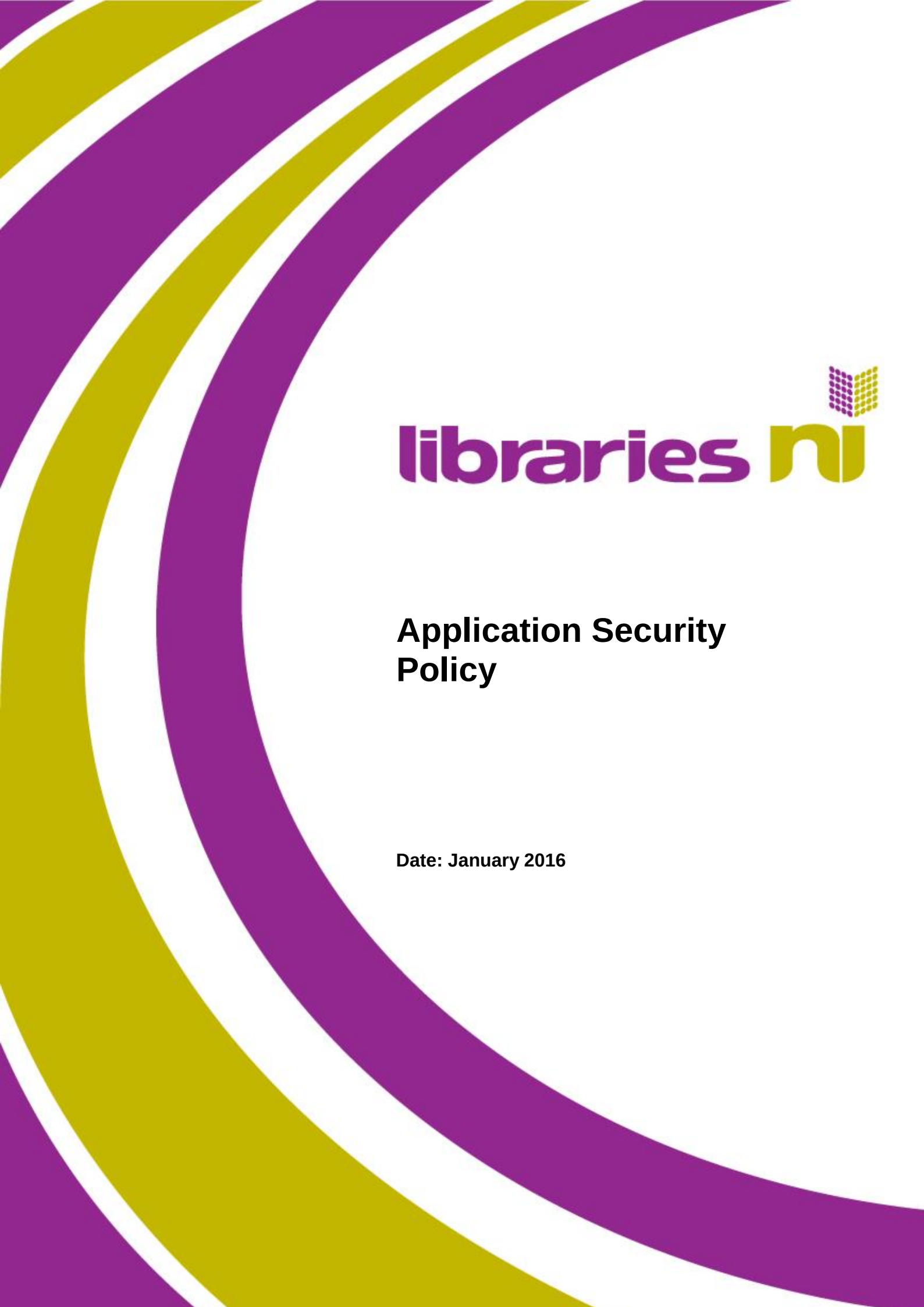

# Application Security Policy

**Date: January 2016**

| | |
|---|---|
| **Policy Title** | Application Security Policy |
| **Policy Number:** | POL 034 |
| **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<br>POL030 Network Security Policy<br>POL031 Internet Security Policy<br>POL032 Information Security Policy<br>POL033 Microsoft Windows Client Security Policy<br>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 applications used in Libraries NI. All such application software is considered to be at high-risk, but some particularly high-risk systems will need to take additional security steps beyond those prescribed in this document.

This Application Security Policy applies to all information systems and information system components of the IT environment. Specifically, it includes:

- Servers and other devices that provide centralised computing capabilities.
- SAN, NAS and other devices that provide centralised storage capabilities.
- Desktops, laptops and other devices that provide distributed computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.

## 3. Policy

In order to accurately create a security standard to control applications, it is necessary to first define the types of application software that will exist in Libraries. These may be categorised as follows:

### 3.1 Standard Applications

A standard application is one that is included on the list of permitted applications, contractually agreed by the Authority and its supplier(s). Specifically, applications of this nature will fall into one of three categories: Library Management Applications, Office Productivity Applications and Administration Applications.

New applications may be added to the list of Standard Applications on the request of the Authority and agreed with their supplier(s)

**Control Statement:** Standard documentation shall be produced describing the standard configuration of applications within the IT environment.

