix H

9.3.2 Unattended user equipment

Inactive computers should be set to time out after a pre-set period of inactivity. The MS Windows screensaver must be implemented on all computers and must be set so that they will automatically be invoked no later than 15 minutes after the last keystroke or mouse movement. Screensavers must be fingerprint protected (see Appendix H)

Computers left unattended out of office hours or during planned absences exceeding 2 hours must be logged out of the Network or shut down. The users should not leave the workstation until they have visual confirmation of the logoff/shut down. Because of the ease with which they can be removed portable computers, including PDAs, should be locked away when not in use for periods exceeding 4 hours.

Staff carrying or using computers off the Organisation's premises must take all reasonable steps to guard against their theft, loss or damage, and against unauthorised use

Assignment of Portable Computers

No computer may be removed from the premises of the NICR unless authorised and recorded.

Portable computers are assigned to members of staff who require them for fulfilling their duties. The assignment is recorded. The assigned equipment must be returned by the agreed date (if any) and must not be passed on to any other person.

Portable computers should be returned to the NICR premises and connected to the network at least once a month, in order to perform a backup to the server of the collected/updated data and to allow the antivirus software to be automatically updated. At the end of each working day a backup to a memory stick should be performed. The procedure specified in Appendix E should be followed, in order to retain the encryption of the files on the removable medium.

9.4 NETWORK ACCESS CONTROL

Access to the networked services should be controlled. This is necessary to ensure that users who have access to network services do not compromise the security of these network services. The following must be considered:

a) appropriate authentication mechanisms for users and equipment;
b) control of user access to information services.

See appendix B for details.

9.4.1 Policy on use of network services

Any system connected to the NICR network must be managed in accordance with guidelines contained in this policy. This includes appropriate access and change control procedures.

9.5 OPERATING SYSTEM ACCESS CONTROL

Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following:

a) identifying and verifying the identity, and if necessary the terminal or location of each authorised user;
b) recording successful and failed system accesses;
c) providing appropriate means for authentication; if a password management system is used, it should ensure quality passwords [see 9.3.1 d];
d) where appropriate, restricting the connection times and/or locations of users.

Other access control methods, such as challenge-response, are available if these are justified on the basis of business risk.

9.5.1 Automatic terminal identification

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

9.5.2 Terminal log-on procedures

Access to ICT services should be via a secure log-on process, designed to minimise the opportunity for unauthorised access. The log-on process should:-

- not display system or application identifiers until log-on has been successfully completed;
- ideally display a general notice warning that the computer should only be accessed by authorised users and that access by unauthorised users may constitute an offence under the Computer Misuse Act, for which they may be prosecuted;
- not provide, during log-on, help messages that would aid an unauthorised user; validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

- limit the number of unsuccessful log-on attempts allowed to three (3), where passwords are in place, or twenty (20), where fingerprints are used. After which the following actions should take place:--
    - the unsuccessful attempt is recorded;
    - a time delay is forced before further log-on attempts are allowed;
    - data link connections are disconnected.
- limit the maximum time allowed for the log-on process. If exceeded the system should terminate the log-on;
- display the following information on completion of a successful log-on:
    - date and time of the last successful log-on;
    - details of any unsuccessful attempts since the last successful log-on.

Where it is important that a session should be initiated only from specific locations automatic terminal identification should be implemented. An identifier can be used to indicate whether a particular terminal is permitted to initiate or receive certain transactions.

9.5.3 User identification and authentication

Each user should have a unique identifier (user-id) for their personal and sole use. The user-id should give no indication of the user's privilege level. Systems can be designed to utilise a unique user-id to ensure that all activities on the system can be traced to the individual responsible. The user-id should not indicate whether a user is a manager, supervisor or has special privileges.

9.5.4 Password management system

Passwords are one of the principal means of validating a user's authority to access a computer service. Password management systems should provide an effective, interactive facility, which ensures quality passwords.

9.5.5 Use of system utilities

The use of system utilities should be restricted and controlled. System utilities can be capable of over-riding system and application controls. Therefore the use of those utilities should be restricted to those who need to use them, and their use controlled by the following:-

- password protection for system utilities;
- segregation of system utilities from applications software;
- limitation of the use of system utilities to the minimum number of trusted, authorised users;
- limitation of the availability of system utilities, for example, for the duration of an authorised change;
- logging of all use of system utilities;
- defining and documenting authorisation levels for system utilities;
- removal of all unnecessary utility and system software.

9.5.6 Duress alarm to safeguard users

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

9.5.7 Terminal time-out

A limited form of time-out facility should be provided for all computers which clears the screen and prevents unauthorised access but does not close down the applications or network sessions.

9.5.8 Limitation of connection time

For high risk applications, connection times should be restricted. Limiting the period during which terminal connection to ICT services are allowed reduces the window of opportunity for unauthorised access. This should be considered for sensitive systems. A restriction could be:-

- using predetermined time slots;
- restricting connection times to normal office hours if there is no requirement for overtime or extended hours operation;
- limiting the elapsed time for any connection.

9.6 APPLICATION ACCESS CONTROL

9.6.1 Information access restriction

Access to data should be granted only to staff who need to use the data to perform their job function. This applies particularly to security data which should be accessed only by security staff. Security data includes password files, encryption and authentication algorithms and user profiles.

If data access rights are changed or by-passed a report should be produced showing:-

- the identity of the person making the change;
- the authority for the change;
- what is being changed;
- who would or could be affected by the change;
- the date and time of the change.

If the mechanisms have been bypassed by an unknown intruder then the incident should be treated as a breach of security and fully investigated.

Except in emergencies, staff should not be granted access to live data over and above that originally assigned. Where emergency access rights are granted (for example, to technical support staff or engineers) they should always be granted under a specially allocated user-id and be password controlled. The password should be changed on completion of the emergency activity. All activity during the emergency should be automatically monitored and covered by logs and audit trails.

All detected unauthorised attempts to access systems or data should be reported to the ICT Security Officer as a security incident.

9.6.2 Sensitive system isolation

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

9.7 MONITORING SYSTEM ACCESS AND USE

9.7.1 Event logging

Audit logs recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs should also include:

a) user IDs;
b) dates and times for log-on and log-off;
c) terminal identity or location if possible;
d) records of successful and rejected system access attempts;
e) records of successful and rejected data and other resource access attempts.

Certain audit logs may be required to be archived as part of the record retention policy or because of requirements to collect evidence (see also Chapter 12).

9.7.2 Monitoring system use

9.7.2.1 Procedures and areas of risk

There should be established procedures, authorised by management, for monitoring system use. Areas that should be considered are:-

- access failures;
- review of log-on patterns for indications of abnormal use or revived user- ids;
- allocation and use of accounts with a privileged access capability;
- tracking of selected transactions;
- the use of sensitive resources.

These procedures are necessary to ensure that users are only performing processes that have been explicitly authorised.

9.7.2.2 Risk factors

The result of the monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:

a) the criticality of the application processes;
b) the value, sensitivity or criticality of the information involved;
c) the past experience of system infiltration and misuse;
d) the extent of system interconnection.

