INFORMATION SECURITY POLICY

The National Library of Wales

November 2013

INTRODUCTION

Information is at the heart of what the National Library of Wales ('the Library') does and our most important assets are in the form of information. The Library is committed to enhancing access to and sharing of information and the security of the Library's information assets – be they part of the collections, about the collections, regarding the Library's management of the collection or related to other aspects of its business – is crucial to its success in achieving those aims. The Library is therefore firmly committed also to ensuring that its information assets are suitably protected in the interest of the general public, the organisation and others who may have rights subsisting in the information (such as data subjects and owners of intellectual property).

Information security is the protection of information from a wide range of threats in order to ensure legal compliance, business continuity, minimize business risk, protect reputation and maximize business opportunities. It concerns the preservation of confidentiality, integrity and availability of information and also involves authenticity, accountability, and reliability.

Much of the work of information security is the assessing of risks associated with a particular use of information, be that sharing, access, storage or processing. Risk assessments should identify, quantify and prioritize risks against criteria for risk acceptance and the Library's business objectives. The result of the risk assessments should guide and determine appropriate management actions and controls to protect against the risks.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the Library are met.

This Policy states the overall intention and direction in relation to information security and describes the measures adopted to ensure that the Library's information is adequately protected. It also sets out in general terms the framework for the sub-policies, procedures and guidelines for the implementation of those measures.

1. SCOPE AND DEFINITIONS

1.1 Who

This Policy applies to all staff of the Library and authorised users of the Library's non-public ICT facilities. Subordinate policies may also apply to readers, contracted suppliers and others.

1.2 What

This Policy aims to protect the information assets of the Library both in physical and electronic form. These include, but are not limited to: corporate financial and personal information, customer and reader information, catalogue information,

outputs of the Library's digitisation programmes, software both licensed and developed, email and communications, limited resources such as bandwidth and processing capacity.

1.3 Where

This policy applies within the Library but also covers the use of assets off-site and remote access to the Library's network.

1.4 Legal and Regulatory Issues

The Library and its staff are subject to the Data Protection Act 1998 (see the Library's Data Protection Policy), the Freedom of Information Act 2000, intellectual property law and other legislation governing the management of information.

1.5 Authority

This Policy is approved by the Executive Team and the Library's Board of Trustees.

The Policy shall be reviewed and developed by the Information Systems Strategic Committee and revisions shall be approved by the Executive Team.

1.6 Definitions

For the purposes of this Policy, the following terms and definitions apply.

asset	anything that has value to the organization
control	means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
DMZ	a perimeter network that exposes the Library's external-facing services to the Internet
incident	an information security incident is a single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening information security
integrity	assurance that information has not been modified
privileged account	an account on a system or application that has more permissions or abilities than a regular user account
threat	a potential cause of an unwanted incident, which may result in harm to a system or organization
vulnerability	a weakness of an asset or group of assets that can be exploited by one or more threats

2. ROLES AND RESPONSIBILITIES

2.1 Corporate responsibility

The Library's Board of Trustees is ultimately responsible for Library's compliance with the legal and regulatory requirements relating to information security.

Overall responsibility for information security within the Library's own organisation is assigned to the Executive Team.

The Information Systems Strategic Committee is the committee with responsibility for coordinating information governance, including information security, with a remit to direct, monitor and control the implementation of information security within the Library's own organisation. The Head of ICT is the technical security officer with responsibility for the security of information in electronic form within the Library's own organisation.

The Policy is reviewed and developed by the Information Systems Strategic Committee and any revisions must be approved by the Library's Executive Team.

2.2 Ownership of information assets

All information assets should have a nominated owner, which can be an individual or a committee. Information owners are responsible for maintaining information assets in accordance with the Policy, and they shall define, and where possible apply, the controls to those assets. Where systems and network administrators are needed to apply controls, they will work with the information owners to apply appropriate controls to meet the Policy's requirements.

2.3 Technical measures

The Head of ICT is responsible for the implementation of the technical measures specified in this Policy, its sub-policies and related procedures, in order to maintain the security of the Library's information assets.

2.4 Management responsibility

Managers are responsible for ensuring that assets within their area of responsibility are used in compliance with applicable security policies. Managers are responsible for ensuring that staff members receive appropriate security awareness training. Where appropriate, they must also ensure that job descriptions, statement of works for contractors and procurement terms and conditions include information security responsibilities.

2.5 Staff responsibility

All members of staff have a responsibility to ensure that they have read and are familiar with the Library's Policy, sub-policies and procedures relating to information security that are relevant to their work and to manage information accordingly.

