

NATIONAL LIBRARY OF SCOTLAND

INFORMATION SECURITY POLICY

APPROVED BY: Board of Trustees (28 July 2008)
Trade Union Side (22 May 2008)

REASON FOR POLICY: It is vital that all staff and all contractors, consultants, volunteers and others are fully aware of their responsibilities for the proper security of Library information. This policy document clarifies the obligations of such people and states what practices are acceptable. It also clearly identifies what would be deemed to be inappropriate security of such information and explains what action might result from such unacceptable use.

SCOPE: This policy applies to all National Library of Scotland employees, to Trustees and to others carrying out work for the Library including contractors, consultants, volunteers and any other such agents.

The policy is broadly in line with ISO 17799, but has been developed to meet the specific needs of National Library of Scotland.

This policy directly links to the following National Library of Scotland policies:

- Acceptable Use of ICT Equipment Policy
- Data Protection Policy

Contents

- Key Points4
- 1. Policy Ownership & Responsibilities5
 - 1.1 Scope5
 - 1.2 Guiding Principles5
 - 1.3 Review.....6
 - 1.4 Responsibilities6
 - 1.5 Independent Review.....6
- 2. Access Controls.....7
 - 2.1 Human Resource Security7
 - 2.2 Use of IT Systems and Networks8
 - 2.3 Enhanced Access Privileges8
 - 2.4 Access Management.....9
 - 2.5 Time-out Requirements.....9
 - 2.6 Secure Areas.....9
 - 2.7 Equipment Security Off-Site9
 - 2.8 Portable Media10
 - 2.8.1 Electronic Payments.....10
 - 2.9 Encryption11
- 3. Data Transfer.....11
- 4. Asset Management12
 - 4.1 Labelling Information and Media12
 - 4.2 Inventory.....12
 - 4.3 Ownership13
 - 4.4 Relocation of Assets.....13
 - 4.5 Secure disposal or reuse of equipment.....13
- 5. System Acquisition and Development.....15
 - 5.1 Approved Software and Hardware15
 - 5.2 Methodology15
 - 5.3 Development Concepts15
 - 5.4 Information System Integrity.....16
- 6. System Management.....17
 - 6.1 Security Administration Requirements17
 - 6.2 Audit Logging17
 - 6.3 Configuration and Change Management18
 - 6.4 Protection against Viruses and Malicious Code19
 - 6.5 Production Network19
 - 6.6 Separation of Duties.....19
 - 6.7 Sensitive Posts.....19
 - 6.8 Data Integrity20
 - 6.9 Capacity Planning and Scalability20
- 7. Business Continuity Planning.....20
 - 7.1 Backup20
 - 7.2 Redundancy21
- 8. Information Security Awareness and Training.....22
 - 8.1 Training22
 - 8.2 Information Security Training22
- 9. Audit and Compliance23
- 10. Incident Management.....24
 - 10.1 Reportable Incidents24
 - 10.2 Reporting Security Weaknesses24
 - 10.3 Responsibilities and Procedures25
 - 10.4 Staff Breaches.....25

Key Points

- We all need to work together to protect the information and information systems of National Library of Scotland
- Managers are responsible for ensuring compliance with this policy in their areas
- We need to treat sensitive information in different ways from other types of information
- Use of information system is subject to the Acceptable Use of ICT Equipment policy
- For sensitive or critical information systems, access will be based on providing users with the minimum level of information systems and system functionality to perform their duties
- National Library of Scotland ICT equipment may only be used off-site following written permission from the staff member's line manager. ICT equipment taken off-site should at no time be left unattended in public places
- National Library of Scotland ICT equipment should not be used by unauthorised users
- The Scottish Government requires all users of laptops, Blackberries, mobile phones and other portable equipment to protect the devices by password or PIN as a condition of their use
- It is strongly recommended that sensitive information not be stored on portable media, taken off-site or stored on non-National Library of Scotland equipment. If staff choose not to heed this advice then they will be held responsible for any breaches. ICT will provide software to encrypt data on all laptops, removable media and storage devices such as USB / flash drives to meet the Scottish Government's requirements
- Encryption is to be used for sensitive information that is stored in non-secure locations or transmitted over un-trusted networks such as the Internet
- Before releasing information on electronic media outside of National Library of Scotland, the information must be copied onto factory-fresh media (never used) or onto media that has been appropriately degaussed to prevent inadvertent release of sensitive information
- To ensure the integrity of National Library of Scotland systems, only software and hardware which have been approved by the ICT Manager (or his delegate) may be used in the production network environment
- All changes to National Library of Scotland's production network are to be performed in accordance with the ICT Change and Release Management policy
- All users must run virus protection software prior to using shared or retrieved files from workstations, laptops, removable media and other information systems
- All staff must participate in ongoing information security awareness and training activities at least once every two years
- Suspected breaches of this policy should be reported to the ICT Helpdesk

