University System of New Hampshire

ACCESS MANAGEMENT STANDARD

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

1 PURPOSE

The University System of New Hampshire (USNH) is committed to promoting secure and appropriate access to its information and information technology resources. This Standard defines the baseline security controls designed to minimize the potential for unauthorized access to or use of information technology resources and the information they contain and to preserve and protect the confidentiality, integrity, and availability of USNH information and information technology resources.

2 SCOPE

This Standard applies to all administrative, academic, and business units at USNH and its component institutions. The requirements documented here apply to all information technology resources that capture, store, process, transmit, or otherwise manage institutional information.

3 AUDIENCE

All USNH community members, including but not limited to applicants, faculty, staff, students, prior students/alumni, and emeriti of all USNH institutions should be familiar with the specifics of this Standard.

4 STANDARD

COMMUNITY MEMBER RESPONSIBILITIES

All USNH community members are responsible for all actions carried out using any account associated with a USNH information technology resource issued for their use. As such, account holders shall take all reasonable actions to safeguard institutional information and USNH information technology

resources by protecting their accounts from unauthorized use and compromise, including, but not limited to, the following:

- Completing all cybersecurity training required for their role
- Creating passwords that comply with the *USNH Password Policy* and maintaining the confidentiality of those passwords for all USNH accounts under their control
- Securing workstations and mobile devices by engaging the screen lock before leaving them unattended
- Taking care not to misuse their USNH accounts. Examples of misuse include, but are not limited to:
    - Using access granted to view or modify information they are not authorized to view or modify
    - Allowing anyone else to access information or resources, which includes providing access to parents, spouses, children, or any other relatives for any purpose, even to perform actions on their behalf
    - Using anyone else's USNH account to gain access to information or resources they are not authorized to access

MANAGER RESPONSIBILITIES

Managers of USNH employees, including students, are responsible for notifying Enterprise Technology & Services (ET&S) when individuals change jobs from one part of the University System (or one of its component institutions) to another. This ensures that an access review can be completed, and modifications can be made so that each individual has access to only those information technology resources appropriate for their role(s).

ACCESS MANAGEMENT OVERVIEW

Access to information technology resources and the institutional information those resources capture, store, process, transmit, or otherwise manage shall be granted based on business need and the concept of least privilege. This means that USNH community members shall only be granted access to those information technology resources, and information required to fulfill their responsibilities.

Access to most USNH and component institution information and information technology resources requires three things.

> First, an identifier associated with a valid USNH identity, an accepted federated identity, or an identity established for the purposes of collaboration on a specific information technology resource.

Second, those with a valid identifier must be able to prove who they are through the process of authentication.

Third, the authenticated identity must be authorized to access the information technology resource or information they are trying to access. This is handled through the establishment of an account or other authorizing mechanism.

IDENTITY

An identity is a set of physical and behavioral characteristics by which an individual entity is uniquely recognizable. Access to USNH information technology resources is generally associated with a primary USNH identity. Access may also be granted using other types of identities, including federated identities or local identities, established on a specific information technology resource (e.g., to support research collaboration). An identity is represented by one or more identifiers, most commonly a username.

To access a USNH information technology resource, authorized individuals shall provide the USNH identifier assigned to them for the purpose of accessing that resource.

Additional Information about USNH identities and identifiers is provided in the *Identity Management Standard.*

AUTHENTICATION

Authentication is the process an information technology resource uses to confirm that a USNH community member, authorized user, device, or other information technology resource is who or what it is claiming to be. Access to any USNH information technology resource that captures, stores, processes, transmits, or otherwise manages institutional information that is classified as anything other than PUBLIC shall require authentication.

Standard Authentication

There are three different factors that can be used to confirm that someone or something is who they claim to be:

- Something you know – a password, an answer to a secret question, or a PIN number are all examples of this kind of factor
- Something you have – an application on your phone, an electronic certificate installed on a device, or a physical key that plugs into your device are all examples of this kind of factor
- Something you are – biometrics like a fingerprint, facial recognition, or a retinal scan are all exampled of this kind of factor

To authenticate, USNH community members or the devices they are using shall provide a confirmed USNH identifier and the requested factors. The factor(s) provided must match the factor(s) associated with that identifier within the USNH resource. Commonly used methods of authentication include username & password, biometrics, and device certificate.