9.7.2.3 Logging and reviewing events

A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of security incidents are given in 9.7.1.

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered.

When allocating the responsibility for log review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Particular attention should be given to the security of the logging facility because if tampered with it can provide a false sense of security. Controls should aim to protect against unauthorised changes and operational problems including:

a) the logging facility being de-activated;
b) alterations to the message types that are recorded;
c) log files being edited or deleted;
d) log file media becoming exhausted, and either failing to record events or overwriting itself.

9.7.3 Clock synchronisation

The correct setting of computer clocks is important for audit logs. The service *W32Time* should be used to automatically synchronise all workstation clocks with the server clock. Users should not be granted the permission to adjust the system clock.

9.8 MOBILE COMPUTING AND TELEWORKING

9.8.1 Mobile computing

When using mobile computing facilities special care should be taken to ensure that NICR information is not compromised. Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of NICR premises. Protection should be in place to avoid the unauthorised access to or disclosure of the information stored and processed by these facilities. It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorised persons. Procedures against malicious software should be in place and kept up to date. Mobile computing facilities should be physically protected against theft. Equipment carrying important, sensitive or critical NICR information should not be left unattended.

9.8.2 Teleworking

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

10 SYSTEMS DEVELOPMENT AND MAINTENANCE

Configuration Management

Installation of new software or hardware, or changes to configurations, should only be allowed to members of ICT staff.

ICT staff are advised to consult the ICT Manager before installing new software or making configuration changes since this may cause faults or operational problems on the computer concerned.

10.1 SECURITY REQUIREMENTS OF SYSTEMS

10.1.1 Security requirements analysis and specification

Security issues should form part of any project's definition. The PRINCE project initiation document (or any alternative project management methodology) should contain explicit products and tasks such as the preparation of secure operating procedures. Security, like quality, is best built into a system as it is designed and developed, rather than added on as an afterthought. The main security issues of confidentiality, integrity of data and continuity of service from the system can all be affected significantly by how the system is designed and built and may all affect the costs and timescales of the system development.

Project approval should be withheld until the necessary security requirements have been built into the project plan. Each new application development should receive formal approval to proceed. Where personal data are involved, this approval should take into account the need to comply with an existing Data Protection Act registration, or to set up a new one. Project approval should also consider the risk that a new application using existing data files may compromise the security or performance of current applications.

A written statement of system security policy should be incorporated into, or annexed to, the specification for all new or replacement information systems. It should address the different aspects of:-

- principles for physical, staff and document security;
- communications security;
- hardware and software security measures;
- administrative and procedural security rules.

The system security policy should spell out the level of security required for a particular computer system with the aim of ensuring that the system is adequately protected in the light of the perceived risks to that system. A system security policy is prepared along the same lines whether the system is large or small, stand-alone or networked. The level of detail contained in the document will vary substantially depending on the size of the system and the sensitivity of data processed.

10.2 SECURITY IN APPLICATION SYSTEMS

10.2.1 Input data validation

Data security controls should maintain the accuracy, completeness and currency of data input, held and processed. Controls should include at least:-

- Referential integrity checking, which is the cross checking of logical consistency between data fields (for example checking that date of admission to hospital is later than (or equal to) date of birth). Validity checking includes ensuring that a field is within a certain range, or only alphabetic, or only numeric;
- Reconciliation which should span initiation of data to final disposition and could be based on the number of records, cash value, or hash totalling (i.e. totalling of any field in all records to produce a subsequently checkable field);
- Batch control totals and logging of batches of data where relevant;
- Rejected data, or data removed in an emergency, which should be output with a reason for rejection, and either held on a suspense file and the user notified of the rejection or removal, or returned to the user for completion of processing.

A record should be kept of any data removed and the reason(s) for removal. Any loss or corruption of data should be reported to the ICT Security Officer and the ICTM. The report should include:-

- date and time of discovery;
- which data has been lost or corrupted;
- remedial action taken;
- reason for the loss or corruption;
- follow-up action taken or required.

There should be automatic controls to ensure that the correct version of data is used for live processing.

10.2.2 Control of internal processing

10.2.2.1 Areas of risk

Internal application system data should be validated. Data correctly entered into an application system can be corrupted by processing errors or deliberate acts. Validation checks should be incorporated to detect such corruption.

10.2.2.2 Checks and controls

Validation checks could include:-

- session or batch controls, to reconcile data file balances after transaction updates;
- balancing controls, to check opening balances against previous closing balances;
- validation of system generated data;

- checks on the integrity of data or software downloaded, or uploaded, between central and remote computers;
- hash totals of records and files.

An audit trail facility, allowing the tracing of all transactions in a system, should be provided. The ICTM should specify the retention period of the audit trail. The retention period should be agreed with the ICT Security Officer. The audit trail should include attempted and failed transactions, where the reason for failure should be clearly stated.

10.2.3 Message authentication

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

10.2.4 Output data validation

Data output from an application system should be validated to ensure that the processing of stored information is appropriate to the circumstances. Output validation may include:

- plausibility checks to test whether data output is reasonable;
- reconciliation control counts to ensure processing of all data;
- procedures for responding to output validation tests.

10.3 CRYPTOGRAPHIC CONTROLS

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

10.4 SECURITY OF SYSTEM FILES

10.4.1 Control of operational software

All software should be quality assured before release for live use. This includes software acquired, or written, by the NICR. The process should include:-

- stand-alone and integration testing by an independent test group;
- the use of configuration management to construct and retain controlled versions of the software releases;
- Installation of new software or hardware, or changes to configurations, is only permitted provided appropriate licensing arrangements or other similar conditions of the supplier are met.
- validation that any changes to a version of software correspond to either:-
    - authorised change to requirements; or
    - an authorised correction of a failure to achieve an objective;
    - maintenance of auditable records of each process undertaken in providing a version or release.

Software should be quality assured to ensure that current requirements continue to be met, and that any new features are tested to ensure functionality. Prior to quality assurance the criteria for measuring the acceptability of software against installation requirements should be defined.

Where the software release is to be used at several locations, the quality assurance process should be carried out by a central group. It should also be ensured that the software is compatible with any associated existing systems.

Testing should be fully documented and the results distributed to interested parties.

10.4.2 Protection of system test data

The access control procedures which apply to operational application systems should also apply to test application programs. Access to operational application systems should be limited to those that use the software (the end users), while access to test programs should be limited to development staff. Maintenance staff should not have access to live files, even for copying purposes. Live files should be under the care of staff (operations staff or users) who have no maintenance responsibilities. These staff should make copies if programmers require them. Failure to separate responsibilities in this way increases the risk of procedures being evaded by programmers in a hurry, with subsequent loss of confidentiality.

The copying, archiving or dumping of any data should be authorised by the ICT Manager and copies should be treated as having the same level of security and access restrictions as the originals.