<u>Violation of the Information Security Policy, whether deliberate or through</u>

negligence, may lead to disciplinary action being taken and/or access to Library facilities being withdrawn. In instances where the actions of the individual may be deemed unlawful, it may even lead to criminal prosecution.

3. PHYSICAL AND ENVIRONMENTAL SECURITY

3.1 Staff areas

The Library shall have measures in place to prevent unauthorised access to areas which should only be accessed by members of staff. The level of access control shall be adequate and proportionate to the nature of the information that it is intended to protect.

3.2 Secure areas

The Library shall designate server rooms, data storage locations and other areas containing information processing facilities as secure areas where appropriate. Secure areas shall:

- be protected by a physical security perimeter;
- be protected by auditable access control mechanisms to allow and deny physical access;
- have policies detailing who is authorised to access and under what circumstance.

3.3 Server rooms

Server rooms are secure areas as described above but additionally they shall have sufficient environmental controls to ensure correct operating conditions for the equipment and equipment failures shall be logged. Server rooms shall have:

- environmental monitoring systems to alert of any deviation from correct operating conditions;
- means of providing power to all critical systems in the event of a main electricity supply failure; and
- conditioned power to safeguard systems.

4. BUSINESS CONTINUITY AND DISASTER RECOVERY

4.1 Strategy

The Library shall incorporate information security into the Business Continuity and Disaster Recovery Strategy.

4.2 Backup

The Library shall incorporate Information Security into the Backup Policy to ensure the integrity and availability of assets, and to ensure that assets are protected adequately.

4.3 System Availability

The Library shall establish procedures for allowing limited downtime. These procedures shall establish who may decide to initiate downtime on which systems and under what circumstances. The procedures shall include authorisation from information owners and notification and communication with users.

5. INTELLECTUAL PROPERTY RIGHTS

5.1 Intellectual property rights

The Library's Intellectual Property Rights Policy shall state its position and practice with regard to the intellectual property owned and/or managed by the Library.

5.2 Licensed software

The Library shall carry out regular software audits to ensure that all software is properly licensed and that licence terms are observed.

5.3 Infringement of intellectual property rights

It is a disciplinary offence for Library staff to exploit their privileges in order to make illicit copies of items, physical or electronic, which are stored in the Library's collections or on its systems. The Library shall provide awareness sessions and training for staff as required in order to mitigate the risk of copyright being infringed unknowingly.

6. RECORD MANAGEMENT, ARCHIVAL STORAGE AND DISPOSAL

6.1 Records Management Policy

The Library shall ensure that Information Security is incorporated into its Records Management Policy.

6.2 Archived information

Archived information must be subject to controls as is live information.

6.3 Disposal or deletion of information

When information is disposed or deleted, an appropriate level of security must be observed. The Library's measures for secure deletion of information shall be detailed in the Data Deletion Policy.

7. NETWORK AND SERVICE SECURITY

7.1 Routers and switches

Network routers and switches shall be:

- physically secure by being located in secure areas or in locked cabinets;
- protected against main power supply failure for a limited time by alternative power sources;
- supplied by a conditioned power supply; and
- protected by suitable access controls to ensure that authorised users only may access or modify the configuration.

7.2 Network services and addressing

Network name services shall be configured so as not to expose names and/or addresses of machines providing internal services only.

Network addresses shall be predefined and registered for each network-attached Library device and may be configured on the device or allocated centrally when attached to the network.

7.3 Segmentation and access ports

The Library shall use Virtual Local Area Networks (VLANs) to segregate appropriately traffic on the Local Area Network (LAN). Each VLAN shall be documented as to its use and scope, including a policy on access.

Network ports in publicly accessible areas of the Library shall be subject to additional controls to ensure that the risk of unauthorised access to the LAN is reduced.

The Library shall not permit staff or users to connect unauthorised devices to the network that allow other devices to access the network, such as access-points or modems.

7.4 Sensitive traffic

Authentication credentials that grant access to systems shall be transmitted with effective encryption wherever possible.

Authentication credentials for privileged accounts shall be transmitted with effective encryption.

8. INFORMATION ACCESS CONTROL

8.1 Access Control Policy

The Library shall establish an Access Control Policy based on business and security requirements, relevant legislation and contractual requirements. The policy shall be documented and reviewed, and consider both physical and logical access to information.

9. TELECOMMUTING

9.1 Working from home

The Library shall describe the information security measures taken and the responsibilities of staff in relation to working from home in the Working From Home Policy.