1. Policy Ownership & Responsibilities

National Library of Scotland has invested significant amounts of money and staff time to develop information systems that meet the needs of customers and staff. Information systems and the information stored in them are strategic assets vital to the business performance of National Library of Scotland. These strategic assets must be protected commensurate with their tangible value, legal and regulatory requirements, and their critical role in the Library's ability to conduct its mission. These information systems and resources belong to National Library of Scotland as an organisation rather than individuals or groups of individuals.

The intent of this policy is to ensure the creation and implementation of an environment that:

- Protects information and information systems critical to National Library of Scotland
- Protects information as mandated by legislation
- Protects the personal information and privacy of staff and customers
- Reinforces the reputation of National Library of Scotland as an institution deserving of public trust
- Complies with due diligence standards for the protection of information systems and resources
- Assigns responsibilities to relevant National Library of Scotland staff, managers, directors, contractors, partners and vendors
- Treats people as adults and implements technical restrictions to ensure compliance only where necessary

The definition of *sensitive* information in this document includes, but is not limited to:

- Personal information about individuals not generally available in the public domain
- Information that is commercial-in-confidence
- Information that is embargoed

This policy is concerned with the protection of information and information systems held by National Library of Scotland. However, the Freedom of Information (Scotland) Act may result in sensitive information being disclosed in certain circumstances; this is outside of the scope of this document. The Data Protection policy should be consulted for further guidance.

1.1 Scope

This policy applies to all information, in any form, related to National Library of Scotland business activities, staff or customers which has been created, acquired or disseminated using National Library of Scotland systems, brand or funding. Moreover, this policy applies to all technologies associated with the creation, collection, processing, storage, transmission, analysis and disposal of information. This policy also applies to all information systems, infrastructure, applications, products, services, telecommunication networks, computer-controlled equipment and related systems which are sponsored by, operated on behalf of, or developed for the benefit of National Library of Scotland.

1.2 Guiding Principles

The following principles guide the development and implementation of National Library of Scotland information policies and practices:

Information is:

- A critical asset that must be protected
- Freely available to staff, customers and other stakeholders
- Restricted to authorised staff for authorised uses when of a sensitive nature

Information security is:

- A cornerstone for maintaining public trust
- A business issue, not a technical issue
- Risk-based and cost-effective
- Aligned with National Library of Scotland priorities, industry-prudent practices and government requirements
- Directed by policy but implemented by business owners
- Everybody's concern

It has been decided to implement a modified version of the Scottish Government's Information Security policies because of the additional burdens that would have been placed on staff and customers; not to mention the cost. National Library of Scotland does not hold large quantities of sensitive information and this policy has been drafted accordingly.

1.3 Review

This policy will be reviewed annually to ensure it keeps up with changes in technology and industry best practice.

1.4 Responsibilities

While responsibility for information security ultimately lies with the Library's Accountable Officer, on a day-to-day basis this is delegated to the Director of Corporate Services. The ICT and HR Divisions are at the hub of implementing and managing information security policies, but information security is a multi-disciplinary activity requiring the input and support of all parts of the Library. The Senior Management Team takes information security seriously, with regular reports being given at the Board of Trustees and Audit Committee.

1.5 Independent Review

National Library of Scotland may have in place a standing relationship with a specialist external security consultancy organisation and shall use this organisation as a trusted partner to assist in ensuring that information systems security consistently complies with all necessary standards, is managed and implemented in accordance with this policy and that any security incidents requiring external assistance are dealt with rapidly and competently.

The normal regime of Internal and External Audit will be used to supplement the abovementioned reviews.

2. Access Controls

A security requirement is a type or level of protection that secures an information system. A control consists of safeguards designed to respond to a security requirement. National Library of Scotland uses the following three categories of security requirements to protect information systems according to their sensitivity and criticality:

- Baseline
- Mandatory
- Discretionary

Baseline. All information systems must implement controls sufficient to satisfy the baseline security requirements. Baseline security requirements have been established to protect National Library of Scotland's systems environment and infrastructure from intentional or unintentional unauthorised use, modification, disclosure or destruction.

Mandatory. Additional security controls must be implemented to satisfy the mandatory security requirements to protect sensitive, critical and business-controlled information systems and resources. Mandatory requirements are compulsory and are based on the sensitivity and criticality of the information system.

