University System of New Hampshire

PRIVILEGED ACCESS MANAGEMENT STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: PUBLIC
Status: IN FORCE

1 PURPOSE

The University System of New Hampshire (USNH) is committed to preserving the privacy of the individuals who entrust us with their personal information and to safeguarding the confidentiality, integrity, and availability of all institutional information and information technology resources. As such, this Standard defines privileged access and identifies the security controls required for management of this elevated level of access.

2 SCOPE

This Standard applies to all administrative, academic, and business units at all USNH component institutions and the University System Office. The requirements documented here apply to privileged access granted within all information technology resources that capture, store, process, transmit, or otherwise manage institutional information.

3 AUDIENCE

Any USNH community member with responsibilities that may require a higher-level of access to one or more information technology resources should be familiar with the specifics of this Standard. For example, community members with roles like application administrator, database administrator, or system administrator are likely to need a higher-level of access in order to perform their job duties.

4 STANDARD

Privileged access, which may also be referred to as “administrative access,” “administrator access,” or “super-user” access, is defined as access to a USNH information technology resource that enables an individual to directly modify that resource. For example:

- Access to a database that allows direct modification of the data in that database or to change the structure of the database itself, or to alter the configuration of the server the database sits on, would all be considered privileged access
- Access within an application that allows configuration or modification of the application for other users, allows for granting of access to that application, or that is used to administer that application in a way that the majority of users cannot
- Access to technology infrastructure (e.g., server, disk array, network device, router)
- Access to manage a cloud hosted service

Privileged access makes it possible to compromise the:

- Underlying stability and security of critical information technology resources
- Confidentiality and integrity of institutional information
- Availability of the resources and information necessary to conduct normal operations at all USNH component institutions

As such, additional security controls for managing privileged access shall be followed to mitigate the increased risk of compromise and unauthorized use.

Access to an application where a community member can configure their own experience or take actions within the application that result in modification of the data as the result of normal use of the application would not be considered privileged access.

TYPES OF PRIVILEGED ACCESS

Privileged access can only be granted to those community members whose job responsibilities require it. There are two specific types of privileged access recognized at USNH.

Administrator Access

Administrator access is associated with specific types of roles like system administrator, database administrator, or network administrator. Although this type of privileged access encompasses the administration of a range of information technology resources, for ease in differentiation, this type of privileged access is referred to as Administrator Access throughout this Standard.

This type of privileged access provides one of the following types of authorizations, which are defined in more detail later in this Standard.

- Application Administrator Accounts
- Database Administrator Accounts
- Device and Interface Administrator Accounts
- Server Administrator Accounts
- System Administrator Accounts

Elevated Access

This type of privileged access relates specifically to authorizations that provide super-user level access to perform functions within an application. Unlike an Application Administrator Account, this access is not built into the application. It is an account set-up within the application to perform privileged functions like enabling access or determining authorization levels for other accounts, up to and including administering, configuring, or otherwise managing the application itself.

Elevated access may authorize a community member to perform an action or interact with information as another community member or to add/modify/delete information belonging to other community members in ways that other community members who do not have elevated access would not be able to.

SHARED ADMINISTRATOR ACCESS REQUIREMENTS

Administrator accounts, as defined in this section, are not generally associated with a named individual but are used by a small team that is responsible for administering the application, database, or other information technology resource. The team approach is only allowed when:

1. It is required to ensure redundant coverage for support of the application AND
2. The password for the account is managed in an approved password vault tool, where it can be checked out by authorized community members when this level of privileged access is required AND
3. For Application Administrator Accounts only, the application only allows for one account with this kind of authorization to exist within the application.

This is one of the few circumstances under which it is allowable for a shared account to exist at USNH.

Although this type of account cannot be tied to a non-primary identity, whenever possible, it should mirror the naming convention defined for non-primary identities used to provide administrator access defined in the *Non-Primary Identity Management Standard*.

This type of privileged access is considered a system administrator-level authorization under the *USNH Password Policy*. Additionally, as more than one individual has knowledge of the password for these accounts, the password shall also be changed whenever the membership of the team administering the information technology resource changes.