Multifactor Authentication

There are some information technology resources at USNH that require an additional level of protection to authenticate USNH community members. In these cases, multifactor authentication (MFA), which requires that USNH community members provide 2 different factors from the list above, shall be used.

Central Authentication

Authentication services can be handled, using a central repository of identifiers and authentication factors. This type of authentication can be used to authenticate USNH community members across multiple information technology resources using the same identifier/authentication factor set.

A centrally managed account is created and managed in a central directory, allowing it to be used to access many information technology resources. These accounts use a single set of credentials (e.g., USNH username associated with a USNH identity and the password paired with that username) to access many information technology resources.

Central authentication services can provide both standard authentication and MFA, and is the mechanism used to provide single sign on (SSO) capabilities. This is the preferred method for authenticating USNH community members and shall be used wherever it is technically possible to do so.

Local Authentication

In some cases, information technology resources require local authentication, which means USNH community members need a set of credentials (e.g., username and password) that are different from a community member's centrally managed USNH credentials and that are only used to access that resource. Local authentication uses locally managed accounts, which are created in local repositories within a specific computer, device, or application, to enable access. In cases where local authentication must be used, USNH community members shall not use their USNH password as their authentication factor.

Each information technology resource that uses a locally managed account shall have separate credentials that are only used to access that resource. Use of local application accounts must adhere to the requirements outlined in the relevant Standards.

Administrators of information technology resources that must use local authentication shall, whenever possible, utilize USNH usernames as the authentication identifier or instruct USNH community members to use their USNH username as the authentication identifier/username for that application. Additionally, per the requirements in the *USNH Password Policy*, application administrators shall instruct

and encourage USNH community members not to reuse their USNH password as the password in any locally authenticated information technology resource.

AUTHORIZATION

Authorization is the third element that is required when accessing USNH information and information technology resources. Where identity confirmation and authentication are used to determine and confirm the USNH community member's identity, authorization defines what that community member can access, as well as what they can do with that access.

Authorization can occur on several different levels.

A USNH community member can be authorized to access an information technology resource, which is usually done with an account. The account pairs credentials with a set of permissions, which are the specific instructions defining what that account is authorized to do. When a USNH community member has an account for a resource, they are authorized to access it. For some information technology resources, this is the only level of authorization required, USNH community members either have access or they don't.

However, most information technology resources use multiple levels of authorization in order to ensure that each community member only has access to the information and functionality necessary. This structured authorization is called the principle of least privilege. To ensure each USNH community member is only able to access what they need to, specific authorizations, also called permissions, are associated with each account. The permissions granted to an account determines what information that account can access and what functions it can perform.

Permissions can also be grouped into roles which simplifies management of access for groups of USNH community members that need the same level of access. Roles used for authorization can be coarse-grained, like those defined in the *Identity Management Standard*, but they can also be fine-grained or information resource specific.

To demonstrate, if the information technology resource was a house, having an account, the first level of authorization, allows a USNH community member to come through the front door but the other levels of authorization, organized by permissions or roles, determine where that community member can go, what they see, and what they can do once they are inside.

Least Privilege

Authorization to access USNH or component institution information and information technology resources shall be based on job function, responsibilities, and/or need-to-know according to the principle of least privilege. Individual USNH community members, groups of USNH community members, and roles shall only be authorized to access the information and functionality necessary for the work to be performed or access needed, and no more.

University System of New Hampshire

ACCESS PROVISIONING

Any information technology resource that captures, stores, processes, transmits, or otherwise manages PROTECTED, RESTRICTED, or CONFIDENTIAL information per the *USNH Information Classification Policy* shall have documented access management procedures that meet the minimum requirements outlined in this Standard.

Gaining access to information and information technology resources is done is several ways, as outlined below.

Birthright Access

There is a level of role-based access provided to all USNH community members as soon as their USNH credentials are established. This is called birthright access. Birthright access is coarse-grained role-based, which means it differs based on the active roles associated with the community member's primary identity – an employee's birthright access is different than the birthright access for students. Birthright access changes when the active coarse-grained roles change, ensuring that birthright access also follows the principle of least privilege.