Live sensitive data should not be used for testing, training or demonstration purposes unless it is transformed such that identification of the original content is not possible. This applies in particular to all personal data as defined by the Data Protection Act. If live personal information is being "transformed" to use for test purposes, it should be borne in mind that simply changing a name may not be sufficient protection. If the person could be identified, by anyone, from the rest of the data (for example, medical history, address or other personal details) then all the data would need to be transformed.

Live and test data files should always be logically separated. Live and test data should, where possible, be physically separated. Where this is not possible, then the data should be logically separated by being placed in separate partitions or directories or the equivalent. If data is to be moved between live and test environments then the migration should be strictly controlled. An automatic log should be produced and audit trails maintained.

10.4.3 Access control to program source library

Where the NICR maintains its own program source libraries, the following principles will apply:-

- where possible, program source libraries should not be held in operational systems;
- a program librarian should be nominated for each application;
- ICT support staff should not have unrestricted access to program source libraries;
- programs under development or maintenance should not be held in operational program source libraries;
- the updating of program source libraries and the issuing of program sources to programmers should only be done by the nominated librarian upon authorisation from the ICT Support Manager for the application. If emergency re-compilations need to be done without prior authority, a record of all the circumstances should be kept for subsequent investigation;
- program libraries should be held in a secure environment;
- an audit log should be maintained of all accesses to program source libraries;
- old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures;
- maintenance and copying of program source libraries should be subject to strict change control procedures;
- vendor-supplied software packages should be used without modification. If any changes are necessary, these should be obtained from the vendor.

10.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

10.5.1 Change control procedures

All proposed changes to the system should be processed under a formal change control system which includes an assessment of the change's impact on security. System security can be compromised by changes which are made before or after the system has gone live.

The System Manager is responsible for ensuring that changes to the system do not alter, degrade or compromise:-

- security controls;
- access rights;
- audit and security software.

A record of all changes should be maintained. The record should include:-

- identity of the person making the change;
- details of the change;
- any other systems affected;
- date and time;
- test results.

10.5.2 Technical review of operating system changes

When any change(s) to the operating system are necessary, application systems should be reviewed to ensure that there is no impact on security. This review process should include review of application control and integrity procedures to ensure that they are not compromised by the operating system changes.

10.5.3 Restrictions on changes to software packages

As far as possible and practicable, vendor-supplied software packages should be used without modification.

10.5.4 Covert channels and Trojan code

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

10.5.5 Outsourced software development

Where software development is outsourced, consideration must be given to licensing arrangements, code ownership and intellectual property rights. Attention should also be paid to rights of access for the purpose of auditing and certification the quality and accuracy of work done.

11. BUSINESS CONTINUITY MANAGEMENT

11.1 ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

11.1.1 Business continuity management process

There should be a managed process in place for developing and maintaining business continuity throughout the NICR. This process involves an understanding of the risks the NICR faces in terms of incidents (whether breakdown, disaster or some form of human action such as theft) and their potential impact, followed by the formulation and documentation of an organisational contingency strategy consistent with agreed organisational objectives and priorities. Regular review and updating of such strategies and plans are essential.

11.1.2 Business continuity and impact analysis

Business continuity should begin by the identification of events that may cause the disruption of processes within the NICR. Such identification must be followed by a risk assessment of the impact of such disruptive events. The risk assessment should lead to the development of a strategy plan to determine the insurance of NICR continuity, such plan to be endorsed by management.

11.1.3 Writing and implementing continuity plans

A Contingency or Disaster Recovery Plan is a written list of actions which need to be taken to restore normal service following an incident (whether breakdown, disaster or some form of human action such as theft). It will cover where to go for computer support, where copies of the data files are to be found, how the new site is to link with the users and all of the actions and procedures needed to make the contingency plan work.

A contingency plan should be produced, tested regularly and kept up-to-date for each application and/or installation.

11.1.5 Testing, maintaining and re-assessing business continuity plans

11.1.5.1 Testing the plans

Contingency plans should be tested regularly, with the participation of all relevant staff, to ensure that such plans are up to date and effective.

11.1.5.2 Maintaining and re-assessing the plans

Contingency plans require maintenance by ongoing reviews and updates in order to ensure their continuing effectiveness. Such reviews and updates must be included in any relevant NICR change management programme.

12 COMPLIANCE

12.1 COMPLIANCE WITH LEGAL REQUIREMENTS

12.1.1 Identification of applicable legislation

Legislation imposes a need for ICT security and steps must be taken to ensure compliance with relevant requirements. Currently, legislation includes:-

- The Data Protection Act;
- The Copyright, Designs and Patents Act;
- The Computer Misuse Act;
- The Access to Health Records Act;
- The Health and Safety at Work Act;
- The Human Rights Act.

The EU directive "For the protection of individuals with regard to the processing of personal data and the free movement of such data" was adopted on 24 July 1995 and must be implemented within three years. The scope includes manual as well as automatically processed personal data. Additionally, staff are under a common law obligation to preserve the confidentiality of this information.

12.1.2 Intellectual property rights (IPR)

12.1.2.1 Copyright

Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights or trade marks. Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. Copyright infringement can lead to legal action which may involve criminal proceedings.

12.1.2.2 Software copyright

All users must comply with software licenses and prohibit the use of unauthorised software. No copyright material should be copied without the copyright owner's consent. In the UK, under the Copyright, Designs and Patents Act (1988), certain software copyright infringements are criminal offences.

Proprietary software products are usually supplied under a licence agreement which limits the use of the products to specified machines. The agreement may limit copying to the creation of back-up copies only. Users must not contravene the agreement without the copyright owner's written authority.

Copying of proprietary or organisational software for use on computers that do not belong to the organisation, for any purpose other than fully authorised business, might similarly infringe copyright.

Violation of copyright, license agreements or other contracts, for example, copying and using software for business purposes from an Internet site where there is a clear limitation for personal use only.

Where it is necessary to use a software product on additional machines, licences should be extended, or additional copies purchased. Site licences, permitting use of software on all computers within a specified site, may be obtainable.

Regular audits of software use should be taken and software asset registers maintained.

12.1.3 Safeguarding of organisational records

Guidelines on the retention, storage, handling and disposal of medical, confidential and other records and information, should be observed. These guidelines should be aimed at protecting essential records and information from loss, destruction and falsification. A retention schedule should be drawn up identifying essential record types and the period of time for which they should be retained.

12.1.4 Data protection and privacy of personal information

Identifiable patient/client information

The ease with which health and other personal data can be identified as belonging to a particular individual depends on the number and nature of the data items which, individually or together, could allow the individual to be identified. For example, replacing name and address by UPCI (Health & Care) number or other unique number, although not anonymising data, would reduce the risk of revealing personal health data through casual prying. A combination of data items such as age, sex and full post code could allow an individual to be identified, whereas a post code restricted to the first three characters (identifying only the post code area) can substantially reduce that risk.

Chapter 4 of the document *The Protection and Use of Patient and Client Information* issued by the HSSE in Spring 1996 addresses the issues associated with safeguarding patient/client information.

Data protection

The ICT Manager is responsible for ensuring that, where applicable, the system is registered under the Act. Authority to access identifiable patient/client information must be in accordance with the Data Protection Act.