Any actions with this type of account must be logged, whenever it is technically possible to do so, to ensure an audit trail exists

Application Administrator Accounts

Application administrator access exists entirely within the bounds of the application that is being administered and is the account built into the application to provide full administrative control of the

application. For example, when setting up most web applications, there is an account built into the application, often called “admin” or “administrator” that has all rights over the configuration and management of that application.

If the individuals responsible for administering the application also need user-level (non-privileged) access that allows them to use the application, the non-privileged access shall be provided by a separate authorization. The account used for administering the application cannot be used to perform non-privileged actions.

Database Administrator Accounts

Database Administrator access is provided by a local “root” or master account that exists within and provides full access to the database. It allows creation, modification, and deletion of all databases within that instance and is also authorized to setup other identities and authorize access to databases.

If the individuals responsible for administering the database also need user-level (non-privileged) access that allows them to use the database, the non-privileged access shall be provided by a separate authorization. The account used for administering the database cannot be used to perform non-privileged actions.

Device and Interface Administrator Accounts

Device and Interface Administrator access is provided by a local account that is embedded in the operating system of the device. These accounts are used for management and administration of Internet of Things (IoT) devices including, but not limited to, cameras, printers, network switches, uninterruptible power supply (UPS) systems, temperature sensors, and lights-out-management interfaces.

Server Administrator Accounts

Server administrator access is provided by a local master account that exists within the operating system installed on a server. This is the equivalent of a local admin account on a desktop or laptop. It is the “administrator” account on Windows servers, the “root” identity on a Linux/Unix server, and the first user account created on a macOS installation.

Although this type of administrator account must exist, it shall not be used to gain direct access to these resources, except in emergency situations. Regular access to these resources is provided via other mechanisms defined here.

This information is provided in the Standard for clarity only.

System Administrator Access Requirements

System administrator access is granted to a specific named individual using a non-primary identity and

cannot be granted to an individual's primary identity or authorized for any account tied to a primary identity. A non-primary identity is used to enable this kind of access as it segregates privileged access from non-privileged access and decreases the likelihood of, and potential for, unauthorized use of the privileged access.

System administrator access applies to management of operating systems as well as applications, appliances, or tools.

Non-primary identities established for the purposes of enabling privileged access shall follow the following naming convention adm_username as defined in the *Non-Primary Identity Management Standard*.

System administrator access can only be used to perform actions that require privileged access. Non-privileged actions like checking email, using an internet browser, etc. shall only be performed with the individual's non-privileged access.

Although a system administrator account is, by nature, a privileged account, it shall still be configured based on least privilege, and only the privileged access needed to perform job duties shall be granted. Privileged access and additional permission within that authorization shall never be granted "in case" a community member might need them.

System administrator accounts can only be used by one individual and all access granted to the non-primary identity used to provide the access shall be revoked when the community member's primary identity access changes.

This type of privileged access is considered a system administrator-level authorization under the *USNH Password Policy.*

Any actions with this type of account must be logged, whenever it is technically possible to do so, to ensure an audit trail exists

ELEVATED ACCESS REQUIREMENTS

Elevated access is granted to a specific named individual using a non-primary identity, whenever technically possible and administratively practical, and should not be granted to an individual's primary identity or authorized for any account tied to a primary identity.

A non-primary identity is used to enable this kind of access as it segregates privileged access from non-privileged access and decreases the likelihood of, and potential for, unauthorized use of the privileged access.

Non-primary identities established for the purposes of enabling elevated access shall follow the naming convention adm_username as defined in the *Non-Primary Identity Management Standard*.

Elevated access shall be configured based on least privilege, and only the privileged access needed to perform job duties shall be granted. Privileged access and additional permissions within that authorization, shall never be granted "in case" a community member might need them.

Elevated access accounts are not considered system-administrator-level authorizations for the purposes of password management.

GRANTING PRIVILEGED ACCESS

Privileged access shall only be granted to individuals who have an active USNH employee role associated with their primary identity, as defined in the *Identity Management Standard*.

Sponsored users and students at USNH component institutions cannot be granted privileged access to any USNH information technology resource. In circumstances where this type of access is necessary to fulfill a business need, an exception to this Standard shall be requested and approved.

