University System of New Hampshire

IDENTITY MANAGEMENT STANDARD

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

1 PURPOSE

This Standard outlines the requirements for establishing and using identities across the University System of New Hampshire (USNH) and its component institutions. A USNH identity, in this context, is the establishment of unique identifiers, associated with a collection of personally identifiable information (PII), to differentiate one specific person from another specific person. At USNH, identities are used to provide access to institutional information and information technology resources.

2 SCOPE

This Standard applies to all USNH community members, including those with current, past, or future relationships with the University System or any of its component institutions.

3 AUDIENCE

All members of the USNH community, including faculty, staff, applicants, students, prior students/alumni, and sponsored users, should review and understand the requirements in this Standard.

4 STANDARD

PRIMARY IDENTITY

Upon establishing a relationship with the USNH or any of its component institutions, each USNH community member shall be assigned a primary USNH identity. This primary identity is represented by two identifiers, a USNH username and a 9-digit USNH ID number. This primary identity shall remain

consistent across USNH and its component institutions for that specific individual for any and all relationships, now and in the future. Each individual person shall only have one USNH primary identity.

For example, if a prospective student applies to both the University of New Hampshire and Plymouth State University, that individual will be assigned one USNH username and USNH ID number that will serve as their primary identifiers at both institutions. If that individual then becomes an employee at Keene State College, they will maintain the same USNH username and USNH ID number assigned to them as an applicant.

This provides identity continuity for an individual who has various relationships with USNH institutions over the course of their lifetimes. To ensure identity continuity, an assigned, confirmed primary identity is never retired, reassigned, or reused.

Establishment of a new primary identity is authorized by the creation of an identity or person record in a designated USNH identity system of record, which includes the employee information system, any of the institutional student information systems, and the sponsored access system. New identity records from identity systems of record are compared against existing USNH primary identities and, when possible, are matched to existing primary identities to provide identity continuity. If there is no primary identity found to match the new identity record, a new USNH primary identity is created for that individual.

The two USNH identifiers, USNH username and USNH ID number, are classified as SENSITVE information in the *USNH Information Classification Policy*. This means that in the general course of business, usernames for other community members can be shared with others inside the community when there is a valid business purpose to do so.

Some email addresses issued to community members include the community member's username in the email address. It is not a violation of this Standard or the *USNH Information Classification Policy* for these email addresses to be used, as needed, for their intended purpose, to send or receive email communications, and while conducting USNH or institutional business. However, this information is still considered sensitive, in that, email addresses for community members other than yourself cannot be shared or published publicly without the approval of the relevant data steward.

Due to the complexity involved and the potential to negatively impact the community member’s ability to access USNH information technology resources, requests to change an assigned username shall not be granted except in very limited, specific circumstances (e.g., change to a username that includes a complete former last name when there is a legal name change). Any username change shall be approved by Cybersecurity Ops, Engineering, & IAM. In circumstances where a username change is approved, a new username will be assigned in alignment with the current USNH username construction standard.

Cybersecurity Ops, Engineering, & IAM, under the oversight of the Chief Information Security Officer (CISO), is responsible for creation and maintenance of all USNH identities. PII used for establishing USNH identities and for the identity matching and confirmation process, shall only be added, deleted,

modified, or otherwise managed from within the appropriate USNH identity system of record, defined above.

While every USNH community member is assigned a primary identity, there are also circumstances where some community members require one or more alternate identities, called non-primary identities. A non-primary identity does not supplant or replace a primary identity, and an individual must have a primary identity with an active role, as defined below, to be granted a non-primary identity for any purpose. Details about non-primary identities are defined in the *Non-Primary Identity Management Standard*.

UNRESOLVED RECORDS

During the primary identity matching and confirmation process, circumstances arise where an automated determination cannot be made as to whether or not a new identity record matches an existing primary identity record. In these circumstances, a new primary identity is not created, and an unresolved record alert is sent to Cybersecurity Ops, Engineering, & IAM. Resolution of an unresolved record may require a more comprehensive examination of the person record, modification of information provided from an identity system of record, or other analysis and investigation.

Cybersecurity Ops, Engineering, & IAM is responsible for coordinating all activities required to address unresolved records. Data stewards for each identity system of record shall be responsible for assisting in the resolution of unresolved records. In some circumstances, resolution of an unresolved record may require data stewards to make modifications to a person record in an identity system of record.