12.1.5 Prevention of misuse of information processing facilities

Employees of the NICR and any third party users should be informed that access to systems is not permitted except where this has been formally authorised and documented. Any use of ICT facilities for non-business or unauthorised purposes, without management approval, will be regarded as improper use of the facilities.

Note that the Computer Misuse Act (1990), introduced three criminal offences:-

- unauthorised access;
- unauthorised access with intent to commit a further, serious offence;
- unauthorised modification of computer material.

12.1.6 Regulation of cryptographic controls

See section 10.3.

12.1.7 Collection of evidence

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

12.1.7.1 Rules for evidence

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy.]

12.1.7.2 Admissibility of evidence

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

12.1.7.3 Quality and completeness of evidence

[This element of ISO 17799 is deliberately left blank since it falls outside of the scope of this NICR ICT Security Policy]

12.2 REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE

12.2.1 Compliance with security policy

The ICT Security Officer should ensure that each system under the control of the organisation is subject to regular security risk assessments. It is important that systems are reviewed regularly to ensure that their criticality rating is updated on a regular basis. Three years is considered to be a reasonable maximum period between reviews.

12.2.2 Technical compliance checking

Information systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented.

12.3 SYSTEM AUDIT CONSIDERATIONS

12.3.1 System audit controls

Audit requirements and activities involving checks on operational systems should be scheduled to minimise the risk of disruption to business processes.

Requirements for special or additional processing should be identified and agreed with service providers. All procedures, requirements and responsibilities should be documented.

Audit checks should be limited to read-only access to software and data. All access should be monitored and logged. This will provide an audit trail of the audit.

12.3.2 Protection of system audit tools

Access to system audit software tools should be controlled to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems, and not held in media libraries or user areas, unless given an appropriate level of additional security protection

Appendix A

Physical Security within NICR

Perimeter security

Access to Mulhouse Building

Entrance to the Mulhouse Building which houses the NICR (on the 1st floor) is via electronic keypad access at the ground level main door or via mechanical keypad access at the door leading from the external metal bridge/walkway to the 1st floor. Outside normal office hours (from 4:30pm to 7am next morning) the electronic keypad at the main ground floor entrance becomes active and only authorised personnel may enter the building using their staff number as the password. Otherwise a powerful electromagnet lock prevents access to the building. The keypad numbers change positions each time an access is requested. The mechanical keypad is normally active at all times.

There is one main fire-door leading onto the car park directly opposite the Mulhouse Annex. This door is shared with the Medical Library which is sited on the ground floor. This fire-door is always alarmed except for deliveries to the NICR or Medical Library. A further internal door leading from the fire-door into a link corridor is always locked and the key to this door is held by NICR alone. Entrance through this door leads to a staircase to the 1st floor the top of which leads into the main NICR corridor.

Main Door to NICR

The NICR is located in the annex part of the Mulhouse Building on the 1st floor. An electronic keypad is used to gain access to the main NICR door which is protected by a powerful electromagnetic lock. The code of the main door is known to all members of staff and temporary users of the Registry who need access outside normal hours of work. It should not be divulgated to anybody else. The code should be changed every year and whenever any of these persons ceases to need access to the NICR premises, by implementing the following procedure:

1. Before the first Staff Meeting after the change is needed, the new code is created and added to a list kept in the fireproof safe;
2. The new code should not match any of the previous codes;
3. During the Meeting, the new code is announced to all members of staff, with the recommendation not to write it down;
4. A member of the Administrative staff is identified for communicating the new code to the rest of the persons not present at the meeting.
5. The new code is communicated to QUB Security Department.

For visitors there is an intercom system and buzzer to request access. The main access door to the NICR should be kept closed at all times

Internal Doors and Windows

Within NICR most offices have doors which are protected by means of mechanical keypad locks and require a sequence of key presses (password) to be known in order to gain entry. These offices have computers which are connected to the NICR network (a physically separate network with no connection to other networks or the internet) and thus are designated ‘secure areas’. Consequently these computers have access to the main registration

system and thus to patient data. Separate passwords are used for each office and are changed every 6 months. The codes for accessing the rooms of individual members of staff are also known by the administrative and ICT staff. The same procedure as above, but involving only the relevant members of staff, is followed immediately after the change is needed.

The code of the main TVO room door is known to all members of staff, temporary users of the Registry who need access outside normal hours of work and nobody else. The code should be changed every year and whenever any of these persons ceases to need access to the NICR premises, by implementing the same procedure as above.

The codes for all offices are stored in a fireproof safe located within the IT Manager's office and also off-site in a bank deposit facility – the same facility used for off-site storage of server backups. The codes are also passed to the Security Department of Queen's University in order to gain access if required (for example, to check for fire in the event of an alert).

All internal doors with keypad access should be kept closed when nobody is in the corresponding secure area.

Other office internal doors have standard locks and the owner of each office is responsible for their own key. In addition, copies of the keys for these offices are held in a lockable key-box within the main TVO room (access to which is protected via a mechanical keypad lock as mentioned previously). The key to the key-box is held by the Data Manager.

Windows

All windows should be securely closed when no members of the staff are in the NICR. Each member of staff who has their own office shall be responsible for closing their office window at night before leaving for home. The last person left in the registry shall be responsible for checking that windows in common areas (specifically the kitchen area and the toilets) and the main TVO room are securely closed – this is usually the IT Manager or one of the IT team.

Physical Security of Servers

The servers are located in a dedicated room which has a standard key lock. This room is further located within an office which has a mechanical keypad lock. The office is used by members of the IT team. The sequence of keys required to gain access to this office shall be changed quarterly or whenever a member of the IT teams ceases employment with the NICR. Additionally, the servers themselves are housed in cages which are bolted to the concrete floor therefore making their removal more difficult.

Fire proof safe

An on-site fire proof safe is used for storing daily backup tapes and other media containing confidential and business critical information.
The fire proof safe is located in one of the secure areas of the NICR and is locked by electronic keypad and mechanical key. The key is not labelled and is stored in a locked key-box, bolted to a wall in the secure area, together with other keys for doors and cabinets; the key for the box is not labelled and is stored in a place known to the members of staff who need access to it.

Appendix B

User Access Management

The network security of NICR is provided by the security features of Microsoft Domain and Active Directory (AD).
The following table shows the groups existing in the NICR Domain AD and the default privileges granted to the users belonging to them. All users are assigned to one or more of these groups, and individual users privileges are customised where needed.

			Object access privileges						
			Shares			*Misc*			
			\Common	\Common\ System	Other shared folders	Print	Logon Hours	Removable storage	Logon Workstations
AD Groups	*NICR staff*	IT	Full control	Full control	Full control	Yes	8 to 19	RW	All
		Data Manager	Read\Write	None	RW	Yes	8 to 19	RW	No servers
		TVO	RW	None	None	Yes	8 to 19	RW	No servers
		Statisticians	RW	None	None	Yes	8 to 19	RW	No servers
	External	Guests	RW personal folder only	None	None	No	8 to 19	R	TVO room only
		Students	RW personal folder only	None	None	No	8 to 19	Disabled	TVO room only

User accounts should never be deleted nor re-assigned to another user. When not in use or ceased they should only be disabled.

