

SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	User Access Management (UAM)
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/314
DATE OF PUBLICATION	September 2024
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standard: Standard 1 – Clinical Governance ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems
REVIEW DATE	September 2029
FORMER REFERENCE(S)	Nil
EXECUTIVE SPONSOR	Director, Digital Health ICT
AUTHOR	Shane Feeney
POSITION RESPONSIBLE FOR THE DOCUMENT	Head of Business Technology Services Digital Health Jith.Perera@health.nsw.gov.au
FUNCTIONAL GROUP(S)	Information Management and Data
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance, User Access.
SUMMARY	This document provides the overarching policy under which granting User Access to digital information systems in the South Eastern Sydney Local Health District is mandated.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY
This Policy is intellectual property of South Eastern Sydney Local Health District.
Policy content cannot be duplicated.

1. PURPOSE

The security of SESLHD information is critical to meeting our obligations and to ensure the resilience and ongoing success of South Eastern Sydney Local Health District.

The purpose of the User Access Management (UAM) Policy is to describe the principles used to manage user access and protect digital assets that SESLHD manages from deliberate, or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, or misuse.

The policy focuses on establishing a trusted environment for users and leverage off information security mechanisms.

2. AIMS

This User Access Management (UAM) Policy manages user identity and logical access and ensures that all users have the appropriate information access rights in accordance with their needs to meet the business requirements.

3. TARGET AUDIENCE

This policy applies to all parties who may utilise SESLHD infrastructure and/or access SESLHD systems and applications (including systems provided by external providers such as eHealth) with respect to managing the access to the district digital assets and privacy of information. This includes permanent, temporary and casual staff of SESLHD, staff seconded from other organisations and contingent workers, including labour hire, service providers, professional services contractors and consultants,

4. USER ACCESS MANAGEMENT POLICY SCOPE

The following principles are applicable to all account types, systems and applications, and should be considered as a minimum requirement. The security- specific activities;

- a) User Access Management must maintain user access rights in accordance with business (department) function and process requirements. The access rights must align the management of users identities and access rights with the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.
- b) User Access Management must uniquely identify all information processing activities by functional roles co-ordinated with the SESLHD department's business needs to ensure that all roles are defined, including roles that are defined by the SESLHD departments itself within its processes.
- c) The creating of user access rights to digital assets must be based upon their duties with consideration of their accountability and responsibility.
- d) User access rights to digital assets must be audited at least annually to confirm the need for access and appropriateness.
- e) Administration of all changes to access rights (creation, modifications and deletions) to take effect at the appropriate time, based only on an approved and documented transactions authorised by designated authorised management individuals.
- f) Privileged user accounts must be segregated and managed separately from the general access account;
- g) There must be regular management review of all accounts and related

privileges as per the NSW Government Cyber Security Policy.

- h) All users (internal, external and temporary) and their activity on ICT systems (business application, ICT infrastructure, system operations, development and maintenance) must be uniquely identifiable.
- i) An audit trail of access to information must be maintained where classified or highly sensitive data is accessed.

The scope of this policy includes all personnel who use an end-user computer (in any form) requiring a password to gain entry to the District digital assets.

The associated minimum systems specific parameters apply to all computers, laptops, servers, applications, BYODs, mobile and smart devices.

UAM covers;

- a) MACs: Moving users, Adding users, Changing user privileges, suspending or deleting user accounts;
- b) Reviewing user accounts and privileges;
- c) Management of the account including updating of account owner information;
- d) Managing users accounts who have been terminated;
- e) Application of security parameters such as;
 - a. Password guidelines,
 - b. Password length,
 - c. Password complexity and strength,
 - d. Password Age,
 - e. Password History,
- f) Account lockout parameters;
- g) Administration accounts including specialised and resource and third party accounts;
- h) Unattended systems;
- i) Directory and account systems not covered by Stafflink and the eHealth ADM.

