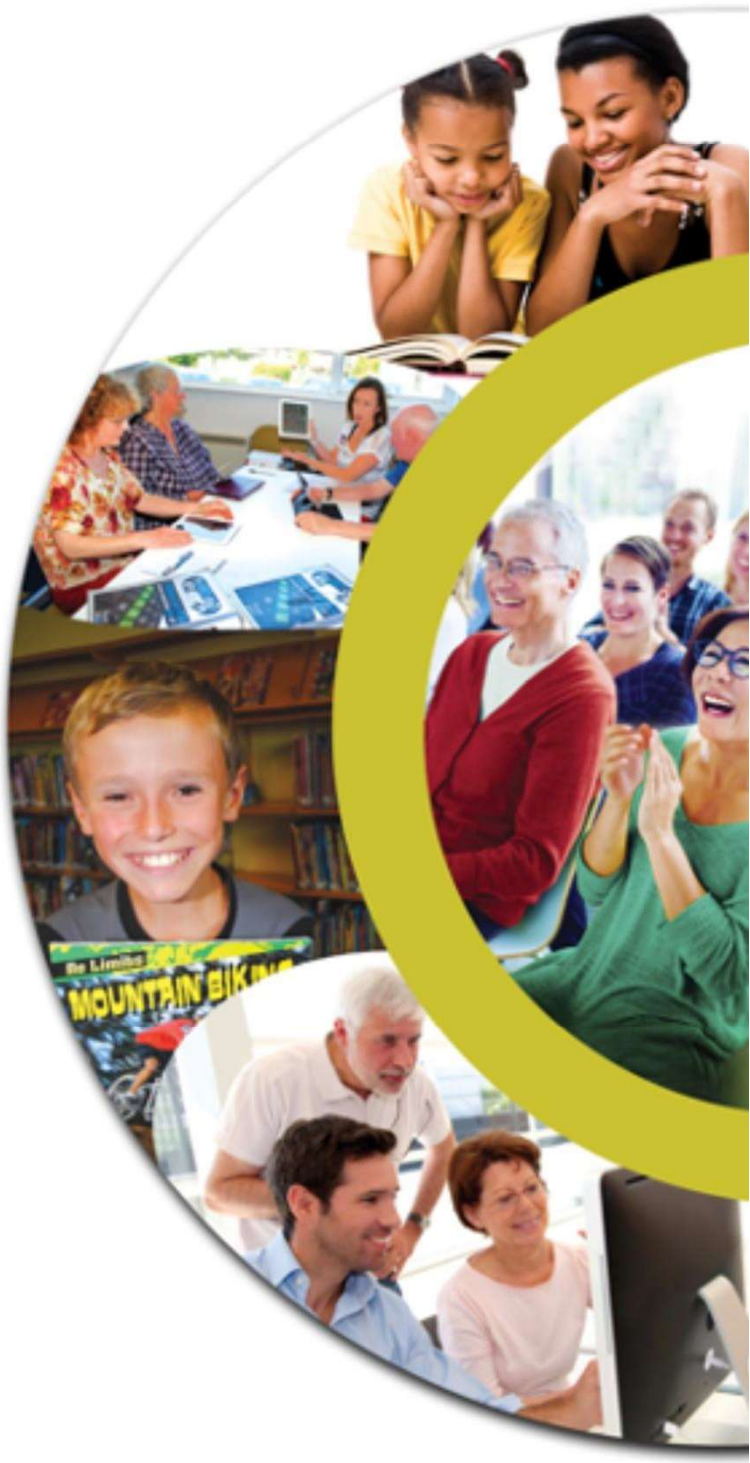
Server Security Policy



Date: 25 January 2024

Review Date: January 2027

Connect with us
www.librariesni.org.uk

Policy Information	
Policy Title	Server Security Policy
Policy Number:	POL 029
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	POL030 Network Security Policy POL031 Internet Security Policy POL032 IT Security Policy POL033 Microsoft Windows Client 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 all Microsoft Windows Servers within the Libraries NI IT environment. All systems are 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.