In order to support identity continuity, all USNH community members responsible for creating new identity records in identity systems of record shall endeavor to enter accurate data into those records. Fake dates of birth and/or social security numbers shall not be entered into identity records as this increases the potential for mismatches and duplicate primary identity creation.

USNH COARSE-GRAINED ROLES

USNH community members may have many different relationships with the University System, concurrently, and over time. For example, a current employee at one institution could also be a prior student from another institution; or a current student at one institution could also be an applicant at another institution. These relationships are designated by coarse-grained roles, which are established based on codification of that relationship in one of the USNH identity systems of record. Individuals can have one or more active coarse-grained roles tied to their primary identity at any time.

Coarse-grained roles are used to provide birthright access to information technology resources. Details about access management, including coarse-grained role-based birthright access, are provided in the *Access Management Standard*. Coarse-grained roles apply to these types of community members:

- Applicants
- Students
- Prior Students/Alumni
- Employees
    - Faculty
    - Staff
- Former Employees
- Sponsored Users

Coarse-grained roles are active when the relationship between the individual and USNH or its component institution is active. For example, to have an active coarse-grained role of UNH Student, an individual must be an enrolled student according to the UNH student information system. Individuals may have more than one coarse-grained role active at the same time (e.g., an employee who is also a student would have an Employee coarse-grained role and a Student coarse-grained role).

Coarse-grained roles are added or removed based on actions performed in identity systems of record. For example, after a PSU student graduates from the university and the PSU student information system is changed to reflect the student's shift from an enrolled student to an alumnus, the coarse-grained roles associated with their primary identity are also changed – the PSU Student role becomes inactive and the PSU Alumni role becomes active. If that individual later becomes a faculty member at PSU, a PSU Employee role and PSU Faculty role would both become active.

UTILIZATION OF USNH USERNAME

USNH username acts as a unique identifier for differentiating community members for the purposes of authentication to and authorization within information technology resources. However, it shall only be utilized as a unique identifier within a specific information technology resource if that resource leverages USNH central authentication. See the *Access Management Standard* and *Account Management Standard* for more comprehensive details of this requirement.

USNH username can also be used as a unique identifier for purposes unrelated to authentication and authorization. In these circumstances, USNH username shall be treated as SENSITIVE information per the *USNH Information Classification Policy*. (See the caveat for email addresses containing usernames under the Primary Identity section above)

USE OF USNH ID NUMBER

USNH ID numbers, which may also be referred to as "Student ID numbers", "Employee ID Numbers" or "9 Numbers" are classified as SENSITIVE Information. This means they can be shared, unmasked, amongst USNH and component institution personnel when there is a valid business or academic

purpose to do so. In contexts where there is no business or academic purpose for information sharing, USNH ID number shall be masked to only display the last 4 digits.

As mandated in the *USNH Password Policy*, USNH ID numbers shall not be used to construct passwords for any USNH account.

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 will 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*.

8 ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO):

- Oversee identity management processes and procedures

Cybersecurity Ops, Engineering, & IAM:

- Create and maintain all USNH identities
- Investigate and resolve unresolved records
- Coordinate all activities required to address unresolved records

Data Steward:

- Ensure accurate identity information is entered into identity system or record
- Assist Cybersecurity Ops, Engineering, & IAM in investigating and resolving unresolved records
- Maintain identity information in identity systems of record
- Modify USNH identity records, as needed, to address identity collisions and unresolved record issues

9 DEFINITIONS

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

- Access
- Authentication
- Authorization
- Birthright Access
- Coarse-grained Role
- Data Steward
- Exception
- Identifier
- Identity
- Identity System of Record
- Information
- Information Technology Resource
- Institutional Information
- Non-Primary Identity
- Personally Identifiable Information (PII)
- Policy
- Primary Identity
- Standard
- Username
- USNH Community Member
- USNH ID Number

University System of New Hampshire

10 Related Policies and Standards

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- USNH Password Policy
- Access Management Standard
- Account Management Standard
- Cybersecurity Exception Standard
- Non-Primary Identity 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, & 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, 09 JULY 2020, v0.2
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, SEP 2020 V0.2 CYBERSECURITY POLICY & STANDARD WORKING GROUP, JUNE/JULY 2020, v0.1
Revision History:	REVISED PER CYBERSECURITY POLICY & STANDARD WORKING GROUP REVIEW, JULY 2020, v0.2 REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 01 JUN 2020 v0.1