Further details that are required to carry out the intent of a policy are prescribed in the UAM procedures documents managed by Health ICT (HICT).


4.1 Target Users

This policy applies to all parties including permanent, temporary and casual staff of SESLHD, staff seconded from other organisations and contingent workers including labour hire, service providers, professional services contractors and consultants, who may utilise SESLHD infrastructure and/or access SESLHD systems and applications (including systems provided by external providers such as eHealth) with respect to the security and privacy of information.

4.2 Password User Self-Management

Passwords form an integral part of accessing information systems and digital resources in SESLHD and its affiliates. As a result, all employees and third parties accessing digital services must adhere to the tenets of this policy.

This includes;

- a) Not writing down your password(s)
- b) Not sharing your password(s)
- c) Not communicating password(s) via e-mail or instant messaging
- d) Ensure you log off before leaving a computer unattended. Use the “ L” keys are a shortcut to locking your PC
- e) Do not use a simple password, but generate a complex one, refer to Section 0 - 2.5.2Users, Admins and Systems Accounts
- f) Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, birthdates and phone numbers
- g) If you suspect your account has been compromised, notify the NSW State Wide Service Desk (SWSD) immediately and change your password
- h) Avoid using the same password for multiple accounts or websites
- i) Avoid using the ‘Remember Password’ feature of browsers such as Internet Explorer, Firefox or Chrome
- j) Be conscious of someone seeing you type your password commonly called Shoulder Surfing.

4.3 Password Length

Systems must set a minimum acceptable password length for designated accounts as exemplified below in **Table 1. Password Length**, however a longer password with mixed characters is preferable to reduce the likelihood of the password being hacked.

- a) *User and Resource* minimum password length must be set and be sufficiently long enough to support mitigation against password hacking. The acceptable minimum is eight (8) characters.
- b) *Administration, Resource and Vendor* minimum password length must be longer than User account minimum password length. The acceptable minimum is fifteen (15) characters.
- c) *Systems and Resource* minimum password length must be longer than Administration password length. The acceptable minimum is twenty five (25) characters.

Minimum systems parameters are to be set to the following for the differing resource types to ensure appropriate security.

Table 1. Password Length

Account Types	Minimum length
User Accounts Password	8 characters minimum
Admin, Resource and Vendor Accounts Password	15 characters minimum
System Accounts Password	25 characters minimum

The State-Wide Active Directory (SWAD) that SESLHD subscribes to from eHealth utilises the above parameters as part of the Stafflink sign in.

4.4 Password Strength

4.4.1 Systems

All systems must use the appropriate password complexity as the default setting where possible.

For systems that do not have extended password management functionality, the system owner/ manager must conduct a risk assessment and put in place mitigating controls and default to the highest complexity allowed.

The system owner/ manager must notify the SESLHD Information Security Governance Committee (ISGC) of the status of the systems along with the risk assessment for acceptance.

4.4.2 Users, Admins and Systems Accounts

To reduce the likelihood of a password being guessed or cracked by a brute force attack, passwords must include a mixture of characters which will improve the strength of a password through complexity.

For example taking a phrase and splitting into two and inserting the a special character and a number;

- a) Brick%99Walls
- b) Carbon#56Neutral

Or the first letter of each word in a sentence such as;

- a) My dog is smart and has a flea collar; Mdisahafc#21
- b) My mother bakes great pavlovas but drinks the sherry: Mmbgp\$44bdts

Strong passwords have the following characteristics:

- a) A mixture of both upper and lower case letters (A-Z, a-z)
- b) Include one or more numerals (0-9)
- c) Include special characters such as (~! @\$%^&* _-+=` \(){}[];:"'<> ,.?!)_
- d) Are not based on any dictionary word
- e) Are not based on any personal information

- f) Are not an abbreviation of the organisation name
- g) Are not based on the username.

4.5 Password Life

For all systems, user password life must be set to change periodically with password history enabled preventing the use of previously used passwords.

