University System of New Hampshire

# ACCOUNT MANAGEMENT STANDARD

**Responsible Executive/University System Officer:** Chief Information Security Officer
**Responsible Office:** Cybersecurity Governance Risk and Compliance (GRC)
**Approved Distribution:** PUBLIC
**Status:** IN FORCE

## 1. PURPOSE

Enterprise Technology & Services (ET&S) is charged by the University System of New Hampshire (USNH) to protect the integrity, confidentiality, and availability of systems and information. This standard establishes directives for managing the digital identity accounts that facilitate access or changes to USNH's information technology resources.

## 2. SCOPE

This standard applies to the following accounts issued from the University System of New Hampshire:

- **Primary Account**
  Primary accounts are the most common account type. It is often referred to as the USNH username and password. All active faculty, staff, and students of GSC, KSC, PSU, UNH, and the USNH System Office are assigned a Primary Account, usually named after the individual (ex: firstname.lastname@yourinstitution.edu). Primary Accounts allow individuals access to USNH information technology systems, devices, and services, requiring single sign-on (SSO). Examples include Canvas, Microsoft Office 365, and Kronos. All Primary Accounts are subject to USNH Information Security Standards and Policies, and the individual to whom the Primary Account is assigned is responsible for the appropriate use of that account.

- **Secondary Account**
  The secondary account also referred to as privileged or elevated access account. This is a second account with a different username and password that is assigned to an individual who has a business need that requires multiple accounts with varying levels of access (i.e., system administrators who require administrative accounts with elevated security permissions, which

must be separate from those of their Primary Accounts). All Secondary Accounts are subject to all USNH Information Security Standards and Policies, and the individual to whom the Secondary Account is assigned is responsible for the appropriate use of that account.

- **Pool Account**
  This IT Account is controlled by a designated USNH employee, called the Guardian of the account, and is assigned to a specific person, called the account user (usually an hourly or temporary student employee), with a set expiration date. The Guardian of the account will supervise the use of this account, ensure that it is used in compliance with all USNH and all Information Security Standards and Policies, and work with the IT Account Administrators to maintain the records related to users of the Pool Account. The default expiration dates for Pool Accounts are set to the end of the current fiscal year (unless otherwise noted) but no longer than one year. Over time, the Pool Account can be re-assigned to several persons but can never be assigned to more than one person at a time. Upon notification by the Guardian that the user of the account has left their position, IT Accounts Administrators will disable the Pool Account. When there is a new user who requires the use of the Pool Account, the Guardian is responsible for requesting that it be re-activated and re-assigned. All Pool Accounts are subject to this and all USNH Information Security Standards and Policies, and the individual to whom the Pool Account is currently assigned is responsible for the appropriate use of that account.

- **Sponsored IT Account**
  This type of primary account is assigned to a non-affiliate of the University who has business with USNH requiring access to IT resources. This includes, but is not limited to, volunteers, contractors, visiting students, and scholars. Sponsored IT Accounts require yearly approval and renewal by a President, Vice President, Provost, Dean, or Designated Sponsor Representative (DSR). All Sponsored IT Accounts are subject to this and all USNH Information Security Standards and Policies. The individual to whom the Sponsored IT Account is assigned is responsible for the appropriate use of that account.

- **Service Account**
  A service account is a dedicated account with escalated privileges for running applications and other processes. Service accounts may also be created to own data and configuration files. They are not intended to be used by people except for administrative operations.

University System of New Hampshire

## 3. AUDIENCE

All USNH community members and partners who use authenticated access to USNH information technology resources should be familiar with this standard.

## 4. STANDARD

Account management includes requesting, issuing, modifying, and disabling all USNH information technology accounts. All account access considerations shall be made per the USNH Access Management Standard.

### 4.1 Account Creation

- Before creating user accounts, the sponsoring unit or division shall verify the user's affiliation with USNH.

- Accounts are reserved for USNH faculty, staff, students, and applicants. Other individuals affiliated or otherwise needing USNH credentials shall request an account provisioned per the USNH Sponsored Account Standard.

- Enterprise information technology account usernames shall conform to the USNH account username convention.

- Accounts shall be provisioned following a role-based access scheme.

- The principle of least privilege shall be applied when provisioning accounts. Users shall not be granted any more privileges than necessary for functions the user will be performing.

    - Non-privileged user accounts must be used and only elevated to root or Administrator when necessary. A secure mechanism to escalate privileges (e.g., via User Account Control or via sudo) with a standard account is acceptable to meet this requirement.