Cybersecurity Ops, Engineering, & IAM, in collaboration with the necessary Business Application and/or Technology Service Owners, is responsible for defining the appropriate access for each established USNH coarse-grained role. This team is also responsible for the processes, procedures, and tools required to provision, deprovision, and modify access for all USNH coarse-grained roles. Birthright access authorization within each individual application is the responsibility of the Business Application and/or Technology Service Owners, of that application.

Fine-Grained Role Based Access

Fine-grained role-based access builds upon Birthright Access, granting access based on user characteristics or attributes. Examples of these attributes are which college a community member belongs to, which class a student is taking, or the department where a community member works.

Request/Approval Access

Access to some USNH information and information technology resources cannot be granted at the coarse-grained or fine-grained role level. In these cases, access is granted on a request/approval basis. To gain access to these USNH information technology resources and the information those resources support, an individual request for that USNH community member shall be made using the designated USNH or institutional process for that resource.

Privileged Access

There are also circumstances where a USNH community member needs an authorization level that allows them to modify the information technology resource itself or the information captured, stored,

processed, transmitted, or otherwise managed by that resource, rather than simply utilizing it. This level of authorization is called privileged access. Definitions, requirements, and security access controls related to this type of authorization are documented in the *Privileged Access Management Standard.*

Sponsored Access

Access to most USNH information technology resources requires that a USNH community member have a USNH identity AND an active coarse-grained role. When there is a need to provide access to an individual who lacks an active, coarse-grained role (e.g., to provide access for a contractor or vendor), that access shall be authorized under the Sponsored Use program. Definitions and information about Sponsored Use and sponsored access are documented in the *Sponsored/Guest Access Management Standard.*

ACCESS MANAGEMENT RESPONSIBILITIES

All administrative, academic, and business units engaged in provisioning, modifying, deprovisioning, and/or managing access shall develop processes and procedures, and implement tools to enable those processes and procedures, that meet the requirements defined below.

Birthright Access

- Requests to add a new information technology resource authorization to birthright access shall be sent to Cybersecurity Ops, Engineering, & IAM
- This team, with the oversight of the Chief Information Security Officer (CISO), has the authority to add authorizations to birthright access and to remove them
- Any request to add an authorization for an information technology resource or resources to the birthright access for a coarse-grained role shall include documentation that explicitly lists the authorizations included for all USNH community members within a coarse-grained role or across coarse-grained roles, as appropriate
    - For example, adding something like the learning management system to birthright access for Faculty would require a detailed explanation of what information and functionality within the learning management system each faculty member is automatically authorized to access
- This documentation shall be included in the access management processes and procedures for that information technology resource and reviewed, annually, as part of the mandatory annual review of access management documentation

Fine-Grained Role Access

- Requests to add a new information technology resource authorization using fine-grained roles shall be sent to Cybersecurity Ops, Engineering, & IAM

- This team has the authority to add authorizations to fine-grained role-based access and to remove them
- Any request to add an authorization for an information technology resource or resources using fine-grained role-based access shall include documentation that explicitly lists the authorizations included for each fine-grained role
- This documentation shall be included in the access management processes and procedures for that information technology resource and reviewed, annually, as part of the mandatory annual review of access management documentation

Access Request and Approval

- There shall be a defined method for USNH community members to request access, notify administrators of a change to access, and request access be removed for each information technology resource that requires authorization
- There shall be an approval process that involves either the service owner of that resource or the data stewards (or their designee) for the information contained on it or accessed through it
- Use of central authentication shall be pursued whenever possible
- Use of role-based authorization schemes over individual authorizations shall be pursued whenever possible
- Access shall be granted at the most granular authorization level possible
- Access shall not be granted to any USNH or component institution information or information technology resource until the required approvals are complete
- An audit trail that contains the details of the request and that documents all required approvals shall be preserved as outlined in the Access Management Audit section of this Standard
- Account approvals shall be retained until the next access audit, as defined below, is performed for that resource

Modifications to Access

When formal notification of a requirement to modify a community member's access is received, modification will be made first by resetting that user's access to only provide Birthright Access based on coarse-grained role and any appropriate fine-grained role-based access. This process may involve a review of existing access to determine the optimal approach to ensuring appropriate access is maintained. Any access based on a request/approval process will need to be reauthorized per the regular process.