Discretionary. Additional security controls must be implemented to satisfy the discretionary security requirements to protect sensitive, critical and business-controlled information systems and resources. Discretionary security requirements are recommended based on the risk, sensitivity and criticality of the information system and its operating environment.

2.1 Human Resource Security

Employment Contracts. Anyone with access to systems containing sensitive information must have the following statement included in their contracts:

'You are authorised to access, use or disclose sensitive information only when you need to do so to perform your operational duties. Any other access, use, or disclosure may only be made on receipt of additional authority in accordance with the Library's Data Protection Policy.'

Before Commencement. All successful candidates for employment must gain satisfactory security clearance, including Disclosure Scotland clearance at the appropriate level, before commencing work.

Routine Separation. Routine separation occurs when an individual receives reassignment or promotion, resigns, retires or otherwise departs in honourable and friendly circumstances. Unless adverse circumstances are known or suspected, the individual will be permitted to complete his or her assigned duties and follow standard staff departure procedures. When staff leave under non-adverse circumstances, the individual's line manager must ensure the following:

- All National Library of Scotland property including keys, access cards, laptop computers, mobile phones and other ICT equipment are returned
- The individual's network username and building access authorisations are terminated, unless needed in the new assignment

- All sensitive information in the custody of the terminating individual is returned to its original location, to the Corporate Information Officer or is destroyed.

Adverse Termination. Removal or dismissal of staff under involuntary or adverse conditions includes termination for gross misconduct, involuntary transfer and departure with pending grievances. In addition to the routine separation procedures, termination under adverse conditions requires extra precautions to protect National Library of Scotland information systems and property. The line manager must:

- Contact the ICT Helpdesk immediately to suspend and take steps to terminate the individual's network username, access to National Library of Scotland information systems and building access authorisations
- Ensure prompt changing of all passwords and access codes used by the individual being dismissed
- Ensure the return of property and correct disposition of sensitive information as described under Routine Separation.

2.2 Use of IT Systems and Networks

The use of National Library of Scotland information systems is governed by the Acceptable Use of ICT Equipment Policy.

Authorisation is the process of determining whether, and to what extent, users should have access to information systems. Information systems must be configured to ensure that no user is allowed access to an information system or resource (e.g. transaction, data, process, etc.) unless authorised by appropriate National Library of Scotland management. Upon employment and agreement to the Acceptable Use of ICT Equipment policy staff will be granted access to a standard baseline suite of information systems and information technology services.

For sensitive or critical information systems, access will be based on providing users with the minimum level of information systems and system functionality to perform their duties. Systems and applications must define as many levels of access as necessary to prevent misuse of system systems and protect the integrity and confidentiality of National Library of Scotland information. National Library of Scotland information systems must be capable of imposing access control based on specific functions (e.g. create, read, update, delete, execute, etc.).

The following baseline information services may be authorised for users:

- Active Directory account (network logon)
- E-mail access
- Microsoft Office application
- Intranet and Internet access

Access to further information systems will require line management approval.

2.3 Enhanced Access Privileges

Staff and other people who require enhanced access privileges or administrator level access to National Library of Scotland information systems in order to perform their jobs will need to apply for a super-user account. These staff members will be required to abide by the Charter

for ICT Staff contained in the Acceptable Use of ICT Equipment policy. More information can be obtained by contacting the ICT Helpdesk.

2.4 Access Management

In order to provide a clear audit trail, all changes to account permissions must be documented. Before a user is given access to an information system the owner of the system must give written permission. A list of information system owners is available on the Intranet.

The account information, or database, must contain the following information for each user account:

- Username
- Group memberships
- Access control privileges
- Authentication information
- Security-relevant roles

If a user telephones the ICT Helpdesk in order to ask for a forgotten password to be reset, he/she must successfully authenticate him/herself. If a user is unable to successfully authenticate then he/she will need to visit the ICT Helpdesk in person with their identification before the password is reset.

2.5 Time-out Requirements

The inactivity time-out standard for National Library of Scotland non-public information systems is 30 minutes. After 30 minutes of inactivity the information system must, where the platform permits, automatically engage the password-protected screen saver or blank the screen and lock the keyboard to allow only the keying of the appropriate password.

2.6 Secure Areas

Sensitive information must be stored in a controlled area in accordance with National Library of Scotland policy. Information systems equipment must also be stored in controlled areas.

Suitable environmental controls shall be implemented and maintained at all times in NLS secure server and communications rooms to ensure uninterrupted ICT services for customers and staff.