Procedures for granting access to a new user

For each new user of the NICR system and/or network a *User management form* (Appendix I) should be printed and filled in by a member of the ICT staff. The following steps should then be followed:

1. System access application (non NICR staff only)
2. Identification of user access level, roles duties and responsibilities and of termination date and subsequent identification of user profile/privileges/group memberships to be granted to the use
3. Confidentiality induction
4. Security induction
5. Creation of new domain account
6. Creation of new Cache' account (if applicable)
7. Creation of new Praxis account (if applicable)

1. System access application form

This form is outlined in the NICR document *Policy Regarding Security, Confidentiality and Issue of Data*. It is only required for users who are not member of the NICR staff.

2. Role management

1. The Director and the ICT Manager decide, jointly, the minimum set of authorisations for access and privileges to needed by the user in order to perform the duties specified in his/her job specification, if the user is a member of the NICR staff, or the activities specified in his/her application form, if the user is not a member of the NICR staff.
2. On the basis of that decision:
    a. the user is assigned to one of the existing AD groups, with or without modifications of the default settings
    b. the user is assigned to one of the existing Praxis groups, with or without modifications of the default settings or, alternatively, does not require access to the NICR main database

Groups the user should belong to

- ☐ IT
- ☐ Data Manager (DM)
- ☐ TVO
- ☐ Guests
- ☐ Students
- ☐ Statistician

Privileges and other settings for the user to override group settings

- ☐ Access to \Common
  - Full control
  - Read/write
  - Personal directory
- ☐ Access to \Common\System
- ☐ Access to \Output
- ☐ Print
- ☐ Telnet (Kea) + Cache' + Praxis
  - Read only
  - …
- ☐ Removable storage (USB/floppy/CD-R)
- ☐ Logon (not) to specific machines …..……
- ☐ Longer logon hours ……..……

3. Confidentiality induction

1. The applicant is briefed by the Data Manager on the general issues of confidentiality in handling patient identifiable data and on the specific policy in force in the NICR

2. The Data Manager provides a copy of the NICR document *Policy Regarding Security, Confidentiality and Issue of Data* and has the new member of staff sign the form *Confidentiality Undertaking for all Registry Staff* there included (Appendix E).

3. The *User management form* is signed off by the Data Manager.

4. Security induction

1. The applicant is briefed by the Security Officer on the general issues of ICT security and on the specific policy in force in the NICR

2. The SO provides a copy of the short version of the ICT Security Policy document and makes clear that the full version is available for consultation at any time.

3. The *User management form* is signed off by the ICTSO

5. Procedure for creating a new domain account

1. Logon with an administrative account on one of the Domain Controllers (DC).

2. In Active Directory (AD), create a new user from the template contained in the group the users will belong to.

3. Fill in as many details as possible (name, job title must be filled in).

4. The username should be formed by the concatenation of the user's first name and first letter of surname. In case of duplicates, additional characters should be used.

5. Ensure that all suitable restrictions are in place (logon hours, logon workstations) and that the user is assigned to other groups he/she needs to belong to.

6. In the Sentrinet tab, the following options should be selected:
   a. Biometric
   b. Random password
   c. Remote enrolment

7. Type in a temporary password when prompted (it does not need to be a strong one, if the fingerprint enrolment is performed immediately).
8. Log off from the DC.
9. Have the new user to log on a machine with the same fingerprint sensor he/she will be using. The username is the one just created at point 4. and the password is the one just created at point 7.
10. When the enrolment window appears, enrol at least 4 fingerprints, 2 from the right hand and 2 from the left hand of the user.
11. Pay attention the user places the centre of his/her fingerprint in the centre of the sensor, that the finger is not moving during the scan and that the pressure exerted on the sensor is firm but not excessive.
12. After the enrolment verify the fingerprints by using the *Verify* button and then by having the user to logoff and logon a couple of times.
13. If difficulties are experienced in the fingerprint recognition:
    a. Logon with an administrative account on one of the DC.
    b. In AD, double click the user item and repeat the procedure starting from point 6., after having deleted all the stored fingerprints from the list.

6. Procedure for creating a new Cache' account

As perquisites, both server and client elements of Cache must be installed on a user machine (indicated by a 'blue' cube in the Windows System Tray) otherwise this must be done on the server console. In addition, the name of the computer to which the new user will be assigned must be known.

1) As a Cache Administrator right click on the blue cube in the system tray and select 'Control Panel'
2) In the left pane of the resulting window expand the 'Security' item and select 'User Accounts'
3) Right click the mouse in the right-hand pane and select 'New User…'
4) Enter the details of the new user account to be created.
   NOTES:
   a) The 'Namespace' property should be changed to point to the location of the live registration database (in the case of N Ireland Cancer Registry this is currently 'LIVE').
   b) The 'Account' property should be set to the computer name of the PC assigned to the new user.
   c) The 'Routine' property can be set to either "^%PMODE" for a user which requires programming mode or to "^CR00LG" to direct end-users to the login screen for the cancer registration application.
5) Click 'OK' to finish entering the user details and exit the cache Control Panel.

7. Procedure for creating a new Praxis account

Only staff with Cache RDBMS administrator privileges and programming mode access to the Cache RDBMS are authorised to complete the following steps:

1) Using the KEA terminal emulation software, connect to the namespace where the main cancer registration system is located (in the case of N Ireland Cancer Registry this is currently 'LIVE').

2) Type “do ^%msql” at the chevron prompt LIVE>.
3) Log into MSQL as ‘system’ with the appropriate password.
4) Use the arrow keys to move down and select ‘System Management’
5) Use the arrow keys to move down and select ‘User Security Definition’
6) Enter a known username to modify that user’s profile or a new username for the new user. The convention for usernames is <first forename> followed by <surname initial>.
7) Enter “Yes” or “No” against the various options available on the form. Note that for system developers and technical users, all items should in general be set to “Yes”. However, for end-users, most items should be set to “No” except for ‘Query Definition Access’, ‘Help Topic/Document/Text Entry Access’ and Cache SQL System Help Access’.
8) Using the arrow keys, move to the bottom of the form until <PROCEED> appears highlighted and hit Enter/Return.
9) Using the minus key on the application keypad back out of MSQL and type the following at the chevron prompt LIVE> “do ^CR00LG”. This will bring up the login screen for the PRAXIS application software.
10) Logon as ‘system’ with the appropriate password.
11) Using the arrow keys move down and select ‘Maintain System Files’
12) Using the arrow keys move down and select ‘System Users’
13) Enter the username for the new user that was defined in step 6 above and hit Enter/Return.
14) Enter the details required ensuring that the field ‘Currently Active’ is set to “Yes”. Note that the field ‘User Type’ should be set as appropriate to one of the following:
“System Manager”
“Data Manager”
“Data Analysis”
“Data Input”
15) Using the arrow keys, move to the bottom of the form until <PROCEED> appears highlighted and hit Enter/Return.
16) Using the minus key on the application keypad back out of the PRAXIS menus and return to the chevron prompt LIVE>. Type “h” or “halt” to exit the telnet session and close the KEA window.

