System

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.

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

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.

There are three different factors that can be used to confirm that someone or something is who the234.05 29.28 reW*nBT

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.

Any information technology resource that captures, stores, processes, transmits, or otherwise manages PROTECTED, or RESTRICTED, information per the 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.

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 fo4 4821 0rQq0.00000912 0 612 792 reW*nBT/F1 11.04 Tf1 0 0 1 1

[redacted]

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

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 involves482.nBT/F4rov2.7 Tmu 0 l.000gTf1 0 0 1 92.304 4820 0 1 T(listeq)

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.

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

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

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

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 M3(g)7Ass)11(et)-3(Ac)11(ces)-2(s)8(an)4(d)3(M3(g)7Ass)1

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.