To ensure continuity of service and prevent accidents, all persons must be formally authorised by the ICT Manager (or his delegate) before they enter secure areas that are under the control of the ICT Division. Physical access controls have been implemented to ensure that unauthorised persons do not enter secure areas. It is the responsibility of all authorised users of the secure areas to be aware of the detailed requirements of this standard, to behave in a way consistent with that standard and to alert management to any non-compliance that they notice.

2.7 Equipment Security Off-Site

National Library of Scotland ICT equipment may only be used off-site following written permission from the staff member's line manager. Where appropriate, permission may be granted for the staff member to use the equipment on an ongoing basis. The equipment must be returned to National Library of Scotland upon request by the line manager or the ICT Manager.

When permission for off-site use has been granted by a manager, the employee shall be reminded that he or she is responsible for ensuring continued compliance with all relevant policies, including the Acceptable Use of ICT Equipment policy. ICT equipment taken off-site should at no time be left unattended in public places. Laptops should be carried as hand luggage when travelling.

ICT equipment should not be used by unauthorised users. The appropriate staff member will be responsible for any damage to the equipment or release of information caused by unauthorised users (such as family members, customers or friends).

2.8 Portable Media

The Scottish Government requires all users of laptops, Blackberries, mobile phones and other portable equipment to protect the devices by password or PIN as a condition of their use. Detailed guidance on how to do this is available from the ICT Helpdesk. Users of portable ICT and removable media devices are reminded that they are responsible for the security of the data held on them when they are working off site and should not leave this equipment unattended in unsecured places, such as an unlocked car, or an unattended briefcase. ICT will provide software to encrypt data on all laptops, removable media and storage devices such as USB / flash drives to meet the Scottish Government's requirements. It is strongly recommended that sensitive information not be stored on portable media, taken off-site or stored on non-National Library of Scotland equipment.

Before releasing information on electronic media outside of National Library of Scotland, the information must be copied onto factory-fresh media (never used) or onto media that has been appropriately degaussed to prevent inadvertent release of sensitive information.

Procurement officers must ensure that contractors, consultants and auditors also comply with this instruction when they are on Library premises and are processing National Library of Scotland data on portable equipment and media.

2.8.1 Electronic Payments

The Library operates electronic payment collection facilities and these are subject to the controls expressed within the Information Security Policy. Payment information is particularly sensitive, therefore this section seeks to highlight the following areas:

- Service managers overseeing payment methods must review their area to ensure that adequate controls are in place to meet the required standards. The Finance Manager will oversee a review the Payment environment annually to ensure that adequate controls are in place throughout the Library.
- All staff must ensure that they comply with the controls outlined within the Information Security Policy:
 - Use of information systems (including employee-facing technologies) is subject to the acceptable use of ICT Equipment
 - Sensitive information will be classified as confidential and access to sensitive information systems will be restricted

- No sensitive authentication data will be stored (eg contents of magnetic strip, PIN or card validation number).
- Encryption will be used for sensitive information
- Strict control will be maintained over storage, accessibility and distribution of any kind of media that contains cardholder data
- Media will be classified so it can be identified as confidential
- There will be accurate tracking of media when it is transferred between locations
- Procedures will be in place to ensure management approval is obtained prior to moving media containing cardholder data
- Local Service Managers managing payment devices will ensure that their staff are adequately and formally trained particularly to ensure they are aware of the importance of cardholder data security.
- Any incidents involving security breaches relating to cardholder data will be reported immediately to the Finance Manager to ensure timely and effective handling of all situations.

2.9 Encryption

Encryption is the primary means for providing confidentiality services for information that can be stored or sent over the network, Intranet and Internet. Information systems that store or transmit sensitive information must have the capability to encrypt information. The minimum encryption standard for National Library of Scotland is triple DES with a 128-bit encryption key or the Advanced Encryption Standard (AES).

Information systems storing or processing sensitive information must implement approved encryption based on National Library of Scotland policies. Encryption is to be used for sensitive information that is stored in non-secure locations or transmitted over un-trusted networks such as the Internet.

Information systems using encryption must only use algorithms and standard encryption products that are approved by the ICT Manager and meet Government processing standards and industry best practice. All encryption products must support functionality of or integrate with applications to make encryption keys available to management. Any use of encryption without such technology must be approved in writing by the ICT Manager.

Encryption keys must be treated as sensitive information and access to those keys must be restricted on a need to know basis.