Note this procedure can also be carried out using the Cache Terminal from the server console or a PC with both client and server elements of Cache RDBMS installed.

Appendix C

Password Management

Application Passwords

1. Each member of staff should have his/her individual user identification and password.

2. For the most effective security, staff should have self-selected and self-changed, individual passwords. A confirmation procedure to allow for typing errors should be provided.

3. Passwords should not normally be written down. It is not uncommon for password protection to be defeated by a user writing the password down on a piece of paper kept close to a terminal. If a user needs a written aid to recall the password, it should be disguised or encrypted such that only he/she can understand it. Where it is necessary to write down a password (as, for example, a contingency measure) it should be stored in a sealed envelope in a safe. Access to the envelope in the safe should be restricted to contingency requirements only. Inspection of the envelope should be carried out on a regular basis by the officer to whom the password belongs and a record maintained.

4. Screens, keyboards and printers should be physically positioned such that they are protected against accidental disclosure of passwords or any other confidential or sensitive data.

5. Where Operating System permits the following functions should be enabled:

Maximum Password Age : 90 days
Password History : 10
Minimum Length : 8
Automatic account lockout : 3 attempts

Passwords should consist of at least one non-alphabetic character. The user should be prompted to change their passwords during the seven days prior to the expiry date.

6. Automated log-on procedures may contain passwords but should themselves be protected. For example, log-on procedures performed by striking a single function key should request the input of the password. If a macro or similar device is used to automate log-on then the user should be required to enter the password in order to activate the macro.

7. Passwords should not relate to the user or to the system being accessed. Many users will opt for passwords that they find particularly easy to remember. Often the password chosen has strong associations with either the system or the user and could be guessed by potential intruders. One way of creating a password meaningful to the user but not easily guessed by anyone else, is to choose a phrase and compose the password from the initial letters and numbers of the words. For example,

"ILIA2BH" - I Live In A 2 Bedroomed House

"IGOH28J" - I Go On Holiday 28th June

"MTNBW62" - My Telephone Number Begins With 62

A viable alternative for selection is to open a book at random and select a phrase or word to form the basis of the password. Other ways could be:-

- Linking two words together with a non-alpha character. For example, "CAT*FOOD" or "BELL%BOOK"

- Forming easy to remember anagrams of words or names and adding a non-alpha character. For example, "NAILGIL*" (GILLIAN*) or "ARDHOW£" (HOWARD£).

- Replacing letters in a word or name by a non-alpha character. For example, "CHA#LE*" (CHARLES) or "CAR&OON" (CARTOON)

NEVER use your own name, car type, car registration number, or those of family or close friends.

8. Passwords should always be changed immediately on suspicion of any compromise. The longer a password remains unchanged, the more opportunity a potential intruder will have to discover it. Any such incidents must be reported to the ICT Security Officer.

9. Where necessary, enforce a more frequent password change for privileged accounts, for example, those with access to system utilities.

10. Password software should ask the user for re-authentication by re-entering the old password before accepting a change of password.

11. Store password files separately from the main application system data;

12. Alter vendor default passwords immediately after installation.

13. The use of software for 'password-cracking' or any other means of discovering passwords is forbidden.

Document protection passwords

1. Some applications (MSOffice applications, WinZip etc.) allow users to password-protects the opening of a file. This protection should be regarded as very weak or inexistent: password in most of the MSOffice applications can be recovered by freeware and commercial tools in a matter of seconds

2. Passwords to open MSWord, MSExcel and WinZip can be regarded as reasonably secure only if they are at least 16 characters long and contain non-alphabetical characters.

Appendix D

Workstation Setup and Networking

All workstation linked for the first time to the NICR domain must be

- brand new, 'out of the box', machines

or

- computers which have been just reformatted and completely reinstalled.

The following are the procedures/checklists for the installation of a new workstation (desktop or laptop) in the NICR domain. A copy of the checklist should be printed, filled in while installing the new workstation and stored away. The second part of the document is updated each time major hardware or software modifications are performed on the machine and, for portable computer, each time the machine is assigned to/given back by the custodian.
A summary of the main information of each machine and the name of the present and previous custodian is also kept in the file *Common\System\Docs\Clients\Hardware Inventory.xls*.

Checklist for the installation of new clients in the NICR

PC connected to the internal network

- ❑ File System must be NTFS
- ❑ Rename the machine
- ❑ Configure network to automatically obtain an IP address and the address of DNS servers. If a static IP address is needed, use the following settings:

IP address	143.117.15.***X***
Subnet Mask	255.255.255.0
Default Gateway	**Blank**
DNS Servers	143.117.15.129 143.117.15.101

- ❑ Join the NICR domain
- ❑ Disable LOCAL Administrator account
- ❑ Software to be installed (as a DOMAIN administrator):
  - ❑ Symantec Antivirus (from \\belfast\SAV\clt-inst\WIN32\Setup.exe)
    - □ Add to group on the server
  - ❑ Latest OS updates (from \\nicanreg1\Common\System\Service Packs and Hotfix\WinXP)
  - ❑ Office XP (from disk)
  - ❑ Latest Office updates (from \\nicanreg1\Common\System\Service Packs and Hotfix\OfficeXP)
  - ❑ SentriNet (from disk) + update (from \\nicanreg1\Common\System\Service Packs and Hotfix\Sentrinet) [NOT the Server Component]
  - ❑ Fingerprint sensor driver
  - ❑ WinZip
  - ❑ Kea
  - ❑ NICR application
  - ❑ Configure WinUpdate Client (no updates)
  - ❑ Acrobat Reader
  - ❑ SPSS
- ❑ BIOS password
- ❑ Multiregional settings: date format dd/mm/yyyy
- ❑ Place "Lock Workstation" shortcut on desktop (all users) + user's taskbar (from *\\nicanreg1\Common\SystemPublic*)
- ❑ TrueCrypt full disk encryption

Model…….
Inventory No……..
Assigned to…….
IP address (if any)……...
Network name……
Installed by……..Date…….

