Microsoft Windows Client Security Policy

Date: 25 January 2024

Review Date: January 2027

Connect with us
www.librariesni.org.uk

Policy Information	
Policy Title	Microsoft Windows Client Security Policy
Policy Number:	POL 033
Version	7.0
Policy Sponsor	Directory of Business Support
Policy Owner	Head of ICU/ICT
Committee and date recommended for approval	Business Support Committee 25 January 2024
Date approved by the Board	08 February 2024
Equality Screening Status	Screening Reviewed: 15 January 2024
Rural Needs Impact Assessment Status	Rural needs impact reviewed: 15 January 2024
Date Set For Review	January 2027
Related Policies	POL029 Server Security Policy POL030 Network Security Policy POL031 Internet Security Policy POL032 IT Security Policy POL034 Application Security Policy POL035 LNI Staff Acceptable Use Policy

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 Microsoft Windows based PCs, supplied by Libraries NI and operating within Library sites across Northern Ireland. It is suggested that the statements and recommendations laid down in this standard are similarly applied to both Libraries NI and public devices, for which ongoing responsibility lies with the Authority.

Some systems in particularly high-risk environments may need to take additional security steps beyond those prescribed in this document. This may include, but is not limited to, ongoing anti-virus provision.

3. Policy

The standards and recommendations laid down in this section should be adhered to for client PCs running Microsoft Windows operating systems.

3.1 Directory Services

3.1.2 Security domain boundaries

Microsoft Windows client PCs will have computer accounts created in the Active Directory during the client build process.

3.2 Hardware Configuration

BIOS passwords

BIOS passwords shall be used to prevent unauthorised access to the BIOS, on client machines in Library sites. This helps prevent unauthorised alteration of the configuration of the machines.

BitLocker

BitLocker drive encryption should be enabled on LNI laptops. This helps reduce the risk of data theft or exposure of data from lost, stolen or decommissioned computers.

Boot sequence

Once a client has been installed, it should always boot from the hard drive first. The boot order will be protected by the BIOS password set-up, as specified above.

Control Statement: All Windows clients shall be set to attempt to boot first from hard disk, then CD/DVD or other devices.

Action after outage

BIOS configuration parameters allow a choice of actions following system outages such as power failures and system crashes. An important consideration is a power outage in out of hours and so for this and other reasons, client PCs should not be set to reboot automatically after an outage.

All Windows clients should be set not to reboot automatically after any outage.

3.3 System Software

Software upgrades and installation

All Windows clients shall be installed to a standard build. This minimises the effort subsequently required to support individual systems. Deviations from the standard build should be documented and justified.

Control Statement: Windows clients shall be installed to a standard build.

Control Statement: Deviations from the standard build shall be documented.

Control Statement: During installation, the Windows time zone shall be set to the appropriate local setting, and the “Automatically adjust clock for daylight saving changes” shall be selected.

Control Statement: During installation, the Windows Regional Settings shall be set to the appropriate local setting.

Control Statement: During installation, the Windows client PCs shall be configured to use a suitable automatic time source that is synchronised to the regional time.

Control Statement: Libraries NI staff PCs, workstations and where possible mobile devices, will be configured to automatically lock after a preconfigured period of time to prevent unauthorised use.

Control Statement: Public Access Terminals (PATs) PCs will automatically logout at the end of a session and Deep Freeze will clear session data.

Control Statement: The system shall require that the Identification and Authentication process is repeated to unlock the device before work can be continued.

Control Statement: A warning screen, which is displayed prior to log- on at PCs and

workstations, will warn the reader that unauthorised access to systems may result in disciplinary or legal action being taken.

Control Statement: Only data input fields required for log-on purposes to be displayed.

Control Statement: No information, other than a log-on prompt, on the log-on screen.

Post-installation procedures

Control Statement: Documentation shall be produced and maintained on the configuration of the Windows client standard build for library sites. This documentation shall include a description of the configuration of Windows operating system as well as a list of the services and applications that have been installed.

Control Statement: Anti-virus software shall run on all Windows clients, and the virus signatures shall be kept up-to- date automatically.

Changes to system software

Critical updates shall be applied in a timely manner to all Windows clients.

Control Statement: All changes to system software shall be made in compliance with Change Management Procedures.

Control Statement: The IT Team will test all patches before they are applied to operational clients.

Control Statement: The Information Security Manager shall liaise with suppliers to identify patches and updates on a regular basis.

Control Statement: All applicable critical patches will be installed on all systems within a timeframe commensurate with the risk and consistent to the effort required by the supplier to apply such patches.

System configuration parameters

When changes are needed to system configuration parameters, care shall be exercised to avoid damaging the operation of the system.

Control Statement: All changes to system parameters shall be made in compliance with Change Management Procedures

Unauthorised software

In order to prevent disruption to service from such software, the following steps are required.

Control Statement: Freeware, shareware and other unauthorised software must not be installed on systems, except with the approval of the Information Security Manager and adequate testing is performed

Control Statement: In order to comply with legal requirements, only licensed software will be installed on client PCs

Control Statement: Original licence documents must be retained and stored in a safe place by the Authority

Control Statement: An inventory of software licences to be maintained

Where is possible configuration management (manual or automated) is required to ensure that the system is checked for unauthorised software.

3.4 User Authorisation

Account management

Local accounts with administrative equivalent permissions will only be provided on client PCs for maintenance operation. Ordinary users will only log in to client machines via domain accounts.

Where Libraries NI desktops are shared by users, each user must log in separately for their own individual session. Where appropriate application sessions are not to be shared by users.

Account creation

Local administrative accounts will be created on all Client machines for maintenance purposes only. Individual local accounts will not be provided.

Administrative rights will be restricted to authorised personal only

All Libraries NI staff user accounts will be domain accounts.

Account passwords

Strong passwords will be set on all local administrative accounts on client machines.

The passwords for local administrative accounts shall comply with the requirements for privileged accounts defined in the Server Security Standard, with regard to length and complexity.

Password expiry will not be applied to local administrative accounts on client machines.

User passwords shall comply with the following:

Control Statement: All passwords must contain at least 10 characters.

Control Statement: All passwords to include alphanumeric text

Control Statement: Password maximum age must be set to 90 days

Control Statement: Passwords shall not be visible in clear text

Control Statement: Password history must be kept up to 6 previous passwords

Control Statement: Password minimum age must be set to 2 days

Employees must be given security awareness training, to guide them on how to follow good security practice in the selection and use of passwords.

Anonymous accounts

Anonymous accounts must not be used on client PCs.

The Guest account shall be disabled on all Microsoft Windows client PCs – this is the default setting.

Log on

The number of false log-on attempts to be limited to, at most, three attempts.

Internet browsing software

All users have access to application software to enable them to access the World Wide Web. Software of this type can cache username and password information.

This information should be stored within each users roaming profile so that it is not available to other users of a machine.

Removable media

Care should be taken when data is transferred to removable media, to ensure that the protection of the data is maintained.

Control Statement: All removable media containing sensitive information shall be stored securely when not in use, to reduce risk of unauthorised access

Windows will, by default, attempt to run software (often an installation program) from media inserted into a CD/DVD drive. This process might inadvertently install rogue software on the system, and shall therefore be avoided.

Control Statement: The Auto run feature shall be disabled on all CD/ DVD drives

3.5 Backup and Recovery

Operating system backups

In the event that the operating system becomes corrupted, the machine will be re-imaged to the original standard build by the supplier.

Data backups

No backups are required of client machines, since they do not hold important user files.

Asset management

All clients, laptops, desktops are to be issued asset tags and to be listed in asset inventories with documented owners assigned.

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.