For users and administrators, a period of no longer than 90 days with password history set where applicable.

Systems and Resource accounts must set their password life to no longer than 180 days with password history set where applicable.

All Passwords must be a minimum of 1 day old before being allowed to be changed.

Table 2. Password Life Parameters

Descriptor	Minimum Periods
Maximum User, Admin & Vendor Password Age	90 days minimum
Minimum User, Admin & Vendor Password Age	1 day minimum
Maximum System & Resource Password Age	180 days minimum
Minimum System & Resource Password Age	1 day minimum

4.6 Password History

Password history must be set for all systems where possible to ensure that account passwords are not re-used. All systems must set their password history to a minimum of 12 previous used passwords for users and 20 previous passwords for Administration, Resources and Systems.

Table 3. Minimum Password History Parameters

Descriptor	Minimum Parameters
User Password History	12 Passwords
All others, Administration, Resources, System & Vendors	20 Passwords

5. ACCOUNT LOCKOUT SETTINGS

5.1 All Accounts

All systems must have account lockout enabled where the functionality is available. In the event of a password authentication failure, the associated account must be locked out after a minimum number of invalid attempts, and will remain locked out for a minimum period.

The lockout reset must be configured to automatically reset bad password attempts after the minimum set period.

User or Administrator has had their account locked out can have the account unlocked by contacting the eHealth State Wide Service Desk (SWSD) or Specialist IT if the system is administered outside of the State Wide Active Domain.

Minimum parameters are:

Table 4. Minimum Account Lockout Parameters

Descriptor	Minimum Parameters
Lockout Threshold	5 invalid attempts
Lockout Duration	30 minutes
Lockout Reset	30 minutes

5.2 Unattended System Protection

All systems must default to a login or lock out screen after a minimum of 15 minutes of user inactivity.

6. SPECIAL ACCOUNTS

6.1 Specialised Accounts

A specialised user account is an account that enables a user to have higher privileges or enables the account to perform a specialised task such as running an application service. Each account that is in one of the four (4) categories listed in the following sections, will be a member of a secured group to enforce the more restrictive password policies as outlined.

Subject Matter Experts (SMEs) such as database administrators, who conduct Administration activities must utilise their Administration assigned account.

6.2 Service Accounts

Service accounts are only used to perform various system tasks such as run a service or an object. Service accounts must not be linked to a User, Administration or Resource account.

6.3 Administrative Accounts

Administrative accounts that conduct designated administrative functions. Administrative accounts must not be linked to a user, service or resources account.

6.4 Resource Accounts

Resource accounts are only used to manage various organisation assets such as meeting rooms, projectors and other facility items. Resource accounts must not be linked to a user, system or administration account.

6.5 Third Party Accounts

Third party accounts i.e. accounts created for vendors organisations must abide by the entire standard user password controls documented in this policy.

Third party vendor accounts must only be enabled on an as-needed basis via the Change Management procedure.

Vendors that require constant access must undergo a risk assessment and appropriate mitigation controls and account monitoring developed to manage vendor's access. The constant vendor access accounts must adhere to the following minimum parameters.

6.6 Cloud Services Accounts

SESLHD internally subscribes to an Active Directory (AD) model to manage user access as part of a global domain. Service providers that supply cloud service must either enable integration of the State-Wide Active Directory (SWAD) as the first preference or utilise role base authentication where access management is conducted by the SESLHD subscriber of the services, i.e.: Customer Managed Policies.

7. CHANGE OF STATUS

7.1 Employees and Contractors

Where the employee changes their employment status such as;

- a) Transferring to another department
- b) Termination
- c) Long Service leave
- d) Retirement, or
- e) Administrative leave

The manager of the employee must immediately notify HICT or the SWSD of the change in status so that the employee's profile can be updated or blocked from access.

Notification of all user account changes should be made at least seven (7) days prior to the known change date.