Please, specify any subsequent modification on the back of this form

Checklist for the installation of new clients in the NICR

Laptop connected to the internal network

- ❑ File System must be NTFS
- ❑ Join the domain and configure network

DHCP or:

IP address	143.117.15.-
Subnet Mask	255.255.255.0
Default Gateway	Blank
DNS Servers	143.117.15.129 143.117.15.101

- ❑ Disable LOCAL Administrator account

- ❑ Disable unnecessary networking devices, where present
    1. Wireless Network Adapter
    2. 1394 Network Adapter
    3. Modem
- ❑ Remove unnecessary software, where present
    1. Norton Internet Security
    2. Norton WMI Update

- ❑ Software to be installed (as a DOMAIN administrator):
    - ❑ Symantec Antivirus (from *\\belfast\SAV\clt-inst\WIN32\Setup.exe*)
        1. Add to group on the server
    - ❑ Latest OS updates (from *nicanreg1\Common\Staff\IT\System\Service Packs and Hotfix\WinXP*)
    - ❑ Office XP/2003 (from disk)
    - ❑ Latest Office updates (from *nicanreg1\Common\Staff\IT\System\Service Packs and Hotfix\OfficeXP*)
    - ❑ SentriNet (from disk) + update (from *nicanreg1\Common\Staff\IT\System\Service Packs and Hotfix\Sentrinet*)
    - ❑ Fingerprint sensor driver
    - ❑ WinZip (from *nicanreg1\Common\Staff\IT\System\WinZip*)
    - ❑ Configure WinUpdate Client (no updates)
    - ❑ Acrobat Reader
    - ❑ SPSS (if needed)

- ❑ Configure power management
- ❑ BIOS password
- ❑ Multiregional settings: date format dd/mm/yyyy
- ❑ Place "Lock Workstation" shortcut on desktop (all users) + user's taskbar (from *nicanreg1\Common\SystemPublic*)
- ❑ TrueCrypt full disk encryption

AFTER THE USER LOGS ON

- ❑ Create "Encrypted folder" on the user's desktop and encrypt it
- ❑ Place "Backup Laptop.vbs" script on the user's desktop (from *nicanreg1\Common /SystemPublic\Scripts*, follow the Readme.txt instructions)
- ❑ Place "Backup to lipstick.bat" batch on the user's desktop (from *nicanreg1\Common /SystemPublic\Scripts*), edit it and change "giulion" into the proper username

Model…….
Inventory No……..
Assigned to…….
IP address (if any)……...
Network name……
Installed by……..Date…….

Please, specify any subsequent modification on the back of this form

Hardware and software modifications

Problem (if any)	Modification	Date

Custodians' history (laptops only)

Laptop assigned to	Removed from NICR	Returned to NICR

Appendix E

Backup Procedures and Data Protection

Backup procedures

Servers

The application "Backup Exec" by VERITAS is used to backup the NICR Domain Controllers.
The adopted backup strategy is a 'Grandfather' one, with a weekly full backup and a daily incremental one. The tapes are labelled and used as follows:

Tape	***Label***	***Use***
1	Incremental tape	Incremental backup on Mon-Tue-Wed-Thu
2	Month 1 week 1 full backup	Full backup on Fri, every other month, in rotation with following tape
3	Month 2 week 1 full backup	Full backup on Fri, every other month, in rotation with previous tape
4	Week 2 full backup	Full backup on Fri, monthly
5	Week 3 full backup	Full backup on Fri, monthly
6	Week 4 full backup	Full backup on Fri, monthly

The resulting tape rotation scheme is the following:

	Mon	***Tue***	***Wed***	***Thu***	***Fri***
Week 1	1	1	1	1	2
Week 2	1	1	1	1	4
Week 3	1	1	1	1	5
Week 4	1	1	1	1	6
Week 5	1	1	1	1	3
Week 6	1	1	1	1	4
Week 7	1	1	1	1	5
Week 8	1	1	1	1	6

The backup jobs are all scheduled at 21:00. The following procedures should be performed before this time (with the annual exception specified below):

- ☐ *Mondays*
  - Run Backup Exec and ensure the weekly backup was successful
  - Ensure the green light 'Operate handle' on the drive is on
  - Remove the tape from the drive
  - Take the tape labelled 'Incremental Tape' from the fireproof safe and slot it into the drive
  - Ensure the format of the tape is recognized by the drive
  - Hand the tape just removed from the drive to the designated member of staff who will
    - Bring the tape to the bank, without intermediate stops, and store it into the safe

- Take the taped stored from the previous week (not labelled "TO BE KEPT INDEFINITELY") back to the NICR, without intermediate stops
- Store this last tape into the fireproof safe

☐ *Tuesdays to Thursdays*
- Run Backup Exec and ensure the daily backup was successful

☐ *Fridays*
- Run Backup Exec and ensure the daily backup was successful
- Press the button 'Unload' on the drive and, when the green light 'Operate handle' on the drive comes on, remove the tape from the drive and store it in the fireproof safe
- Take the relevant full backup tape from the fireproof safe and slot it in the drive (you can double-check which full backup tape is needed by opening the 'Properties' of the previous full backup, clicking the tab 'Job Log' and reading the 'Media Label' name)
- Ensure the format of the tape is recognized by the drive

Annual exception: permanent backup and annual cleaning
The second point of the *Fridays* list in the previous procedure is replaced by the following points on the last working Friday of the year, before Christmas vacation, to allow for the creation of an annual backup to be kept indefinitely:
- Press the button 'Unload' on the drive and, when the green light 'Operate handle' on the drive comes on, remove the tape from the drive
- Add to its label the writing "Annual backup (end YYYY) – TO BE KEPT INDEFINITELY", in red, and store it in the fireproof safe
- Format a new tape and label it as the original label of the tape just removed from the drive, and store it in the fireproof safe

A few days before this procedure is performed, all users who access shared folders on the server should be informed that all files will be backed-up and kept in the bank for ever, and that all files older than 6 month will be deleted permanently from these folders. The should be advised, then, to
- delete from these folders all unneeded files not older than 6 months
- backup all files older than 6 months they still need to access, or give the ICT team a list of those files they whish to retain

When the backup procedure is completed, all files older than 6 months in shared folders are deleted from the system.

Laptops

Backup to server
Server backup of laptops is performed by the script *Backup laptop.vbs* placed on the user's desktop. The procedure is the following and has to be performed by the custodian of the laptop:
- Switch off the machine
- Plug the network cable labelled "Laptop Backup Point", in the TVOs room, into the network socket of the laptop
- Switch on the machine and logon as usual
- Wait until the network icon shows in the tray

- Double click the icon *Backup laptop* sitting on your desktop
- Press Ok when the message "Your files will be backed up to the server..." appears
- Wait while your files are being backed up
- Press Ok when the message "Backup completed!" appears
- Unplug the cable only when the laptop is switched off

Daily backup to memory stick

Daily backup of laptops is performed by the batch file *Backup to lipstick.bat* placed on the user's desktop. The procedure is the following and has to be performed by the custodian of the laptop:

- Plug your memory stick into an available USB
- Wait a few seconds, until the memory stick is recognised and installed on the machine
- Double-click the icon *Backup to lipstick.bat* on your desktop
- You will see some windows coming up, one of which shows you the progress of the operation. When the backup is complete, all windows should close automatically
- Once all the activity has ceased, you can switch off your laptop and, afterwards, remove your memory stick
- The memory stick should be stored in a secure place and away from the laptop

Controls against Malicious Software

Viruses

The NICR network is protected against virus infections by Symantec Antivirus Corporate Edition, provided by the Queen's University of Belfast. The server component of the software is installed on the Domain Controller *Belfast*, while the client component is installed on all the other members of the NICR domain (see Appendix D for the installation procedure). The Virus Definition File is updated every Thursday, by the following procedure:

Virus Definition File Update Procedure

1. On a computer connected to the QUB (external) network, with an up-to-date antivirus software and virus definition file, open the link http://securityresponse.symantec.com/avcenter/download/pages/US-SAVCE.html
2. Download the updated **.xdb** file to a suitable removable storage device (USB, CD…)
3. The name of the downloaded file, in the device, is in the form ***.xdb.zip** (or ***.zip**). Remove the **.zip** extension (or change it to **.xdb**)
4. Logon to a machine belonging to the NICR domain and connect the device with the downloaded file to it
5. Transfer the **.xdb** file to the directory \\belfast\SAV\

The updated virus definition file is automatically propagated to all clients, at their first start up if not already on. In addition to the Realtime Protection, which cannot be disabled by the local users, every Friday, at a time that depends on the Symantec Group the machine belongs to, the Symantec Antivirus Client performs a scan of the whole hard drive. Although

the process could significantly slow down the computer, the logged users should not pause or snooze the process unless strictly necessary.