3. Policy

3.1 Directory Services

Security domain boundaries

Libraries NI servers that are directly connected to public networks such as the Internet must not be able to interact directly with the Active Directory or equivalent directory services within the Libraries NI private network. Such machines must be hardened such that they are resistant to attack.

Domain controllers

Domain Controllers should not have other application software running on them, and all optional components of Windows operating system should be disabled.

Control Statement: Domain Controllers must not run additional application software

Control Statement: Domain Controllers must not run IIS services

3.2 Hardware Configuration

BIOS passwords

Suitable BIOS passwords should be used to prevent unauthorised access to the BIOS such that the configuration of the machine could be altered, particularly on servers that are located outside the Data Centre.

Boot sequence

Once a server has been installed, it should always boot from the hard drive, without attempting to boot from other media, since they could be used to subvert the function of the server.

All servers must be set to boot only from hard disk. Where this is not possible, they must be configured to attempt first to boot from hard drive.

Action after outage

Server BIOS configuration parameters allow a choice of actions following system outages such as power failures and system crashes.
All Windows servers must be set to reboot automatically after any outage.

With the exception of file and print servers, server names should give no indication of their purpose, operating system, or physical location;

Changes to hardware configuration are to be subject to change control procedures.

3.3 System Software

Software upgrades and installation

All Windows servers should 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 servers must be installed to a standard build

Control Statement: Deviations from the standard build must be documented

Dual-boot systems (systems that can boot alternate operating systems or alternate copies of the same operating system) are not permitted.

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

Control Statement: the clocks of all relevant information processing systems within an organisation or security domain shall be synchronized with an agreed accurate time source**.**

Control Statement: Server clocks should be checked at least once a week and reset to the correct time. Automatic synchronisation should be employed where feasible;

During installation, the Windows Regional Settings must be set to the appropriate local setting.

Post-installation procedures

Standard documentation must be produced on the configuration of each Windows server. This documentation must include a description of the configuration of Windows server as well as a list of the services and applications that have been installed.

Anti-virus software must run on all Windows servers, and the virus signatures must be kept up-to-date automatically.

Changes to system software

Critical updates or must be applied in a timely, managed and controlled manner to all Windows servers, in accordance with change control procedures.

All changes to system software must be made in compliance with Change Management Procedures and be subject to test and validation before applying to live environments.

All patches will be tested before they are applied to production servers.

All applicable critical patches will be installed on all systems within a time period agreed with the Authority.

System configuration parameters

All changes to system parameters must be made in compliance with Change Management Procedures.

Unauthorised software

Microsoft Windows environments must adhere to the following:

- user's ability to install software should be prohibited
- computer games including those supplied with the operating system must **not** be installed on servers.
- freeware and shareware must **not** be installed on systems, except with the approval of the Information Security Manager.

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

Original media and licence documents must be retained and stored in a safe place.

The terms of the licence for any piece of software must be followed.

Where users require additional software to be installed, request for such software is to be subject to formal authorisation and approval.

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

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

3.4 User Authorisation

User identifiers

Each user within the IT environment will be issued an individual account, identified by a unique username. This username uniquely identifies the user to the systems for the purposes of logging on, accessing resources, and for auditing purposes.

Usernames must not be re-used for a period of one year after an account is deleted, except in the event of re-instatement of the account for the same individual.

User accounts must only be issued to individuals.

Generic accounts may only be issued for specific purposes, agreed by the Information Security Manager, and may not be granted privileges above those of an ordinary user account.

Account management

Account creation

Before the creation of a user account, an account request form must be completed by the user, and validated by a supervisor or manager for Business Support accounts or a Librarian for member accounts.

Completed account request forms for privileged accounts must be retained by the Information Security Manager for the life of the account.

The user's full name must be recorded in the corresponding field for every user account.

The principle of least privilege will be applied when creating all accounts.