Deprovisioning Access

Loss of a specific coarse-grained role and/or attributes that enable fine-grained role-based access shall result in deprovisioning of any access automatically granted based on those roles. Deprovisioning requirements for request/approval-based access are defined in the *Accounts Management Standard*.

University System of New Hampshire

PHYSICAL ACCESS TO USNH INFORMATION AND INFORMATION TECHNOLOGY RESOURCES

Physical access to USNH information technology resources used to capture, store, process, transmit, or otherwise manage institutional information classified other than PUBLIC shall be limited to USNH community members who have a need to access them as determined by job responsibilities. Access to the facilities where those resources reside shall be restricted according to the requirements provided in the *Physical Information Technology Asset Access and Management Standard* and the *Data Center Facility Security, Access, and Use Standard*.

COMPROMISED ACCESS

Access to USNH information and information technology resources is considered compromised when there is reason to suspect that an unauthorized party or parties has obtained the necessary credentials to access any USNH information technology resources the USNH community member is authorized to access. Upon identification of a compromised account, all centrally managed access authorizations shall be secured until the identity of the USNH community member can be confirmed and the password associated with their USNH username can be changed.

Securing a USNH community member's access temporarily blocks the ability to use that access for any information technology resources that use centrally managed accounts for access.

LOCAL APPLICATION DEVELOPMENT

Applications that are developed by USNH community members for use at USNH or its component institutions shall be designed to support the requirements provided in this Standard as well as those defined in the *System Acquisition, Development, and Maintenance Lifecycle Standard*.

SPECIAL ACCESS MANAGEMENT CONSIDERATIONS

Emeriti Faculty

Access for faculty members who have been granted emeritus status by a University President shall be retained to the level appropriate with their contributions and status for the duration of their lives. As with all USNH access, access granted to Emeriti is intended only for use by the individual with Emeritus status. USNH credentials used to access USNH resources cannot be shared with or used by any other individual.

Revocation of Access

Human Resources (USNH or institutional), Cybersecurity & Networking (CS&N), and the USNH General Counsel's Office (GCO) are authorized to revoke access temporarily or permanently to USNH and institutional information and information technology resources, including Birthright Access authorization.

In circumstances where this is warranted, a confidential request will be submitted in writing to CS&N. Requests from Human Resources and the USNH GCO do not require additional approval.

Requests initiating within CS&N require approval by a member of the CS&N management team (CISO and Direct Reports). Documentation of the request, and where required, any approvals, shall be stored confidentially according to procedures defined by Cybersecurity Ops, Engineering, & IAM, which is part of CS&N.

ACCESS MANAGEMENT AUDITING

Annual Access Audit

The Technology Service Owner or Business Application Owner of each information technology resource that requires authorization/accounts is responsible for conducting an annual audit of all access to that resource. The purpose of this audit is to confirm that all USNH community members who have access to the resource, should have access to the resource and that the access each USNH community member has is appropriate for that USNH community member. Timing of these audits should consider academic or administrative calendar implications (e.g., R+30) and should be done around the same time each year.

An access audit report, which shall include the identities of each authorized USNH community member and a description of their authorizations, shall be created during this audit. Senior management of the administrative, academic, or business unit responsible for managing that access shall sign-off on the finalized access audit report. This sign-off confirms that the USNH community members and authorization levels listed on the report have been confirmed and are appropriate and valid based on the USNH community member's job function and the organization's business needs.

This report, along with a list of the identity and authorizations for any USNH community member whose access was deemed inappropriate as a result of this audit shall be provided to Cybersecurity Ops, Engineering, & IAM for review and audit tracking.

Cybersecurity Ops, Engineering, & IAM is responsible for reviewing all inappropriate access lists resulting from access management audits and determining if any additional investigation is required.

Cybersecurity Ops, Engineering, & IAM is also responsible for maintaining records related to these access management audits for a period of 18 months.

