Network Security Policy

Policy information

Policy number: **282**
Classification: Corporate
Supersedes: Previous versions
Version number: 4.0
Date of Equality Impact Assessment: 24.12.2025

Approval information

Approved by: Digital Data & Innovation Committee
Date of approval: 22.01.2026
Date made active: 28.01.2026
Review date: 22.01.2029

Summary of document:
This policy states the network security requirements for the Health Board

Scope:
This policy applies to all users of the Health Board's digital networks.

To be read in conjunction with:
837 - AW Information Security Policy – opens in a new tab
201 – AW Disciplinary Policy – opens in a new tab
281 – Mobile working policy – opens in a new tab

Patient information:N/A
Owning group: Information Governance Sub-Committee 25.11.2025
Executive Director job title: Director of Finance

Reviews and updates:
1 – new policy 26.6.2012
2 – revised 29.3.2016
3 – full review 28.2.2023
4 – full review 26.1.2026

Keywords: Network, security, access, computing
Glossary of terms: None

Keypoints:
To ensure the security, integrity and availability of the Health Board's digital networks used to support our clinical and administrative services.

Contents

INTRODUCTION

This document defines the computer network security policy for Hywel Dda University Health Board and this policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

It sets out the policy for the protection of the confidentiality, integrity, and availability of the network as well as security responsibilities for ensuring the security of our networks.

The network for the purpose of this policy is a collection of communication equipment such as servers, computers and printers which are connected using our local and wide area networks.

POLICY STATEMENT

The overall Network Security Policy for the Health Board is described below.

The Health Board's information network will be available when needed, can be accessed only by legitimate users and devices, and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this the Health Board will undertake the following: -

- Protect all hardware, software, and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost-effective manner.
- Where relevant comply with the legal, regulatory, and internal policy requirements.

If a user is found to have breached this policy, they may be subject to the Health Board's disciplinary procedure. – opens in a new tab.

If a user does not understand the implications of this policy or how it may apply to them, they should seek advice from the Health Board's Network or Cyber Security Team.

SCOPE

This policy applies to all networks within Hywel Dda Health Board both wired and wireless used for: -

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending, and storing non-clinical or clinical data or images

AIMS

The aim of this policy is to provide assurance through relevant controls and procedures that our networks are secure and the information on them is kept confidential.

OBJECTIVES

The objectives to be achieved by this policy are:

- Suitable controls exist to secure our networks.
- Ensure all those accessing and managing the network understand their roles and responsibilities.
- Ensure suitable procedures are in place.

Risk Assessments

Hywel Dda University Health Board will carry out security risk assessment(s) in relation to all aspects of the network that are used to support business processes. The risk assessment will identify the appropriate security counter-measures necessary to protect against possible breaches in confidentiality, integrity, and availability.

Formal risk assessments will be conducted in line with Health Board's Risk Assurance Framework.

Physical and Environmental Security

The following Physical and Environmental security mechanisms will be employed:

- Network computer equipment will be housed in a controlled and secure environment that is monitored for temperature, humidity, and power supply issues.
- Critical network equipment will be housed in dedicated secure areas protected by physical locks and access control mechanisms.
- The Head of Digital Operations is responsible for ensuring the suitability of these security measures.
- Network equipment will be protected from power supply failures.
- Critical network equipment will be protected by intruder alarms and fire suppression systems.
- Various technical controls will be in place to secure the network including security patching, firewalls, and network admission control.
- All visitors to secure and critical network areas must be authorised by the Head of Digital Infrastructure.
- The Head of Digital Infrastructure will ensure that all relevant digital employees are made aware of procedures for visitors and those visitors are escorted when necessary.

Access Control to the Network

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. Ordinarily, such access is supervised but there may be occasions when trusted engineers may require unsupervised access. The Head of Digital Infrastructure will maintain and periodically review a list of those with unsupervised access. Access to these areas will be restricted by appropriate controls.

Access to the network will be via secure methods and authentication against our directory service. Remote access to the network will conform to the Health Board's Mobile Working Policy – opens in a new tab.

There must be a formal, documented user registration and de-registration procedure for access to the network. All users on the network will have their own individual user identification and password and are ensuring their password is kept confidential. Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working and workstations must be locked if a workstation is left unattended.

User access rights will be immediately removed or reviewed for those users who have left the Health Board or changed jobs.

Any device connecting to the corporate network must comply with the Health Board's Managed security requirements which include domain membership, Endpoint Detection and Response, Secure Web Gateway, and patching procedures. Devices that do not meet these requirements are not permitted to connect to the corporate network.

Clinical devices and Internet of Things (IoT) equipment connecting to the network must be placed in a segregated virtual network to ensure they are protected from the wider network and have controlled access control lists.

Requests for New Devices to Access the Network

Any department that has a need to connect new IoT or IoMT corporate devices to the corporate network must request formally via the Digital Services portal, Device Connectivity Request. The Cyber Security Team will need to review any new devices prior to connection. Departments must request this before procuring any new devices to ensure they meet the Health Boards security standards. Any devices that are procured without Digital Services' approval may require significant network re-configuration to ensure they can be added securely which will incur additional costs.