Administrator Access to information technology resources shall be requested through the Cybersecurity Ops, Engineering & IAM (IAM) team according to the standard processes and procedures provided. This ensures that access will be disabled/deprovisioned appropriately using standard deprovisioning procedures.

Elevated Access shall be requested via the standard request process for the specific application where the access is needed.

Requests for all privileged access shall have documented approval from the appropriate Technology Service Owner or Data Steward. Both the request and approval shall be stored for at least 12 months to preserve the audit trail.

Cybersecurity IAM is responsible for defining standard request/approval processes and procedures for privileged access.

All individuals who are granted privileged access shall be required to sign the *Enterprise Technology & Services Confidentiality and Cybersecurity Agreement* before the access is granted and annually thereafter as part of the annual privileged access review process.

Cybersecurity GRC is responsible for maintaining the *Enterprise Technology & Services Confidentiality and Cybersecurity Agreement*, preserving signed copies of this agreement for all individuals who are required to sign it, notifying individuals when their agreement shall be resigned, and tracking completion of initial and annual renewal agreements.

ANNUAL PRIVILEGED ACCESS AUDIT

Business Application Owners and Technology Service Owners shall conduct an annual review of

privileged access to the information technology resources under their purview. This review shall confirm:

1. Privileged access for each individual community member is still appropriate based on their current responsibilities.
2. Individuals with privileged access are following the specific requirements for this type of access defined in the *USNH Password Policy*.
3. Individuals with privileged access have agreed to the current *Enterprise Technology & Services Confidentiality and Cybersecurity Agreement* within the past 12 months.

The required annual audit of privileged access shall be conducted as part of the overall annual access audit requirement defined in the *Access Management Standard*. Any privileged access identified as no longer needed during this audit shall be revoked immediately. Revocation date and reason shall be documented as part of audit results to preserve the audit trail.

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO 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 where needed, 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 for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

7 EXCEPTIONS

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

University System of New Hampshire

8 ROLES AND RESPONSIBILITIES

Business Application Owner/Technology Service Owner:

- Approve/deny requests for privileged access
- Complete annual access audit process

Data Steward:

- Approve/deny requests for privileged access
- Complete annual access audit process

Cybersecurity Ops, Engineering, & IAM (IAM):

- Preserve privileged access request and approval audit trail
- Define request/approval processes and procedures for privileged access
- Support the annual access audit process as defined in the *Access Management Standard*

Cybersecurity GRC:

- Maintain the *Enterprise Technology & Services Confidentiality and Cybersecurity Agreement*
- Maintain audit trail of agreement for all individuals who are required to sign it
- Notify individuals when their agreement shall be resigned
- Track completion of initial and annual renewal confidentiality agreements
- Support the annual access audit process as defined in the *Access Management Standard*

USNH Community Members Requiring Privileged Access:

- Request privileged access to information technology resources through the appropriate processes
- Sign the *Enterprise Technology & Services Confidentiality and Cybersecurity Agreement* when privileged access is requested, and annually thereafter, as part of the annual privileged access review process

9 DEFINITIONS

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

- Access
- Administrator
- Authorization
- Availability
- Confidentiality

- Data Steward
- Elevated Access
- Guest/Lab Account
- Identity
- Information
- Information Technology Resource
- Institutional Information
- Integrity
- Internet of Things (IoT)
- Least Privilege
- Non-Primary Identity
- Password
- Primary Identity
- Privileged Access
- Security Control
- Server
- Service Account
- Technology Service Owner
- USNH Community Member

10 Related Policies and Standards

- USNH Cybersecurity Policy
- USNH Password Policy
- Access Management Standard
- Identity Management Standard
- Cybersecurity Exception Standard
- Non-Primary Identity Management Standard
- Password Management Standard

CONTACT INFORMATION

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

All other requests can be submitted here: Submit an IT Question.

University System of New Hampshire

DOCUMENT HISTORY

Effective Date:	14 OCT 2022
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 27 JAN 2021 V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 05 NOV 2020 V0.2
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, JAN 2021 CYBERSECURITY POLICY & STANDARD WORKING GROUP, OCT 2022
Revision History:	REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 05 MAR 2020 DR. DAVID YASENCHOCK, 14 OCT 2022