**Control Statement:** Deviations from the standard builds shall be documented.

## 3.2 Non-standard Applications

A non-standard application is a manually installed package that is not part of the contractually agreed application list. For example, this would include applications manually installed by a supplier on an ad-hoc basis at the specific request of a Library or the Authority. Applications of this type should follow the principles of the standard applications and may be reviewed by the Authority to see if they should become part of the standard applications list.

## 3.3 Unauthorised Software

Unauthorised software incorporates any piece of software that is installed on any workstation or server in a library without the prior knowledge of the Authority or their supplier(s). This includes, but is not limited to, rogue software, Trojans, viruses, games, protocol analysers, freeware, shareware, communication software, and any other software that permits or promotes hacking, system intrusion or system performance degradation.

The Information Security Manager reserves the right to remove software of this nature if it poses an issue on any system in a library site.

## 3.4 Control of Applications

Due to the nature and variety of applications that will be used in the IT environment a measure of control over applications will be required to ensure continuity of service. Security, performance and availability may become compromised due to the introduction of non-standard or unauthorised software. In order to prevent disruption to service from such software, the following steps are required:

**Control Statement:** The Information Security Manager shall evaluate all new applications to determine their suitability for installation in the IT environment. Any application that is deemed unsuitable shall be rejected by the Information Security Manager and therefore not installed in any Library site.

**Control Statement:** Group policies shall be set such that ordinary users cannot normally install or remove applications from machines in the IT environment.

**Control Statement:** The Information Security Manager shall retain the right to remove any piece of software that is deemed unsuitable or unacceptable to the environment in any Library site. This includes any software on IT equipment that may impact availability or key performance indicators.

**Control Statement:** The installation of unauthorised software is not permitted on any server or workstation.

**Control Statement:** The Information Security Manager shall keep a list of software that is not permitted and may amend this list at any time.

**Control Statement:** A list of all authorised software licences will be maintained.

In order to comply with legal requirements, only licensed software will be installed on machines.

### 3.5 Application-level Authentication

Some applications require their own authentication within the application. Where possible, they should not use an embedded authentication database in order to limit the number of places authentication information is stored, however it is accepted that most of the chosen database applications behave in this way.

**Control Statement:** Where possible, applications that require authentication should be configured to use Windows Active Directory authentication or equivalent directory service.

**Control Statement:** The Authority must ensure that default passwords on databases with embedded authentication are changed after installation.

**Control Statement:** default passwords on applications are to be changed on first login.

**Control Statement:** Passwords within Applications must have the appropriate complexity as defined in the password policy.

**Control Statement:** Where possible, establish a unique identifier and secret information for each application - but as a minimum establish a unique identifier for each application.

**Control Statement:** The application should be identified to the system.

**Control Statement:** Access to application system files should be controlled.

## 3.6 Changes to Application Software

From time to time, software patches and upgrades are issued to application software, to fix performance and security issues, and to enhance functionality. Critical updates shall be applied to all applicable machines in a timely manner.

**Control Statement:** All changes to the existing standard software builds and application software shall be made in compliance with applicable Change Control Procedures.

**Control Statement:** All patches and upgrades to the existing standard software builds and application software will be tested before they are applied to production environment and machines.

**Control Statement:** The Information Security Manager will ensure that all critical patches are applied in a timely, managed and controlled manner.

## 3.7 Critical Application Parameters and Resource Configuration

### 3.7.1 Application Service Accounts

Some applications will require a Microsoft Windows service account, application logon account or Windows logon account. These accounts must be subject to the same security rules as the operating system accounts.

**Control Statement:** Accounts used by applications shall have passwords of at least 8 characters in length and require a combination of alpha numeric text.

**Control Statement:** The Authority shall ensure that accounts used by applications must not use the default password provided for that application after the installation process.

**Control Statement:** Accounts used by applications should not use the default username provided for that application.

**Control Statement:** Critical applications using Windows Account passwords shall be configured with the 'Password Never Expires' flag set.

**Control Statement:** Accounts used by applications shall be given the least possible privileges and rights necessary to allow the required functionality of the applications.

**Control Statement:** Where privileges and rights are granted to accounts used by applications, these privileges and rights are to be reviewed on regular basis to ensure that privileges and rights that are no longer required are removed.

### 3.7.2 Application Development

Security must be included in the design, development or deployment of an application. Development processes should follow generally accepted standards of good practice. Risk assessment should be conducted to ensure that the proposed application will not introduce risk to the IT environment and Information assets.

**Control Statement:** Secure coding practices shall be followed for all application development.

**Control Statement:** when developing applications, input, output and processing validation assessment must be undertaken to ensure information is not corrupted during processing**.**

**Control Statement:** Applications will be subject to testing prior to being introduced to live environment, to ensure that data is being processed correctly, ensuring the integrity of the data being input, processed and output.

**Control Statement:** During development and testing, applications shall not have access to live production data.

**Control Statement:** Change control procedures are to be followed when implementing the application into Live environment.

### 3.7.3 Software Maintenance

Only authorised software maintenance personnel will be permitted to carry out maintenance tasks. This will be ensured by controls including:

**Control Statement:** The identity of software maintenance personnel must be checked immediately on arrival, and before any physical access is permitted;

**Control Statement:** A contract must exist with the software maintenance company prior to any work being carried out; and

**Control Statement:** Normal operating controls such as supervision, restriction of access to operational data, and controls over the ability to take soft or hard copies of the data, will apply

## 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.