Account revalidation

In order to ensure that obsolete accounts do not remain on the systems, accounts should be subject to periodic revalidation.

All accounts must be revalidated at the start of each financial year. Revalidation is carried out by the Information Security manager for all accounts.

Account expiration

Temporary accounts should be created for all authorised users who are not permanent users of the Libraries environment. These accounts should automatically cease to be available unless extended.

Accounts issued to general public, temporary staff, contractors, and consultants must have an expiration date set.

Expiration dates must initially be no more than twelve months from the date the account was created, but should be shorter if the account is only required for a shorter time.

Not more than one month before the expiration date, the Information Security Manager will carry out account revalidation and extend expiration if required.

Account deletion

Once an account is no longer required, it will be deleted, and the user's files retained for 30 days before they are permanently deleted along with the account.

Accounts for permanent users who are on extended absence will be disabled if not required, but will not be deleted so long as the user is expected to return within eighteen months. If the absence is longer, the account will be removed, and will be reinstated when required again.

All accounts must be deleted once they are no longer required by the user.

An account will be deemed no longer required if it has not been accessed for a period of three months (this excludes users on authorised long-term absences).

The files, folders and other data associated with accounts that are no longer required will be deleted 30 days after it has been deleted from Active Directory.

User accounts that are no longer required will be deleted within three months after they have been disabled, or as part of the housekeeping at the end of the Year, whichever is sooner.

Account passwords

Users are ordinarily authenticated to Microsoft Windows by means of passwords. Passwords should consist of at least 10 characters, and can include Upper and Lower case letters (passwords are case sensitive), numbers, and a variety of special characters.

Passwords that do not meet this standard shall be rejected and password history shall be retained so that passwords cannot be reused consecutively. In addition, it is possible to require a variety of characters in the password, and to reject the username and elements of the full name as passwords, by means of a domain security setting. This functionality should be considered for high-risk domains.

Two individual account flags are available to control the setting of passwords. While the following requirements do not apply to application and service accounts, they are mandatory for user accounts, including those of administrators.

The “Password Never Expires” flag must not be set on user accounts. The “User Cannot Change Password” flag must not be set on user accounts.

The following requirements should be enforced on all Windows servers:

Control Statement: All passwords must contain at least 10 letters

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

System administrator passwords must be subject to more frequent refresh than normal user account standards.

Users with privileged accounts should be encouraged to choose passwords that are stronger than the requirements listed above, including alphanumeric and non-alphanumeric, special characters and upper and lower case, characters.

Account lockout information - The following settings are mandatory on all Windows systems.

Control Statement: Account lockout must occur after a maximum of 3 failed attempts

Control Statement: The lockout counter must reset after not less than 5 minutes

Control Statement: The lockout duration must be not less than 10 minutes

Account access

Logon hours restrictions are not generally applied within the IT environment, but they should be considered for those user accounts that are not needed at all times.

Windows servers should not be used by ordinary users to logon to the network. Should ordinary users log on locally to such machines, their applications may interfere with the business function the machine is intended to support. Where possible, ordinary user accounts must not have the right to log on locally to servers.

Only members of the Administrators, Account Operators, Backup Operators, Server Operators and Print Operators groups are allowed to shut down the systems.

Ordinary user accounts should not be provided with enhanced user rights within the IT environment, in order to maintain the security of the environment.

Account profiles

It is recommended that group policy objects, profiles and login scripts be used to define a standard user environment wherever possible.

Systems administrator accounts

Windows system administrators must be provided with individual user accounts from which to carry out their normal work. They must only use the primary system administrator account when this is a requirement of the task they are carrying out.

The primary system administrator account can have its username changed under Windows. This provides a little extra security, by hiding this account from unauthorised users.

The local Administrator account must be renamed from default and protected by secure passwords on all Windows servers.

An account with the name Administrator must be created with no user rights, with logon hours set to none and its expiration date set to a date in the past.

The password on this account must be set to a random password that is at least 16 characters in length, and is not retained.

