libraries ni

Internet Security Policy

Date: January 2016

Policy Title	Internet Security Policy
Policy Number:	POL 031
Version	4.0
Policy Sponsor	Director of Business Support
Policy Owner	Head of ICU / ICT
Committee	Business Support Committee.
Date Approved	
Date Screening Documentation Signed	
Date Set For Review	December 2018
Related Policies	POL029 Server Security Policy POL030 Network Security Policy POL032 Information Security Policy POL033 Microsoft Windows Client Security Policy POL034 Application Security Policy POL035 LNI Staff Acceptable Use Policy

Document Control

Version	Status	Revision Date	Summary of Changes	Author
0.1	*Draft*	21/12/2013	Initial copy from customer	
0.2	*Draft*	04/06/2013	Updated to reflect new service and contract being delivered by Fujitsu	Inderjit Birak
0.3	*Draft*	25/06/2013	Updated following review by Solution Owner	Inderjit Birak
1.0	*Final*	12/11/2013	Programme Board Approval	e2 Project Team
1.1	*Draft*	16/01/2014	Updated to LNI e2 standards	Jamie Aiken
2.0	*Final*	06/02/2014	Programme Board Approval	Jamie Aiken
3.0	*Final*	18/032014	Information Systems Committee Approval	Jamie Aiken
3.1	*Draft*	05/12/2015	Minor changes suggested by SMT	Jamie Aiken
4.0	*Final*	01/2016	Approved by BSC	Jamie Aiken

1. Introduction

This document forms part of the suite of Security Policy documents for Libraries NI.

The Libraries NI environment provides IT services to all Library locations in Northern Ireland.

The Authority will take appropriate steps to protect the IT environment from threats, including but not limited to unauthorised access, computer viruses, violation of privacy and interruption to service.

2. Purpose

This document lays down the minimum security standard applicable to the interconnection of the Libraries NI IT environment to the Internet.

3. Policy

3.1 Location of Connection

Connections between the Libraries NI environment and the Internet should be made only via a central point such as a Central Data Centre.

> **Control Statement**: Connections from the Libraries NI environment to the Internet that bypass the Data Centre are **not** permitted.

3.2 Firewalls

Control of traffic between the IT environment and the Internet, in both directions, is a key requirement of the Libraries NI IT environment. In particular, only certain types of inbound connection are permitted, and for outbound connections security measures must be applied to filter the content.

> **Control Statement**: All traffic between the IT environment and the Internet will pass through a firewall or equivalent device configured to prevent unauthorised access between the networks.

Data Centre systems must be protected from unauthorised access from the client machines around the IT environment.

> **Control Statement**: Traffic between the Data Centre and the client machines around the IT environment will pass through a firewall or equivalent device configured to prevent unauthorised access between the networks.

Control Statement: The Data Centre firewalls will be configured as a high availability pair in the primary DC allowing for fault tolerance and resilience; these will control all communications for all services. Disaster Recovery services will additionally be available in the secondary DC for failover purposes so the threat and exposure to defects are minimised.

The software running within the firewalls must be kept up to date, in order to provide a continuing barrier against unauthorised access.

Control Statement: Firewall security updates and patches must be applied within one week of release by the vendor. Assessment of vulnerability for firewall updates and patches will be made prior to application and will be subject to testing prior to commissioning. Considerations will need to be made so that service remains unaffected and scheduled accordingly.

All security updates and patches will be subject to formal change control procedures.

3.3 Intrusion Detection

System access control and audit will be managed to ensure that only authorised access is permitted.

Control Statement: appropriate controls will be implemented into the system through firewall proxy, network and filtering systems to ensure that unauthorised access can be detected.

3.4 Web Proxies and URL Filtering

Web browsing will take place through Web proxies in order to make best use of the available Internet bandwidth. URL filtering will be deployed to restrict access to undesirable sites. The level of filtering will be dependent on the type of users and additional levels of filtering must be implemented for Child Users.

Control Statement: All Web Browsing will take place through web proxies implementing URL filtering.

3.5 Web Publishing

Web Servers that publish content to the Internet will be protected from unauthorised access, and will be carefully hardened. Procedures will be implemented to ensure no unauthorised web publishing takes place from the IT environment.

Control Statement: All Internet-facing Web Servers in the IT environment will be behind at least one firewall or equivalent device.

Control Statement: Internet-facing Web Servers will have unnecessary services removed or disabled.

Control Statement: Uncontrolled web publishing from within the IT environment will not be permitted.

Control Statement: access to web servers will be limited to authorised personnel only.

Control Statement: All changes to Web Servers will be subject to change control procedures

3.6 Email Filtering

All email between the Internet and the Libraries NI IT environment will be filtered to remove undesirable content such as viruses and inappropriate material and content.

Control Statement: Email filtering systems should be implemented within the IT environment.

Control Statement: There must be no direct path between the Libraries NI email servers and the Internet, bypassing the email filtering systems.

3.7 Virtual Private Networking

Limited inbound VPN access will be provided to the IT environment from the Internet, and must be suitably controlled.

Control Statement: Inbound VPN access to the IT environment will only be permitted on the authority of the Information Security Manager.

Control Statement: Firewalls will, wherever possible, restrict the parts of the IT environment that can be accessed by a particular user over the VPN.

3.8 Monitoring and Reporting

All traffic between the IT environment and the Internet, in both directions, will be logged and monitored. This will include logging at the firewalls, email filtering systems, and web proxies.

Control Statement: Appropriate logging will be enabled on all firewalls, email filtering systems and proxies within the IT environment.

Control Statement: Logs will be archived periodically, and stored for a period not less than twelve months.

Control Statement: Logged information will be monitored, and significant events will be followed up.

Control Statement: Significant events within the Internet logs will be followed up on a daily basis.

Control Statement: Security incident will be raised where monitoring reveals breach of security policy.

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.