Information Technology Security Policy

Date: January 2021

Policy Information	
Policy Title	Information Technology Security Policy
Policy Number:	POL 032
Version	6.0
Policy Sponsor	Directory of Business Support
Policy Owner	Head of ICU/ICT
Committee and date recommended for approval	Business Support Committee 28 January 2021
Date approved by the Board	11 February 2021
Equality Screening Status	Screening Reviewed: 12 January 2021
Rural Needs Impact Assessment Status	Rural needs impact assessed: 12 January 2021
Date Set For Review	January 2024
Related Policies	POL029 Server Security Policy POL030 Network Security Policy POL031 Internet Security Policy POL033 Microsoft Windows Client Security Policy POL034 Application Security Policy POL035 LNI Staff Acceptable Use Policy

1. Introduction

This policy applies to all employees whether full time or part time, seconded staff, temporary staff and agency staff, contractors, IT Suppliers, consultants and associates. It also applies to customers of Libraries NI (LNI) who have been given access to the information assets within any Library location.

The LNI Information Security Manager owns this policy. The LNI Information Security Manager is responsible for information security across LNI and is the initial point of contact for all queries regarding information security and the content of this policy.

Section 3 of this policy sets out the information security policy statements applicable to Libraries NI.

Information Security

This Policy is aligned with ISO27001 and is underpinned by a number of supporting policies, which cover all aspects of information assurance.

Information is an asset, which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to safeguard customers and staff, ensure business continuity, minimise business damage and maximise operational efficiency.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected and is subject to the provisions of this policy document.

Information security is characterised here as the preservation of:

- *confidentiality*: ensuring that information is accessible only to those authorised to have access
- *integrity*: safeguarding the accuracy and completeness of information and processing methods
- *availability*: ensuring that authorised users have access to information and associated assets when required.
- *legal/compliance ensuring compliance with all applicable legal and regulatory requirements*

Information security is achieved by implementing a suitable set of countermeasures, including policies, practices, procedures, organisational structures and technical measures.

2. Purpose

The objective of information security is to ensure the business continuity of Libraries NI and to minimise risk of damage by preventing security incidents and reducing their impact.

The aim of this policy is to enable Libraries NI to use and share its information with confidence and to reduce to an acceptable level the potential harm and risk of an information security incident through having suitable safeguards against threats whether internal or external, deliberate or accidental, to ensure the confidentiality, integrity and availability of Libraries NI information systems. It aims to do so in accordance with its contractual, statutory and regulatory obligations for information assurance, its business and operational requirements and the costs and logistics of implementing such controls.

3. Information Security Policy

This information security policy aims to provide direction and guidance to users of LNI information and information systems and the security controls that are to be implemented and complied with.

3.1 Definitions

- **information assets**: Assets (equipment or systems or data) that are created or purchased for business operational purposes
- **information assurance:** Operations, processes and procedures that protect and defend information and information systems by ensuring their availability, integrity, authentication and confidentiality. This includes providing for the restoration of information systems by including protection, detection, and reaction capabilities
- **information system**: A system for generating, sending, receiving, storing or otherwise processing electronic communications
- **confidentiality**: Ensuring that information is accessible only to those authorised to receive it and so only disclosed for legitimate purposes
- **integrity**: Safeguarding the accuracy and completeness of information and information processing methods
- **availability**: Ensuring that authorised users have access to information and associated assets when required.

3.2 Risk Assessment

Consideration of risk is essential to this Information security policy. Libraries NI will ensure that a security risk assessment is conducted on the Libraries NI environment in order to determine the risks associated with the service and enable selection, implementation and maintenance of suitable security controls following formal risk management process. The security and control procedures required will take account of the sensitivity and value of information and the requirements for business continuity.

Responsibility for conducting and maintaining the risk assessment and the risk management process along with implementation of controls will lie with the Libraries NI Information Security Manager.

Where services have been outsourced to a third party, the third party is responsible for ensuring that an appropriate risk assessment, against the services being provided to Libraries NI is undertaken and maintained.

Information Security Policy Statements

The following section provides the high–level direction for Information security at Libraries NI and is underpinned by a number of supporting policies, including:

- Libraries NI Staff Acceptable Use Policy
- Byelaws
- Library Computers Conditions of Use
- Application Security Policy
- Microsoft Windows Client Security Policy
- Internet Security Policy
- Network Security Policy
- Server Security Policy
- Data Protection Policy.

Libraries NI is committed to maintaining and improving information security within all aspects of the Libraries NI environment, (Services and Business Support) and all staff, third party, contractors, and public users of the services shall ensure that:

Protection of Data

Libraries NI staff and their IT Suppliers will take all necessary steps to prevent, detect and recover from any loss or incident, whether accidental or malicious, including error, fraud, damage and disruption to, or loss of computing or communications facilities.

Operating procedures will be documented and designed to minimise the risk of loss of data within the Libraries NI IT environment.

In particular, data will be backed up regularly, with a copy kept in secure off-site storage.

Organisation of Information Security

- management are committed to ensuring the information security of Libraries NI environment;
- information security responsibilities will be defined and allocated
- appropriate contacts with relevant authorities and special interest groups shall be maintained.

Asset Management

- assets are to have an assigned owner and be documented in an appropriate inventory
- assets should be classified and labelled in accordance with their respective protective marking. It is the asset owner's responsibility to determine the appropriate protective marking
- assets are to be handled in accordance with their respective protective marking.