Anonymous (guest) accounts

Anonymous (guest) accounts must not be used on IT Windows servers.

The Guest account must be renamed and disabled on all Windows servers.

The renamed Guest account must have no user rights, its logon hours set to none and its expiration date set to a date in the past.

The password on the renamed Guest account must be set to a random password that is at least 16 characters in length, and is not retained.

3.5 Backup and Recovery

Server configuration backups

Server configuration files and data must be backed up in order to recover the system in the event of file corruption, or disk failure. Backups should be carried out on a regular basis, and the backup media stored securely.

All server images must be backed up regularly to protect all centrally hosted applications and data. Backup media must be kept in a secure environment.

The responsibility for backup of individual servers within the IT environment lies with the supplier of the appropriate service.

A Virtual Server image must be maintained for every server in the IT environment and should be updated after every significant configuration change on the system (e.g. installation of a new application).

Data backups

Data files must be backed up in order to recover the system in the event of file corruption, or disk failure. Backups should be carried out on a regular basis, and the backup media stored securely.

All data files should be backed up regularly.

The data files involved with individual applications must be backed up in accordance with the defined requirements of the application concerned.

Backup media must be kept in a restricted, secure access area.

Off-site storage of backups

In order to facilitate recovery in the event of a major disaster involving the loss of access to a Data Centre, copies of recent operating system and data backups should be kept in secure off-site storage. This may involve exchanging backup media between IT sites, or the use of third party storage arrangements.

Documented procedures must be laid down for the transfer of backup media to off-site storage for all Windows servers.

Backup media must be transferred from site to off-site storage by secure means.

A record must be kept of backup media being transferred both in and out of off-site storage.

Off-site backup media must be stored in a secure and restricted access area
For servers located outside the Data Centre, appropriate steps should be taken to ensure copies of backups are available following a site disaster.

Where possible, backup media, from servers outside the Data Centre, should be kept in a secure place off site.

Should off-site storage not be possible, backup media must be kept in an appropriate fireproof safe.

Data recovery

A record must be kept of all files restored from backup including when individual files are restored or whole systems or disks.

3.6 Auditing

Security event auditing

The following security events must be audited on all Windows systems:

- all failure events
- successful logon events
- account management events
- policy change events
- system events.

Remote unauthenticated access to the System and Security Event Logs must be disabled.

Consideration should also be given to placing the Security and System Logs on a dedicated disk partition.

Incorrect log-on attempts should be recorded in an audit log. After three consecutive incorrect attempts user accounts should be suspended. Where sensitive or personal data is held on a server or access is by an administrator then successful log-on attempts should be recorded in the audit log as well. Logs should be reviewed periodically for potential unauthorised activity

Log file retention

Audit log files are subject to the standard rules that govern the retention of IT business records. These log files include the Security and System Event Logs, and any other service log files described above.

All log files must be backed up daily to tape.

Backup tapes containing security audit files must be retained for 1 year.

3.7 Networking

Network logins

All Windows servers should display a warning message to users before they log on.

Interactive logon screens must be preceded with a warning banner indicating that the system is owned by IT, and that unauthorised access is prohibited.

Other network services must present a similar warning to users wherever possible.

Anonymous (guest) access

Anonymous services are not permitted on the network and this restriction should be applied to the individual network services.

The use of the automatic logon capability in Windows is not permitted. The automatic logon capability in Windows must not be enabled.

Network services

Windows servers connected to the Libraries NI network must not at the same time be connected directly to a public network (e.g. the Internet), unless the machine is designed to be a *firewall* between the two networks.

All connections with services outside of Libraries NI must pass through approved firewalls

Only the required network services should be installed on Windows servers on the Libraries NI network. The required network services should be configured to provide only the minimum required access.

The only Network Layer protocol supported on the Libraries NI network is IP. Other Network Layer protocols must not be installed on IT Windows servers.