3. Data Transfer

National Library of Scotland has a duty under the Data Protection Act 1998 to process personal data securely and not to transfer data to a country or territory outside the European

Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In addition to the 27 EU member states and Iceland, Liechtenstein, and Norway, the European Commission has also recognised the following as providing adequate protection for personal data processing; Switzerland, Canada, Argentina, Guernsey, Isle of Man, the United States Department of Commerce's Safe Harbour Privacy principles, and the United States Bureau of Customs and Border Protection (transfer of air passenger records). This list is not static; the latest version is available at:

http://ec.europa.eu/justice_home/fsj/privacy/thirdcountries/index_en.htm.

Staff transferring sensitive data, either within the EU or elsewhere, are responsible for such transfers. Secure networks must be used where available; data sent via non-secure networks are to be encrypted. When sending sensitive data on portable media (e.g. USB memory sticks), the portable media must be password protected and the data encrypted; the data should be sent via a secure posting method such as special delivery.

Data transfer agreements between NLS and other organisations should be given formal approval by the Corporate Information Officer. This is to ensure that data shared will be protected by the other organisation in accordance with the obligations placed on National Library of Scotland.

If staff have any questions about data transfers they should contact the Corporate Information Officer or the ICT Helpdesk.

4. Asset Management

All National Library of Scotland information is to be properly handled and controlled based on the information sensitivity and criticality. Labelling, retention, storage, encryption, release and destruction of information must comply with established National Library of Scotland policies and procedures.

4.1 Labelling Information and Media

Sensitive information included on electronic media (e.g. disks, tapes) is to be legibly and durably labelled in accordance with National Library of Scotland policy.

4.2 Inventory

The ICT Division shall be responsible for maintaining the ICT Asset Register. The ICT Manager (or his delegate) shall review the register each quarter to ensure that it is being kept up-to-date.

The HR Division shall be responsible for maintaining the Corporate Information Asset Register. The HR Manager (or her delegate) shall quarterly review the register and ensure that it is being kept up-to-date.

The asset registers shall accurately record the details of each asset, the owner of the asset, its location and other relevant information.

4.3 Ownership

All NLS information systems have two nominated owners:

- ICT Owner
- Business Owner

The Business Owner is responsible for ensuring that the system meets the needs of the staff and customers using it and that the system adds value to Library activities. The Business Owner will be consulted with regard to system upgrades, planned downtime and related matters.

The ICT Owner is responsible for the technical administration of the system to ensure it runs effectively and is subject to business continuity planning. Each Owner must be a named postholder.

The ICT Owner shall be responsible for ensuring that the asset is:

- Accurately recorded in the NLS ICT Asset Register
- Properly protected against theft or misuse
- Properly maintained under an approved maintenance or support arrangement
- In the case of software, licensed in accordance with the supplier's licensing terms
- Only accessed by the persons properly authorised by the Business Owner and ICT Manager
- Is properly decommissioned in accordance with UK environmental legislation
- Wiped to securely remove all personal information before disposal

Responsibility for corporate information assets is detailed in the Data Protection policy.

Where an employee, who is an asset owner, leaves National Library of Scotland, the assets shall pass to the ownership of another suitable responsible employee and the Asset Register shall be amended accordingly. Human Resources shall ensure that this occurs as part of the HR exit processes.

4.4 Relocation of Assets

So that the ICT Asset Register can be kept up-to-date, ICT assets (other than designated portable devices) may only be moved after ICT has been notified. If a staff member wishes to have an ICT asset moved they should contact the ICT Helpdesk, request the change and give a brief explanation of why the move is necessary.

4.5 Secure disposal or reuse of equipment

All ICT equipment that has been earmarked for reuse shall be reconfigured by the ICT Division. This reconfiguration process will include erasure of all sensitive data stored on the equipment.

Surplus or redundant equipment will be disposed of in an economic and environmentally friendly manner, in accordance with the EU WEEE¹ Directive. All sensitive information and

¹ Waste Electrical and Electronic Equipment

all licensed software must be removed from ICT equipment or media before or during disposal to prevent inadvertent disclosure.

5. System Acquisition and Development

All hardware and software used on the production network is procured through the ICT Division. All software used on National Library of Scotland systems must be procured in accordance with National Library of Scotland policies and procedures and be licensed and registered in the name of National Library of Scotland. All staff must abide by software copyright laws and must not obtain, install, replicate or use software except as permitted by the software licensing agreements.

The Library has a responsibility to ensure that unlicensed software is not installed or used. In order to prove compliance with copyright legislation all software media and licenses shall be held by the ICT Division and stored in the Definitive Software Library. ICT will be responsible for maintaining a register of software licenses. The penalties for not using software in accordance with license terms are severe and may include time in prison.