Access Management Processes and Procedures Assessment and Audit

At the discretion of the CISO, the access management processes and procedures used by any unit at any USNH institution can be assessed by Cybersecurity Governance, Risk, & Compliance (GRC) to ensure that those processes and procedures include all required security controls. This assessment shall also confirm that all aspects of those processes and procedures are being followed as documented and that an appropriate audit trail is being maintained, including, but not limited to the following:

- A documented request for every account that is manually created
- A documented approval and justification for each account request that requires approval
- Confirmation that every account is held by a USNH community member who is still at the institution
- Confirmation that every account is held by a USNH community member with an appropriate coarse-grained role for the access provided
- Confirmation that the account holder's job function still requires the granted access

Additionally, USNH Internal Audit may perform informal or formal access management audits, as needed, on any USNH or component institution information technology resource.

Situations that are not covered by this Standard or where there is question about whether an employee's account or access rights should be changed or terminated shall be brought to the attention of the CISO for guidance.

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 shall 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*.

8 ROLES AND RESPONSIBILITIES

Administrative, Academic, or Business Unit Leadership:

- Signoff on annual access audits
- Notify Cybersecurity Ops, Engineering, & IAM when an employee changes jobs to ensure access is audited and modified appropriately

Chief Information Security Officer (CISO):

- Review all access management processes and procedures
- Direct completion of access management audits
- Request out of band access audits

Cybersecurity Governance, Risk, & Compliance (GRC):

- Assess all access management processes, procedures, and tools to ensure appropriate security controls are in place and being followed

Cybersecurity Ops, Engineering, & IAM:

- Define the appropriate birthright access for each established USNH coarse-grained role in collaboration with the necessary data steward
- Manage processes, procedures, and tools required to automatically provision, deprovision, and modify birthright access for all USNH coarse-grained roles
- Secure compromised accounts
- Review all inappropriate access lists resulting from access management audits and determining if any additional investigation is required
- Maintain access management audit records for a period of 18 months

Technology Service Owners/Business Application Owners:

- Define, document, and manage the access management processes, procedures, and tools required to provision, deprovision, and modify access to information technology resources

- Conduct an annual audit of all access to information technology resources
- Instruct community members not to use their USNH username or the password associated with their centrally managed USNH account for any locally managed accounts

USNH Community Member:

- Complete all cybersecurity training requirements for their role
- Create passwords that comply with the *USNH Password Policy*
- Maintain the confidentiality of all account passwords
- Use USNH accounts appropriately
- Secure workstations and mobile devices by engaging the screen lock before leaving them unattended

9 DEFINITIONS

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

- Access
- Access Control
- Account
- Administrator
- Authentication
- Authentication Factor
- Authorization
- Availability
- Birthright access
- Business Application Owner
- Central Authentication
- Centrally Managed Account
- Coarse-grained Role
- Compromised Account
- CONFIDENTIAL Information
- Confidentiality
- Credentials
- Data Steward
- Deprovision
- Exception
- Fine-grained Role
- Identifier

- Identity
- Information
- Information Technology Resource
- Institutional Information
- Integrity
- Least Privilege
- Local Authentication
- Locally Managed Account
- Multi-Factor Authentication
- Out of Band
- Password
- Phishing
- Policy
- Privileged Access
- PROTECTED Information
- Provisioning
- RESTRICTED Information
- Security Control
- Service Account
- Single Sign On (SSO)
- Standard
- Technology Service Owner
- Username
- USNH Community Member
- USNH ID

10 RELATED POLICIES AND STANDARDS

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- USNH Password Policy
- Account Management Standard
- Application Administration Standard
- Cybersecurity Exception Standard
- Data Center Facility Security, Access, and Use Standard
- Identity Management Standard
- Physical Information Technology Asset Access and Management Standard
- Privileged Access Management Standard

University System of New Hampshire

- Remote Access and VPN Standard
- Sponsored/Guest Access Management Standard
- System Acquisition, Development, and Maintenance Lifecycle 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.

DOCUMENT HISTORY

Effective Date:	01 MAY 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 02 SEP 2020 V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 13 AUG 2020, V0.2
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 27 JAN 2021 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 13 AUG 2020, V0.2
Revision History:	REVISED PER CYBERSECURITY POLICY & STANDARD WORKING GROUP REVIEW, 12 AUG 2020, V0.2 REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 08 MAR 2020, V0.1