The following points are also related to the virus protection issue and are pointed out to new users during the security briefing:

1. The careless use of just one computer, especially when part of a network, could lead to widespread virus infection and damage to other people's systems and data;

2. All computer media entering or leaving the organisation should be virus-checked. In the event of any infection being discovered, the SO should be immediately informed, so that the source can be traced and other users or recipients of disks from the same source can be warned that they might be infected. Software disks should be checked before the software is installed and used;

3. Wherever possible, computer media should be "write protected" until a write operation is required. As viruses spread by writing themselves to uninfected disks, write protection, wherever possible, is advised. This is particularly important when using master copies of system and program disks;

4. Only officially provided and approved software should be loaded on to computers. In many cases viruses are transmitted to computers by one of the following routes:-

- free disks from magazines;
- "pirate" software and games;
- public domain games and software;
- programs from "Bulletin boards".

5. Procedures, for checking and "disinfecting" any machine suspected of holding any malicious software, should be established. They should contain:-

- Immediate virus checking of all other possibly infected machines;
- Isolating the machine immediately. For example, if networked, the machine should be disconnected to prevent the infection spreading;
- Preventing the use of the infected machine again until its reuse has been approved by the ICTSO;
- Checking all software and data on the machine for the presence of viruses. If a virus is present:-
    - memory and disks should be wiped clean;
    - safe master copies of software should be virus scanned and then reloaded;
    - the most recent data back-up should be virus scanned and, if clean, then reloaded.

6. Alternatively, it may be possible to remove the virus from the system by use of a reputable commercially available anti-virus tool. This has the advantage of being a potentially quicker solution than re-loading data from back-up. Before embarking on this method, it is essential that:-

- the virus type is correctly identified;
- the ICT Security Officer is consulted for advice and has contacted the anti-virus tool supplier if appropriate.

7. If an officially provided machine is used outside secure official premises, it should be used only by the authorised member of staff. The machine must not be connected to any unauthorised external networks and must not use disks that have not been officially approved.

8. Staff needing to work on a computer outside official premises should use one that is supplied officially, and should ensure that it is used only for authorised work. They should also ensure that no-one else but themselves has access to the machine while it is outside secure, official premises.

9. Any computer that may previously have been connected to the Internet other than through the local network must not subsequently be attached to the local network without first being virus checked.

10. Those staff who have been assigned portable computers must take steps to ensure that those portables have not been exposed to other networks when not under their direct care.

Security Patch Management

Unless required for resolving specific issues, patches, security updates and software updates in general are not installed on a regular basis on the internal machines.
Exceptions: MS Windows and MS Office Service Packs are downloaded, tested for compatibility and installed on all the machines as soon as they are available.

Appendix F

Sensitive Information Labelling and Handling Procedures

Paper documents
All printed documents containing sensitive information should be collected immediately. While the documents are not in use, they should be stored out of sight, in a locked drawer or cabinet inside the secure area.
When the documents are no longer needed, they should be destroyed by using the shredder in the library.

Removable storage media
The use of removable storage media for sensitive information is strongly discouraged. Information that needs to be shared among users should be placed in the *Common* directory on the server (*Z:* drive in *My computer*). If, in exceptional circumstances, sensitive information needs to be temporarily stored on removable storage media only approved SanDisk Cruzer Enterprise FIPS Edition should be used.

- *CDs and DVDs*
    - CDs and DVDs are allowed to contain sensitive information only for backup purposes and must be stored in the fireproof safe. If the user has not been granted the right to write data to CDs and DVDs, this procedure should be performed by ICT staff.
        - When the data are backed up to the disk, specify the content of the disk on its label, by writing with a permanent marker.
        - Immediately place the disk in the fireproof safe.
    - CDs and DVDs used for exchange of sensitive data with non-NICR parties must be encrypted using the 256-bit AES algorithm and a long random password, to ensure security and confidentiality. The password is sent separately and only after the verified contact acknowledges the safe reception of the disk.

Hard disks
Working files containing sensitive information should be kept in the *Common* directory on the server (*Z:* drive in *My computer*) or in the personal folder on the server (*W:* drive in *My computer* – the name of the drive is the same as the username). This practice ensures higher security and daily backup for the data.
In some cases, when working with voluminous data files, the performance of the system is so badly affected that you need to work on a local copy of the file. In those cases the procedure 'Working locally with sensitive data file' below has to be followed.
The following procedure has to be implemented when a hard disk, in conjunction or not with a container workstation, is to be moved to a non secure area, redeployed outside the NICR or disposed of
Hard disks redeployment and disposal

- Scan the whole disk for files that need to be kept for future reference
    - If any, backup those file either
        - to a folder in the *Common* directory, named as the workstation containing the hard disk

      or
        - CD/DVD archive, labelled with the workstation name and some information about the content of the archived files, and store the media in the fireproof safe.
- Format the hard disk

- Install the hard disk into another workstation, as a secondary disk, and erase the disk by using the application *Eraser* (if not present, install from *\\nicanreg1\Common\System\Software\Eraser*). The number of passes should be at least 7
- Format the hard disk and put it back into the original workstation

Working Locally with Sensitive Data Files

Laptops

All computers connected to the NICR network are protected by TrueCrypt full-disk encryption. Additionally, each laptop used for collecting and storing sensitive data is individually assigned to a single user. All files containing sensitive data must be kept in the directory *Encrypted Folder* placed on the user's desktop and should never be moved to another location, with the exception of the backup procedure (See section 'Laptops' in 'Appendix E – Backup procedures')

Appendix G

Event Auditing

Event logs

The Domain Group Policy should be set to audit success and failures of all account logon and management events and only failures of directory service access, logon, object access and policy change events.
On the last Friday of each month, a scheduled task on each of the NICR Domain Controllers should launch a script which copies all the event logs to a specified folder on the Domain Controller, without overwriting previously copied ones. This ensures that the auditing of past events is possible even if the events have been removed from the live logs.
On the following Monday, or immediately after, the ICTSO should analyse the events logged during the previous four weeks.