Supplementary notifications may come from SESLHD HR.

7.2 Vendors

When a vendor's status changes, the Vendor Manager or IT Specialist must immediately notify SWSD of the change in status so that the vendor's profile can be updated or blocked from access.

7.3 Other Applications

Where an account is not covered by the State-Wide Active Directory (SWAD) solution, it is the responsibility of the user's manager or project sponsor to notify the State Wide Service Desk (SWSD).

8. PASSWORD ADMINISTRATION

The password administration guidelines listed below are designed to ensure best practice in maintaining a secure network environment for SESLHD.

- a) **Temporary passwords:** Where users are required to maintain their own passwords, they should be provided with a secure and unique temporary password that must expire on initial login.
- b) **Password resets:** The user identify must be verified prior to providing a replacement or temporary password as per the procedure.
- c) **Password notifications:** Temporary passwords must be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided.
- d) **Password Storage:** Passwords must never be stored on a computer system in an unprotected (clear text) form.
- e) **Acknowledgement:** Users should acknowledge receipt of passwords.
- f) **Default Passwords:** Default systems and applications passwords must be altered following installation of systems or software.

9. USER ACCESS REVIEWS

Access Review helps to protect the confidentiality, integrity and availability of assets by ensuring that only authorised users are able to access or modify them.

Access Reviews must be conducted at least annually or earlier as outlined in **Section 7.1 Triggers** due the fluid nature of the SESLHD workforce to ensure that staff, contractors and vendors who have changed their status are captured as a mitigation to missing notifications.

9.1 Triggers

- a) Reviews scheduled in the Operational Security Calendar;
 - i. Regular Systems User Access Review – at least every 12 months
 - ii. Sensitive Systems User Access Review – at least every 6 months
 - iii. Privilege User Access Review – at least every 3 months
- b) When a security incident has occurred.

- c) A major change to a system (change in 3rd party management of system, migration to new platform or major version change, etc.) as a result of change management.

10. COMPLIANCE REPORTING AND MONITORING

UAM must where possible be monitored to ensure that the policy and processes are effective and achieving the level of compliance required. SESLHD ICT may use an automated mechanism for reporting the compliance of systems that are in the SESLHD domain and UAM application.

Systems that cannot be actively monitored must have a schedule determined by the risk posture that would determine the frequency of the checks.

Specialists IT that manage systems not under SESLHD ICT management or connected to the State-Wide Active Directory (SWAD) are responsible for confirming compliance of their systems and taking prompt remedial action where systems are found to be not fully compliant.

The status must be reported to the SESLHD Information Security Governance Council (ISGC) and SESLHD ICT Director at least annually or more frequently depending upon the risk and threat landscape assessment. The reporting must list key parameters such the following as but not limited to:

- a) Identity;
- b) Current privileges categorised against access type;
- c) Last login;
- d) Status (disabled/enabled/terminated).

Compliance reporting details can be found in the SESLHD Compliance reporting process and procedures documents.

11. DOCUMENTATION

Procedural documentation for the management of User Access is described in the [User Access Management Procedure](#).

12. REFERENCE DOCUMENTS

The following documents are referenced in this policy:

Legislation, Policies and Guidelines.

- a) [SESLHD Information Security Policy SESLHDPD/310](#)
- b) [NSW Government Cyber Security Policy](#)
- c) [NSW Health Policy Directive PD2020_046 - Electronic Information Security](#)
- d) [eHealth Password Policy HS/2013_07](#)

12.1 Standards

- a) ISO 27001:2013 Information technology - Security techniques - Information security management systems.

- b) ISO/IEC 27002:2013. Information Technology - Security Techniques - Code of Practice for Information Security Management.
- c) ISO 31000 Risk management - Principles and guidelines

13. DEFINITIONS

Administrator: a user account with elevated privileges. Administrative accounts allow execution of tasks that can alter the configuration of systems and resources.