The *SNMP* service must be installed on all Windows servers on the Libraries NI network. The *Public* SNMP community must not be configured to provide *Set* access.

Any WWW and FTP Services that are provided must be secured, in order to prevent disruption to the system through these services, and to ensure the integrity of the information provided by these services.

WWW and FTP Services must use dedicated directories as document roots. (It is permissible to use the same directory for both services, though care must be taken to ensure that this does not compromise the security of the services.) The document root directories must not contain any operating system files or directories.

WWW and FTP document roots are not permitted on the same partition as the operating system.

Users of WWW and FTP Services must only have read and execute permissions to the document root directories. (Additional access is permitted for those users responsible for the administration of content on these services.)

Specific hardening rules should be developed for servers running other applications, with a general goal of providing minimum access to the operating system and network services on the machine. These hardening rules should then be applied uniformly across all servers running that application on the network.

3.8 Physical Environment

Location of systems

Critical business servers must be installed in secure and restricted Data Centres.

Environmental monitoring systems should be in place to monitor the power, temperature and humidity of the server room.

Access to Data Centres and Server Rooms should be restricted to authorised systems and networks administrators. Other individuals admitted should be required to sign in. The signing in log should record date, name, company, reason for entering, time in and time out.

Consideration should be given to the installation of security cameras to monitor and record individuals going in and out of Data Centres/Server Rooms. Access to diagnostic ports or other facilities should be controlled to ensure they are only available to approved persons.

Storage of magnetic media

Magnetic media should always be stored securely in a restricted access environment.

Removable media containing data must be stored securely in a lockable and fireproof container

Removal of storage media is to be approved and handled in accordance with appropriate removal procedures.

A record must be kept of all media held and this record must be available for audit.

A log must be maintained of all media, removed from site and reconciled upon receipt. This log must be retained and made available for audit.

When transported the media must be protected from physical damage, sealed in tamper-evident packaging and transported by an authorised courier.

Keyboard and display security

The console of a Windows server should be logged out when not in use whenever possible. Logged on, unattended Windows servers provide an opportunity for unauthorised access that must be avoided.

Windows servers must be logged out when left unattended for a period of more than 1 hour.

A password protected screen saver must activate automatically after a period of no more than 10 minutes inactivity on a logged on Windows server.

Asset management

All servers are to be documented in the asset inventory and have an assigned owner.

Inventories should be reviewed to ensure that asset details remain accurate.

3.9 Disposal of System Data

Servers assigned for disposal or decommission must have all data removed prior to disposal or decommission.

Magnetic and optical media

All magnetic and optical media that are no longer required should be erased before it leaves the control of IT. Where erasure is not feasible, for example in the event of a disk failure or for write-once optical media, media should be destroyed securely and receipt confirmation obtained to confirm destruction.

Hard disks must be reformatted once they are no longer required.

Magnetic tapes must be erased once they are no longer required.

All magnetic media that cannot be erased must be securely destroyed when no longer required.

Optical media that cannot be erased must be shredded once they are no longer required. Where this is not possible, arrangements must be made for alternative secure disposal of optical media.

Printout

Sensitive material must be shredded once it is no longer required.

Where shredding is not available at the location, arrangement must be made for alternative secure disposal of sensitive printout.

3.10 Day-to-Day Operations

Separation of duties

Wherever possible the individual duties of “running”, “securing” and “auditing” a system should be separated to different individuals.

Audit logs should be maintained for administrator access and activities, in particular for sensitive systems or servers containing sensitive and or personal data.

Performance monitoring

Performance monitoring should be applied to all Windows servers at the Data Centre, with data collected at least during working hours. Regular reviews of this data should be undertaken, to identify performance trends. This process allows upgrades to systems to be planned and installed before problems occur.

All servers must be configured to feed into the standard IT performance monitoring environment.

Security monitoring

Security event logs should be monitored on a regular basis to detect unauthorised access attempts to systems.

The security logs on all Windows servers must be checked on a daily basis for unauthorised accesses to the systems

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.