Third Party Access to the Network

If external third-party owned devices require access to the corporate network this will be allowed only once the third party has provided assurances of their security posture of the organisation and device to the cyber security team where possible the free public and patient guest Wi-Fi service should be used ('Hywel Dda Public').

All third-party access to the corporate network must be logged and access to Hywel Dda Health Board's systems must be always audited.

Third party users must have an Active Directory account created for them for the duration of their stay with appropriate permissions and will not use generic accounts or service accounts.

Any department that has a need to connect new third-party owned devices to the corporate network must request formally via the Digital Services portal, Device Connectivity Request.

All third remote access by external third parties must be approved following the Code of Connection process and must utilise Hywel Dda approved remote access methods.

Physical access by 3rd parties to network equipment locations (Server Rooms, Communication Rooms, Cabinets etc) must be approved by Digital Services. 3rd parties must be supervised when physically working in these areas to maintain system security.

Network Monitoring

The Hywel Dda corporate network is monitored by an Armis network discovery tool. This monitors all devices connected to the network and provides a status of the device's vulnerabilities. New devices that are connected to the network are automatically reported to the Cyber Team via Armis. If a formal request to connect the device has not been received prior to connection, the Cyber Team reserve the right to block the device until an appropriate security review has been conducted.

External Network Connections

Any external network connections must only be through approved access methodologies and managed by the Digital Services department to ensure they can be appropriately secured and monitored.

Any connections not formally approved may put the Health Board at risk by disconnection from the Public Sector Broadband Aggregated Network (PSBA)

Personally Owned Devices

Under no circumstances should personally owned devices be connected to the corporate network. This includes plugging them into any network sockets located on walls throughout the estate or attempting to connect them to corporate Wi-Fis (i.e. Hywel Dda or Hywel Dda Corporate).

Personally owned devices are only permitted to be connected to the available guests Wi-Fi networks available through the estates (i.e. _Hywel Dda Public)

Maintenance Agreements

The Head of Digital Operations will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Digital Department's Configuration Management Database.

Operating Procedures

Documented Security Operating Procedures will be created for the network that reflects this policy and changes to these procedures must be authorised by the Head of Digital Infrastructure.

Change Control

Any changes proposed to the network must consider the security of the network.

Changes must be in line with the Hywel Dda change control procedure and must be reviewed by the Digital Change Advisory Board and approved by the Head of Digital Infrastructure.

As part of acceptance testing of all new network systems the Cyber Security Manager will undertake security tests to ensure compliance with this policy.

Security Monitoring

The network will be monitored for potential security breaches and automated alerts will be generated to highlight potential issues.

All potential security breaches must be reported to the Cyber Security Team using the Digital Portal. The Cyber Security Manager is responsible for auditing the network to ensure it meets agreed security standards.

RESPONSIBILITIES

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

Users

The health Board will ensure that all users of the network are provided with the necessary security guidance, awareness and, where appropriate, training to discharge their security responsibilities.

All users of the network must be made aware of the contents and implications of the network security policy and that irresponsible or improper actions by users may result in disciplinary actions(s).

All users should safeguard hardware, software and information in their care and prevent the introduction of malicious software onto the organisation's digital systems.

They also have an obligation to report on any suspected or actual breaches in security.

Digital Operations

Digital Operations will be responsible for:

- Management of network equipment.
- Management of network security including that of the Wireless LAN and any external connections not a part of the PSBA network.
- Disaster Recovery and Business Continuity Plans and for the testing of those plans.
- Providing support to users in gaining access to the network and their use of services provided over the network.
- Periodic penetration testing to ensure the security of our networks.

Head of Digital Operations

Will be responsible for implementing an effective framework for the management of network security and ensuring the production of all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of this policy.

Head of Digital Infrastructure

Will be responsible for the implementation of effective security countermeasures, contacting the Cyber Security Manager when incidents or alerts have been reported that may affect the security of the Health Board's networks.

Responsible for ensuring all network components will have effective configuration management procedures in place in line with the Hywel Dda Configuration Management Procedure.

Cyber Security Manager

The Cyber Security Manager will be responsible for:

- Mandating effective security countermeasures.
- Acting as a central point of contact for cyber security within the organisation.
- Assisting in the updating of this policy and related policies for approval by the Information Governance Sub-Committee.
- Producing organisational standards, procedures, and guidance on cyber security matters.
- Liaising with external organisations on cyber security matters, including representing the organisation on the national Operational Security Service Management Board and associated sub-groups managed by Digital Health & Care Wales (DHCW).
- Advising the Head of Digital Operations on cyber security breaches and recommended actions.
- Encouraging, monitoring, and checking compliance with this policy.
- Promoting awareness and providing guidance on this policy.
- Creating, maintaining, and giving guidance on and overseeing the implementation of network security.

Line Manager's Responsibilities

Ensuring all employees are made aware of their security responsibilities as indicated in this policy.

TRAINING

All staff will be required to have appropriate information governance training which will include guidance on network security.

IMPLEMENTATION

All staff must adhere to this policy and failure to follow these policies may lead to disciplinary action being taken. This policy will be disseminated through global email and through periodic Information Governance training.