Administrative Account: administrative accounts allow execution of tasks that can alter the configuration of systems and resources.

Asset: anything of value to SESLHD, such as hardware and software components, communication systems, data, personnel, documentation, reputation and public confidence.

Authentication: to verify the identity of an entity requesting the use of a system and/or access to network resources. The steps to giving an entity access to an object should be identification, authentication, and authorisation.

Brute Force: a mechanism by which a computational action is used to achieve a predefined goal. Brute force attacks continually try different inputs to identify weak passwords to gain unauthorised access.

Contextual Authentication: is where the context (or factors) around a user's login are considered and assessed, to then decide whether the person is who they say they are. Such factors may be; location, IP address, device name and time.

Cracking: a mechanism by which security controls are circumvented to gain access to resources and services.

Lockout: a security mechanism by which a user account is automatically locked out if a set number of failed login attempts occur within a specified period of time.

Malicious User: a malicious user is any user deemed to be acting deliberately out of malice with harmful intentions towards NSW Health.

One-Time-Password (OTP): a password only used once, thus countering replay attacks.

Oracle IDM/ IDME/ SWAD: the identity management solution implemented by NSW Health to manage user lifecycle by interaction for the Oracle HRIS system. Primarily, this system manages the account lifecycle within the Oracle product suite with connectors into the NSWHEALTH.NET domain to manage accounts within Active Directory.

Resource: a means provided by SESLHD ICT systems or departments to facilitate an organisational objective. Resources may include file servers, printers, network access etc.

Resource Account: resource accounts are assigned to SESLHD ICT Systems in the State-Wide Active Directory services, such as meeting rooms, pool cars etc. These accounts differ from ordinary user accounts as they are not assigned to an individual and hence cannot provide an audit trail back to an individual user.

Server: a computer (including mainframes) used to run programs that provide services to multiple users. For example, a file server, email server or database server

Service: a means of delivering value to staff by facilitating a number of components such as IT software, hardware, and facilities to meet SESLHD ICT Systems objectives.

Service Account: service accounts allow authenticated access to manage and access services. These accounts differ from ordinary user accounts as they are not assigned to an individual and hence cannot provide an audit trail back to an individual user.

State-Wide FIM Solution: an identity management solution initially developed by the Oracle IDM with Dimension Data to facilitate the user lifecycle for Active Directory (AD) systems not in the NSWHEALTH.NET forest. This has been further refined by the SWIS team in conjunction with the Oracle IDM and Dimension Data teams to work within the State-Wide Active Directory (SWAD) solution and still provide user lifecycle management to Active Directories outside the NSWHEALTH.NET domain i.e. child domains like hneahs.nswhealth.net and other domains like int.ncahs.net

Third Party: any person or organisation outside of SESLHD employment that requires access to SESLHD Information Systems resources. Third Party includes any contractors or vendors with a work order to perform a body of work on behalf of SESLHD.

Threat: a potential cause of an event.

Unauthorised: any type of access by an entity without having any authority, or has not been granted explicit access rights to a resource are deemed unauthorised.

User: any end User of SESLHD SWAD services including; elected officials, full- time, part-time, and temporary employees, officers, agents, contractors, consultants, and volunteers or any individual authorised to use SESLHD’s computing and communications systems assets.

Vulnerability: a weakness of an asset or group of assets that can be exploited by one or more threats.

14. VERSION AND APPROVAL HISTORY

Date	Version	Version and approval notes
March 2019	DRAFT	Initial draft. Shane Feeney, Program Manager ICT Security and Strategy
May 2019	DRAFT	Listed on Draft for Comments. No feedback received. Final version approved by Executive Sponsor. Formatted by Executive Services prior to tabling at June 2019 Executive Council Meeting.
June 2019	1.0	Endorsed at June 2019 Executive Council meeting.
16 September 2024	1.1	Minor review to update references and position titles.