9.2 Equipment

Staff shall be required to use Library supplied equipment only for telecommuting and remote working. Equipment supplied by the Library for such a purpose must not be used for personal use, and its use is subject to the Acceptable Use Policy. Staff working off-site on Library equipment shall also abide by the Library's Software Security Policy (see 14) and Backup Policy.

10. REMOTE ACCESS

10.1 Policies, sub-policies and procedures

The Library's Information Security Policy, sub-policies and procedures apply to staff accessing the library's network remotely as well as on-site and they should be observed by staff at all times.

10.2 Entry points

All remote access must be through designated remote-access entry points.

10.3 Communication

All remote access communication must be authenticated and encrypted to industry standards.

10.4 Logs and audits

All remote access must be logged and auditable.

10.5 Authorisation and documentation

All remote access provision must be authorised and documented.

11. REMOVABLE MEDIA

11.1 Removable Media Policy

The measures taken and the responsibilities placed on staff to ensure the security of information held on removable media shall be described in the Removable Media Policy.

11.2 Prevention of unauthorised use

The Library shall effectively control the use of removable media to prevent the unauthorised disclosure, modification, removal or destruction of assets.

11.3 Encryption

The Library shall supply and mandate the use of effective means of encryption to protect sensitive data on removable media.

12. INTERNET SECURITY

12.1 Firewall

The Library shall have a Firewall Policy maintained by the ICT Department that details the applications that are authorised to communicate in and out of the Library's LAN to the internet. The Firewall Policy shall be subject to effective change management.

12.2 DMZ

The Library's network shall be segmented to include a DMZ which is separated from the internal LAN by the internal firewall. All externally accessible services must be hosted within the DMZ.

12.3 Public machines and wireless network

The public wireless network and terminals provided for public use at the Library must be isolated from the Library's internal networks, with an effective firewall limiting their access to the Library's services.

13. USER SECURITY

13.1 Staff

The Library shall maintain an Acceptable Use Policy that details the rules for acceptable use of the Library's information assets and systems. As part of their terms and conditions of employment, all staff must agree to observe the Acceptable Use Policy.

13.2 Readers

The Library shall maintain terms and conditions of use for readers that include provisions for information security. When requesting a Reader’s Ticket, readers shall sign to show that they have accepted the Library’s terms and conditions of use.

13.3 Contractors

The Library shall maintain a Contractor Security Policy with rules for acceptable use of the Library’s information assets and systems. Contractors working on-site, accessing the Library’s network remotely or working off-site with Library information assets shall receive a written copy of the Contractor Security Policy which must be signed and returned before access is granted.

14. SOFTWARE SECURITY

14.1 Internal software development

The Library shall maintain a Software Development Policy that covers information security in software development.

14.2 Contracted software and third-party services

The Library shall mandate compliance with information security standards in contracted software development and third-party services. The Library shall check the implementation of contracted software or third-party services, monitor their compliance and manage changes to ensure that information security standards are met.

14.3 Commercial or packaged software

Commercial or packaged software shall not be modified without an exceptional business or operational need. Any such modifications should be fully tested and documented, and the original software retained.

15. MONITORING, COMPLIANCE AND INCIDENTS

15.1 Monitoring

The Library may, in accordance with its fair processing notices and Acceptable Use Policy and subject to existing legislation or regulation, review and/or monitor systems activities and network traffic to enforce the Information Security Policy, sub-policies and procedures. The Library may assign monitoring and other duties to appropriate administrators.

15.2 Security events

Where possible, the Library shall configure and keep logs to support the identification of security events. Administrators shall report any evidence of violation of policy or network security in logs as a security event.

15.3 Security testing

Testing for security vulnerabilities shall be undertaken by authorised and specialist staff. The Library shall document all staff authorised to test for security vulnerabilities and the scope and duration of the testing.

Exceptions during software development shall be detailed in the Software Development Policy.

Users shall not install, download or use tools to manage and test information security without authorisation.

15.4 Incident management

All staff, contractors and third parties have a responsibility to report security events

through appropriate channels as soon as possible.

The Library shall have responsibilities and procedures in place to evaluate and handle security events.

The Library shall have mechanisms in place to quantify, monitor and assess the impact of security incidents.

16. POLICY REVIEW

16.1 Review

This Policy and its subordinate policies shall be reviewed every two years or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. The Information Systems Strategic Committee shall have responsibility for reviewing and developing the Policy.

End.