    - Privileged accounts must not be used for non-privileged activities.

    - USNH enterprise administrative accounts are reserved for USNH employees with a demonstrated need.

- All privileged account activity is required to be logged and monitored per the USNH Log management standard.
    - Vendor or contractor accounts requiring elevated privileges shall make arrangements per the USNH Sponsored Account Standard and/or the Exception process.

- There shall be one user associated with an account.

- Account usage requires the account owners' formal review acknowledging they have read and understood the USNH Acceptable Use Policy (AUP).

- Devices must be configured with separate accounts for privileged (administrator) and non-privileged (user) access.

## 4.2 Account Management

- ET&S shall establish and maintain an inventory of all information technology accounts managed within USNH.

    - The inventory, at a minimum, shall contain the user's first and last name, username, start/ stop dates, and department.

- When feasible, centralized authentication and account management shall be employed through the central USNH directory or identity service.

### 4.2.1 Account and Access Reviews

- All active USNH privileged accounts shall be authorized on a recurring schedule, at a minimum annually.

- Access modifications shall include valid authorization from appropriate administrative, academic, or business unit management and ET&S.

    - The Identity and Access Management team shall review active directory-privileged accounts.

    - The appropriate business unit leadership shall review local privileged/administrative accounts.

- The employee's manager is responsible for reviewing employee accounts and access privileges with ET&S upon job changes (e.g., termination, position changes).

### 4.3 Account Protection

- All accounts used to access USNH's information technology resource shall comply with the USNH Password Policy
- System administrator accounts shall use centralized authentication.
- Central authentication systems should lock user accounts in accordance with industry best practices.
- Administrators shall verify user identity prior to re-enabling or resetting user accounts.
- Multi-factor Authentication (MFA) shall be implemented with all USNH administrator accounts.

### 4.4 Disabling and Deletion of Accounts.

- Accounts out of compliance with the USNH Password Policy will be disabled and may be deleted.
- All user accounts must be deprovisioned, and access attributes removed immediately upon separation unless a prior exception is in place.
    - Faculty leaving USNH in good standing may request access for up to 90 days past their last day of employment.
    - ET&S will assist users with data transfer upon request.
- Self-service mechanisms may not be used to re-enable the account.

### 4.5 Local Administrative Accounts

Local administrative accounts may be created to provide administrative access for individuals to conduct Privileged Access on USNH-owned devices for academic and research purposes only. USNH ET&S does not create these accounts, and they are not managed as USNH accounts. The responsibility for these accounts is owned solely by the local account owners. Owners of such accounts are responsible for compliance with all USNH policies and standards and all local, state, and federal laws.

University System of New Hampshire

## 5. MAINTENANCE OF THIS STANDARD

As part of the mandatory annual review of this Standard required by the USNH Cybersecurity Policy, the processes and procedures that support the requirements defined in this Standard shall be reviewed and updated to ensure currency and continuous improvement.

## 6. ENFORCEMENT

Failure to comply with this Standard puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations (e.g., student conduct and/or applicable personnel policies). Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO (Chief Information Security Officer) and/or CIO (Chief Information Officer).

## 7. EXCEPTIONS

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the Cybersecurity Exception Standard.

## 8. DEFINITIONS

See the ET&S Policy & Standard Glossary for complete definitions of each term.

- Access
- Accounts
- Authentication
- Availability
- Centralized Account
- Centralized Authentication
- Confidentiality
- Integrity
- Least privilege
- Password
- Privileged Access
- Provision

- Role-based access
- Service account
- Single sign-on
- Standard

## 9. RELATED POLICIES AND STANDARDS

- Access Management Standard
- USNH Acceptable Use Policy
- Cybersecurity Policy
- Exception Standard
- Password Policy
- Security Configuration Management Standard

## 10. REFERENCES

Center for Internet Security. (2021). CIS critical security controls version 8.2

http://www.cisecurity.org/controls/

## 11. CONTACT INFORMATION

For USNH community members: Questions about this standard, requests for additional information or training, or report violations can be directed to Cybersecurity Governance, Risk, & Compliance (GRC) via this Support Form.

A community member may submit other requests here: Submit an IT Question.

## 12. DOCUMENT HISTORY

Effective Date: October 18, 2022
Drafted: USNH Cybersecurity GRC
Reviewed by: USNH Cybersecurity Committee
Approved by: Thomas Nudd, Chief Information Security Officer