Human Resources

- all individuals, including, staff, third parties, subcontractors involved in the management of the Libraries NI environment will be subject to appropriate screening prior to being granted access to the environment
- staff, including third party suppliers where applicable, in contact with children or vulnerable adults are required to obtain Access NI up to enhanced level prior to being permitted on site. Where access to sensitive material is required and such clearance is in progress of being processed; the individual(s) will be escorted for the duration of their visit by appropriately cleared Libraries NI staff;
- all individuals involved in the management of the Libraries NI environment will have received appropriate information security awareness education and training
- formal Joiners and Leavers processes will be established to ensure that only authorised access to information and systems is provided and such access is removed when no longer required
- non-compliance with this policy may result in disciplinary action being taken.

Physical Security

- all assets including equipment that is part of the Libraries NI environment will be protected physically against misuse;
- all critical business equipment, including servers, sited outside the data centre will be located in a secure area which is not accessible by the general public, is only accessible to authorised persons and is contained in a locked cabinet or room. Access to such rooms should be monitored
- security of equipment located at Libraries NI sites will be the responsibility of Libraries NI
- all equipment will be protected against all forms of malware and virus by appropriate means as agreed with the Information Security Manager.

Communications and Operations Management

- all operational procedures will be documented, including formal change control and procedures
- no changes to systems and networks will take place before the security implications are assessed, appropriate controls applied and required approvals are obtained
- capability management function is to be in place, supported by system planning and acceptance criteria
- regular backups are to be taken. In particular, data will be backed up regularly, with a copy kept in secure off-site storage
- all equipment will be protected against all forms of malware and virus by appropriate means
- infrastructure and system monitoring controls are to be in place to ensure that system alerts and anomalies are detected and addressed
- appropriate network controls and network security controls will be implemented and maintained to enable secure, authorised network traffic flow.

Access Control

- access to the IT environment, both Libraries NI and Public, will be, where appropriate, by individual user account. All users will be required to comply with minimum password standards appropriate to the user group from which they come
- for all types of access, the principle of least privilege will be applied
- where privileges are granted, a record will be maintained of such privilege, including details of duration, approval and who has been assigned the privilege along with a justification
- all privileged accounts will be reviewed on a regular basis to determine if they are still required
- formal user registration and deregistration process will be established, implemented and maintained
- password management controls will be in place to ensure that passwords are of a suitable complexity and require changing at agreed intervals, with system administrator passwords must be subject to more frequent refresh than normal user account standards. Staff should receive security awareness training around password usage and management
- network controls will be implemented and maintained to ensure the security of the Libraries NI network and protect against unauthorised access
- the Information Security Manager must give explicit permission before any new external connections from the Libraries NI environment are implemented. Such permission will generally be granted for a period of one year, after which time it will need to be renewed
- connections to public networks will only be permitted from the Data Centre. All such connections will be made in a manner that minimises the risk of unauthorised access from the public network.

Information Systems Acquisition, Development and Design

- information security will be considered when acquiring, developing and maintaining information systems and security considered at the requirements analysis stage reflecting the business value of the information assets involved
- controls for ensuing correct processing in applications will be established and checked to ensure information is not corrupted during processing
- live data will not be used for testing
- the source code for existing systems and newly developed applications will be kept in the Definitive Software Library maintained under Configuration Control in accordance with the Release Management Process
- changes will be subject to formal change control procedures
- controls will be developed to ensure that technical vulnerabilities are reported upon identification.

Information Security Incident Management

- security incident Management reporting procedures are to be documented and communicated to all staff and third parties
- all security incidents must be reported by employees in line with the Security Incident Reporting Process.

Business Continuity Management

- business c ontinuity plans will be in place for the Libraries NI, and tested at regular intervals.

Note: IT Disaster recovery testing must be carried out at agreed intervals

Compliance

- all users accessing the Libraries NI environment must comply with all relevant legislation and regulation in addition to the provisions of the security policy.

Accountability and Responsibility

All users of and providers of services to Libraries NI are responsible for ensuring that they are aware of and comply with this policy at all times.

The Information Security Manager is responsible for ensuring that this policy is kept up to date and made available to all applicable parties.

All Libraries NI employees whether full time or part time, seconded staff, temporary staff and agency staff, contractors, consultants and associates are required to be aware of policy details and to comply with these at all times. Failure to comply with this policy may result in disciplinary action being taken.

Customers of Libraries NI who have been given access to the information assets within any Library location are required to be aware of and comply with conditions of use at all times when using and accessing Libraries NI information Assets. Failure to comply with this may result in removal of access rights and usage of Libraries NI services

Third parties and contractors providing services to Libraries NI are responsible for ensuring that they comply with this policy in all activities undertaken in delivery of services to Libraries NI under the applicable agreement. Failure to comply with this policy may result in breach of contract.

4. Waiver from Policy

Request for a waiver from this Information Policy must be address to the Information Security Manager. The request for a waiver must describe why a waiver is required, justification why the policy cannot be adhered to, and a plan to bring the application or system into compliance in the future. The Information Security Manager will discuss waiver requests with senior management, as appropriate.

Waivers can be granted by the Information Security Manager for a period not exceeding one year, but may be extended annually if the justification still applies.

5. Monitoring and Review

The Information Security Manager is responsible for monitoring and reviewing this policy and will conduct a formal review of the efficiency and effectiveness of its application on an annual basis.

6. Violations

Any violations of this security policy should be brought to the attention of the Information Security Manager, who will work with the appropriate individuals to rectify the problem.