5.1 Approved Software and Hardware

To ensure the integrity of National Library of Scotland systems, only software and hardware which have been approved by the ICT Manager (or his delegate) may be used in the production network environment. Approval will be given after the software and hardware have been tested and demonstrated not to affect other live systems. To obtain approval a formal request should be made to the ICT Helpdesk. The formal request process applies to:

- Purchased and licensed applications
- Shareware/freeware
- Other downloaded software
- Hardware not already approved by ICT

5.2 Methodology

The Acquisition of ICT Software and Hardware procedure (using the Project Management framework where appropriate) will be used when acquiring ICT equipment or services for use in the production network environment. The procedure ensures that systems are implemented which meet the needs of the end user plus also adhere to other National Library of Scotland policy. The main steps include:

- Identifying the business requirements and documenting them
- Procuring systems in accordance with procurement guidelines, interoperability/accessibility standards and other Library policy
- Ensuring the selected system works with the Library's other systems and the appropriate infrastructure is in place
- User acceptance testing
- Implementing the system
- Reviewing the implementation to ensure the expected business benefits have been achieved

5.3 Development Concepts

Information systems are to be developed under a formal system development methodology. Information security must be an integral part of the system development lifecycle whether development is done in-house, acquired or outsourced. Security must be addressed throughout the information system lifecycle process, from conception, design, development, deployment, operation to retirement from service. All development, acquisition or integration projects for information systems, whether performed in-house or by a business partner, must incorporate the following general lifecycle concepts:

- A comprehensive risk management approach
- A quality assurance programme that includes information security testing
- Rigorous configuration management and change control processes
- Separation of duties
- Restrictions associated with testing (test network separate from production)
- Information security in all phases of the information system lifecycle

5.4 Information System Integrity

Information system integrity ensures that information systems perform their intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation. Integrity provides assurance that under all conditions the operating hardware and software maintain logical correctness, reliability and effective protection mechanisms.

Information systems should comply with integrity requirements including, but not limited to:

- Security features designated in approved hardening guidelines must be invoked
- No information system may undermine the integrity of underlying platforms or supporting infrastructure
- The information system must perform integrity checks for system functions
- The information system must retain the existing security parameters even after a restart or recovery
- Backup capability must be provided to restore the information system to its former state
- Boundary checking must be implemented to prevent buffer overflow conditions
- The information system must provide appropriate alert messages before executing potentially damaging commands
- The information system must provide an administrator with the capability of retrieving the date and time associated with any security-related activity and the username of the user who initiated the activity
- The information system must monitor the status of its components in real time to ensure that all components are still active and to prevent components from failing without detection

6. System Management

6.1 Security Administration Requirements

Security administration functions that should be implemented for National Library of Scotland information systems include, but are not limited to:

- Activating protective features (e.g. requiring a username and password)
- Displaying users logged on
- Creating, retrieving, updating or deleting all security-related attributes of users, interfaces and software and data elements
- Overriding or altering vendor-provided security defaults
- Configuring security-relevant options
- Configuring the display of security-related events
- Recording and archiving the information system configurations
- Monitoring suspected activities related to a potential information security incident
- Detecting information security incidents promptly, isolating and investigating the problem and recovering securely from the incident

Security administrative requirements must be appropriately documented. These requirements include, but are not limited to:

- Cautions about functions and privileges that must be controlled when running a secure facility
- Administrator functions related to security, including adding or deleting users, changing user security permissions, generating keying material and revoking user-related security parameters
- Guidelines on consistent and effective use of security features, including their interaction and how to generate a new security configuration
- Guidelines for retaining accountability tracking information for an administrator-specified period of time
- Procedures necessary to start the information system in a secure manner
- Procedures to resume secure operation after termination of information system processes

6.2 Audit Logging

Audit logging is the process of recording operational and security-related events. All information systems must implement operating system level auditing and logging. Sensitive and critical information systems must implement application level auditing and logging. Information systems must support audit log capabilities including, but not limited to, independently and selectively monitoring (in real time):

- The actions of any user currently logged on and automatic lockout of that user if necessary
- The activities at a specified terminal, port or network address and automatic lockout of that input device if necessary

Audit logs must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred. Information systems must implement the following:

- Providing adequate information for establishing audit trails relating to information security incidents (as part of forensics analysis) and user activity
- Supporting administrator-selectable alerts for specified security-related events
- Recording the username accountable for the event
- Maintaining the confidentiality of authenticators (e.g. passwords) by excluding them from being recorded
- Protecting the audit log and its control mechanisms from modification, deletion or disabling of the function
- Generating real-time alarms of operational problems (e.g. running out of storage space) and audit log malfunctions
- Providing authorised individuals with access to enable retrieval, printing and archiving (copying to long-term storage devices) of audit log contents
- Providing administrators with audit analysis tools to selectively retrieve records from the audit log to produce reports, establish audit trails and perform other related functions

The information system must log security events including, but not limited to:

- All sessions established
- Invalid or unauthorized authentication attempts to access information systems
- System and database administrator actions
- Creation or changes in user or information system security accounts, profiles, ACLs, privileges and attributes
- Use of privileged accounts
- Creation, storage, or revocation of keying material
- Shutdowns, restarts, and backups
- Installation and updates of software
- Changes to logs

The information system must record event information including, but not limited to:

- Date and time of the event
- Username and MAC or IP address of the event initiator
- Event type and success or failure of the event if applicable
- Identification of information systems accessed
- Source host name and IP address generating the log event
- Destination host name and IP address generating the log event

ICT Systems staff review audit logs regularly and maintain a record of the review.

Audit logs, whether in electronic or physical format, must be retained for three years or as directed by National Library of Scotland policy.

6.3 Configuration and Change Management

All changes to National Library of Scotland's production network are to be performed in accordance with the ICT Change and Release Management policy.

6.4 Protection against Viruses and Malicious Code

All National Library of Scotland information systems must be protected against the introduction of viruses and other types of malicious code that can jeopardise information security by contaminating, damaging or destroying information systems.

All information systems must have active virus protection software installed and enabled. Unauthorised people must not modify the configuration of virus protection after installation. To ensure perimeter security, ICT will conduct scans for malicious code on the firewalls, FTP servers, mail servers, Intranet servers, Internet application protocols and other information systems as necessary.

Centralisation of automatic updates to virus software is key to updating information systems with the latest version of virus detection software and updated files of virus types (signature files). Virus protection software and signature files must be periodically updated or immediately updated whenever a new threat is perceived.

All users must run virus protection software prior to using shared or retrieved files from workstations, laptops, removable media and other information systems. All software, information or any other type of digital media must be tested by ICT to identify the presence of computer viruses and other malicious code prior to distribution to National Library of Scotland staff, customers, partners or the public.

6.5 Production Network

Only ICT staff are authorised to add or remove devices from National Library of Scotland's production network. Staff who breach this requirement have committed a serious breach of this policy and may be subject to disciplinary action and/or prosecution.

6.6 Separation of Duties

Staff, or other persons, with access to sensitive information systems should not be assigned duties that could cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud or collusion.

Security permissions are authorisation allocations and changes should be made by ICT staff rather than staff in functional areas of the Library. For example, Finance staff should not be able to change their permissions in the finance system without the involvement of a staff member outside of Finance.

6.7 Sensitive Posts

Sensitive posts include those in which staff could, in the normal performance of their duties, cause material adverse effect to National Library of Scotland information systems. Such duties include, but are not limited to:

- Making changes in the operating system configuration parameters, system controls and audit trails
- Modifying security authorisations
- Making revisions to sensitive programmes and data that could be undetected

Managers at all levels are responsible for taking a risk management approach to identifying posts in their areas and then requesting the HR Manager to designate the posts as sensitive.

6.8 Data Integrity

Data integrity is the security property that ensures that data meet a given expectation of quality and have not been exposed to accidental or malicious modification or destruction. Information systems must comply with data integrity requirements including, but not limited to:

- Information systems must have the capability to ensure that data are not modified, altered or deleted without authorisation either in storage or in transit
- Any unauthorised modification of data must yield an auditable security-related event
- The information system must have the capability of identifying the originator of any information before that information is used in any restricted function of the information system
- The information system must log any attempt by the administrator to authorise any user to bypass the administrator-configured data integrity controls
- Protect data integrity by performing data integrity checks
- When data integrity checks fail, the information system must reject the data

6.9 Capacity Planning and Scalability

For all information systems, capacity planning and scalability must be considered for both the information systems and network components such as routers, firewalls, proxies and encryption. Whenever technically feasible, scalable information systems should be considered that require little or no change to the configuration or the application when adding hardware or data storage.

7. Business Continuity Planning

National Library of Scotland, in continuing to meet its business continuity and contingency planning commitments, protects its staff and assets by implementing Business Continuity Planning (BCP). This reduces the likelihood and impact of a disruption to essential business functions for both itself and its customers. The BCP processes include, but are not limited to:

- Disaster recovery planning
- Relationship of criticality and Recovery Time Objectives (RTOs)
- Recovery testing for ICT facilities
- Backup of information systems
- Operational workarounds

The main business continuity plans are stored in Shadow Planner.

