NETWORK ACCESS POLICY

1. PURPOSE

To ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user.

Controls to ensure,

> *'Access to information systems that process personal information, shall be subject to a formal user registration process. User registration procedures shall ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user. User registration details shall be periodically reviewed to ensure that they are complete, accurate and access is still required.'*

The purpose of this policy is to:

- To protect PaxtechITS Network users by preventing unauthorized individuals from accessing network resources and information intended for authorised staff and approved users.
- Re-enforce the need for a full life cycle approach to identity management;
- Ensure compliance with Australian Standards for information security.

The policy does not describe the technology standards required as these are available line.

2. SCOPE

This policy covers the management of individual identities, their authentication, authorization, and privileges/permissions within or across systems.

This policy applies to all personnel (employees, contractors, students, volunteers and agency personnel) This policy also applies to external organisations and their personnel who have been granted access to Information and Communications Technology (ICT) infrastructure and services.

This policy must be read in conjunction with the information privacy policy. This and other policies and standards are available on line.

3. POLICY

3.1. Individuals wanting to connect to the wired or wireless network are required to provide authentication to gain access.

3.2. Computers and other electronic devices connecting to the wired or wireless network are required to meet Enterprise Architecture Standards and information security standards before being granted access.

3.3. Authorisation for network access wired or wireless will depend on the individual's relationship, or relationships, to PaxtechITS and the requirements associated with that relationship (Role Based Access Control). In all cases, only the minimum privileges necessary (Principle of Least Privilege) to complete required tasks will be assigned to that individual

3.4. PaxtechITS will assign a PaxtechITS Identifier and User Credentials for Identification and Authentication purposes to each individual that has a business, or other approved need to access PaxtechITS ICT Resources.

3.5. Full lifecycle identity management will be employed from creation, through allocation and role changes to eventual de-allocation i.e. Privileges assigned to each individual will be reviewed on a periodic basis and modified or revoked upon a change in individual status with Nelson Systems.

3.6. All internal requests for access to the PaxtechITS network can only be initiated via the Access Request Form .

3.7. A 'Defence in Depth' approach to ICT network access security will be used by PaxtechITS where applicable based on a risk assessment and cost/benefit analysis.

3.8. All external organisations e.g. vendors requiring access for maintenance purposes, requests to connect to the PaxtechITS network can only be initiated via the appropriate form:

3.9. If authentication is not provided or PaxtechITS Enterprise Architecture Standards and information security standards are not met, access to the PaxtechITS ICT network will be automatically denied.

4. POLICY DETAILS

4.1 Access Control.

Identification, Authentication, and Authorization are controls that facilitate access to and protect PaxtechITS Resources and data. Access to non-public ICT Resources will be achieved by unique User Credentials and will require Authentication.

4.2 Technology Standards

See Enterprise Architecture Standards.

PaxtechITS Enterprise identifies relevant technical standards which are. Clarification of these standards can be obtained from PaxtechITS head Office.

4.3 Principle of Least Privilege (POLP)

The principle of least privilege (POLP) is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the POLP translates to giving people the lowest level of user rights that they can have and still do their jobs also referred to as Role Based Access Control (RBAC).

A related concept, privilege bracketing, involves ensuring that when permission levels must be raised temporarily that the higher level is in effect for the briefest possible time. So, for example, you might log on to an administrative account when necessary for some task and immediately revert to a lower-level account as soon as that task is complete.

4.4 Personnal Identifier (PE Number)

All PaxtechITS network access is via a ID number. The construction of this ID is defined in the enterprise architecture standard SS34 Network Resource Addressing & Naming.

4.5 Identity Access Model (IAM)

IAM technology can be used to automate the initiation, capture, recording and management of user identities and their related access permissions. This ensures NETWORK ACCESS POLICY that access privileges are granted according to one interpretation and all individuals and services are properly authenticated, authorized and audited.

With a wider array of IT infrastructure in Nelson Systems, managing that infrastructure and in particular managing users, their identity profiles and their security privileges on those systems becomes increasingly challenging.

The IAM system includes at least the following sub-systems and components:

Platform, Application or Other Accounts Identity Administration Provisioning Services Federation Identities, Groups, Roles Identity Mastering and Publishing Agents Identity Repository Technical Architecture Standards SS21 Authentication Management SS33 Identity & Access Management SS10 User Responsibilities & Passwords SS12 Logon Identity Verification & Credential Management SS20 Roles & Authorisation Management IAM Conceptual Model From SS 33 – Identity & Access Management NETWORK ACCESS POLICY

Audit / Monitor Start Employment End Employment ALLOCATEMANAGE De-ALLOCATE Internal: including employees and contractors. External: including customers, partners and vendors. Changing roles and responsibilities! Changing identity attributes (e.g., user's surname, contact information, manager, etc.). Adjust user identity profiles and security rights. Technical support e.g. forgotten passwords, intruder lockouts, access; and denied errors! Ensure security privileges removal is: (a) Reliable (b) Timely (c) Complete On employment termination.

Identity Access Lifecycle

4.6 Defence in Depth

Defence in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. Components of defence in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection and biometric verification.

5. IMPLEMENTATION

Users of PaxtechITS Network resources must comply with this policy and related standards and expiry periods e.g. password expiry, issued by Nelson Systems.

Centralised and departmental ICT units and ICT Resource owners are responsible for ensuring appropriate enforcement of this policy and related standards on PaxtechITS Resources within their areas of responsibility.

Violations of this policy or any other PaxtechITS policy or regulation may result in the revocation or limitation of Resource privileges as well as other disciplinary actions, or may be referred to appropriate external authorities.

Planned new environments must conform to the PaxtechITS Enterprise Architecture Standards and Information Security Management Group Standards. Clarification of security issues are available from Security Management

6. BACKGROUND

There is a business need to provide secure external access to the Network using technologies such as remote access and the Internet. This is to address the requirements such as: staff working off-site, hardware and software support vendors and other outsourcing arrangements, communication with private hospitals (particularly at joint campuses), research/university staff located on public hospital campuses, and providing future access for GP's from their surgery. Entities to be managed typically include users, hardware, network resources and applications.

This policy establishes principles by which the identity, specifically the electronic identity, of natural persons who have a relationship with WA Health as well as their access privileges are managed across WA Health. This process forms part of identity management system which aims to ensure that unauthorised electronic access to information, systems and physical areas, and potentially fraudulent activities are prevented.

7. RELEVANT LEGISLATION AND GOVERNMENT POLICIES

WA Acts are available at the State Law Publisher website; Commonwealth Acts are available at the Australian Government ComLaw website.

8. ASSOCIATED POLICIES, STANDARDS AND GUIDELINES

- Acceptable Use Policy – Computing and Communication Facilities.
- Computer Virus Protection and Security Software Standard.
- Information Security Policy.
- ICT Risk Management Policy.

9. INTERNATIONAL STANDARDS / SPECIFICATIONS

AS/NZS ISO/IEC 27001:2006	Information Technology – Security Techniques – Information Security Management Systems – Requirements.
AS/NZS ISO/IEC 27002:2006	Information Technology - Code of Practice for Information Security Management.
AS/NZ ISO/IEC 27799:2011	Information Security Management in Health Using ISO/IEC 27002.
ISO/IEC 27005:2011	Information technology - Security Techniques -