7.1 Backup

All information systems must have the capability to perform secure backups and recovery. The responsible Business Owner must agree the appropriate backup type and frequency with the ICT Manager (a list of Business Owners is available on the Intranet). All essential

components must be backed up on a schedule that is sufficient to meet the agreed Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

All essential components of an information system required for continued operation must be backed up. Backups will include, but are not limited to, operating systems, configuration files, general utilities, application software, data, supporting files and tables, scripts, standard operating procedures, specialised equipment and related documentation.

An inventory of backup media and supporting materials must be maintained. A copy of the inventory must be securely stored off-site or stored in a fireproof safe at the location. Backup media must be stored in a secure location, such as a fireproof safe. Backup media for critical applications and data must be stored off-site at a location that is not subject to the same threats as the original media.

Backup media for critical applications and data must be verified to ensure that backups are complete and can be read. Periodically the application/data and associated backup hardware and software should be tested with the backup media to ensure that application/data can be successfully restored and used. The information system must have the capability to check the integrity of data read from a backup file when performing a restore function.

7.2 Redundancy

Redundant systems for servers and firewalls may be recommended where warranted to ensure the availability of critical information systems. The implementation of redundant systems should be based on a cost-benefit analysis and the Recovery Time Objective.

8. Information Security Awareness and Training

All managers should incorporate information security into training courses, service talks and other tools to increase security awareness amongst staff.

8.1 Training

All new staff must receive information security training during their induction.

All staff must participate in ongoing information security awareness and training activities at least once every two years.

8.2 Information Security Training

For sensitive and critical information systems, appropriate operational security training must be developed and conducted.

9. Audit and Compliance

To ensure compliance with its information security policies, National Library of Scotland will monitor, inspect and audit.

Records should be managed in accordance with National Library of Scotland's information management policies, guidelines and the Data Protection Policy.

10. Incident Management

Information security incidents are events, whether suspected or proven, deliberate or inadvertent, that threaten the integrity, availability or confidentiality of information systems. The reporting of incidents enables National Library of Scotland to review the security controls and procedures; establish additional, appropriate corrective measures, if required; and reduce the likelihood of recurrence.

10.1 Reportable Incidents

Reportable incidents include, but are not limited to:

- Physical loss, theft or unauthorised destruction of National Library of Scotland information systems; e.g. missing or damaged hardware, software or electronic media
- Unauthorised disclosure, modification, misuse or inappropriate disposal of National Library of Scotland information
- Internal or external attempts to access information or the facility where it resides
- Unauthorised activity or transmission using National Library of Scotland information systems
- Internal or external intrusions or interference with National Library of Scotland networks such as denial-of-service attacks, unauthorised activity on restricted systems, unauthorised modification or deletion of files, or unauthorised attempts to control information systems
- Information systems with system software that is not patched to the current level
- Information systems with virus protection software that is not patched to the current level or is disabled
- Sudden unavailability of files or data normally accessible
- Unexpected processes, such as e-mail transmissions, that start without user input
- Files being modified, though no changes in them should have occurred
- Files appearing, disappearing or undergoing significant and unexpected changes in size
- Systems displaying strange messages or mislabelled files and directories
- Systems becoming slow, unstable or inaccessible
- Detection of unauthorised people in controlled information security areas
- Security violation, suspicious actions or suspicion or occurrence of embezzlement or other fraudulent activities
- Prohibited mass electronic mailings
- Illegal activities
- Violation of National Library of Scotland information security policies and procedures

10.2 Reporting Security Weaknesses

Incidents must be reported as soon as possible to the ICT Helpdesk.

10.3 Responsibilities and Procedures

All reported security incidents must be recorded and investigated promptly and thoroughly by ICT and, if appropriate, the Corporate Information Officer and Head of Security. ICT may also notify senior staff of the issue while the investigation is underway.

During the investigation, ICT shall give active consideration as to whether the access rights of any individual or group should be temporarily suspended.

Where a security or processing incident involves personal data, the Corporate Information Officer will advise on the impact on the Library's compliance with the data protection legislation and recommend appropriate action.

The ICT Division shall ensure that the information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

10.4 Staff Breaches

If a member of staff is suspected of breaching this policy then the process outlined in Section 8 of the Acceptable Use of ICT Equipment Policy shall be followed. This may ultimately mean disciplinary action being taken against a member of staff.