Effective: *08/08/2022*
Last Revised: *03/12/2024*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Standard Contact:
IT Security Services
security@nebraska.edu

ITS-02: Access, Identification and Authentication Standard

Standard Contents

1. Purpose

The purpose of the Access Control Standard is to define the organization's requirements for enforcing effective access control management. This Standard serves as a statement of objectives for the protection of information assets against unauthorized access while securely enabling authorized users.

2. Scope

This Standard shall apply to all University of Nebraska System ("University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of the University and to which this Standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this Standard.

3. Standard Statement

It is the intention of this Standard to establish an access control capability throughout the University to help the organization implement security best practices regarding access management for general and privileged users, including but not limited to logical, wireless, network, and remote access requirements. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer ("CISO") as defined in **ITS Policy Exception Standard**. The following subsections outline the Access, Identification and Authentication Standard.

4. Access, Identification and Authentication Requirements

4.1 General System Access Requirements

Access to University technology assets will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All requests for users' accounts additions, changes, and deletions of access to University endpoints, networks, systems, data, and/or facilities must be formally requested via the ticketing system and must be authorized by the applicable business owner(s) prior to the provisioning or change of access. All request and approval activities must be formally documented with a valid business justification.

4.1.1 Procedures and Responsibilities

Access control procedures and responsibilities must be defined, documented, maintained, and disseminated to the applicable parties to which they apply.

4.1.2 Privacy and Security Notices

Privacy and security notices must be provided to all University employees, contractors, third-party vendors, and consultants, posted to an internally available intranet site and be consistent with applicable rules.

4.1.3 Principle of Least Privilege

The principle of least privilege, "need-to-know," or default "deny all" must be applied to all user and system access. Users must be denied endpoint, network, system, and data access by default, and must only be granted the minimum permissions necessary to fulfill their job responsibilities.

4.1.4 Segregation of Duties

Segregation of duties must be implemented in all key systems. Due care must be taken to identify and prevent potential conflicts when provisioning access to users, when making changes to users' access, and when performing user access reviews. In the event that segregation of duties violations cannot be resolved, the Information Security department must be notified and mitigating controls must be designed, implemented, documented, and approved via an approved exception process.

4.1.5 Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)
The University should ensure that only authorized users have access to information systems. Access to networks, systems, and data should be role- or attribute-based where possible to ensure that permissions are assigned to end users in a consistent and uniform fashion based upon the users' job functions and authoritative system of record attributes. The University is less vulnerable to information security attacks if permissions are granted to privileged users.

4.1.6 Portable Storage, Mobile Devices, and Mobile Computing Platforms
The University must limit the use of portable storage and mobile devices and at minimum, encrypt all High-Risk data on portable storage devices, mobile devices, and mobile computing platforms. Access controls must adhere to the **Media and Protection Standard.**

4.1.7 Network and System Interconnectivity
Networks and/or systems must only allow approved connections between systems and must follow the requirements of established procedures.

4.1.9 Access Control for Physical Facilities
Physical access must be managed in accordance with the requirements specified in the **Physical Protection Standard.**

4.1.10 Access Control for Public Platforms
The University should ensure that publicly accessible information must be reviewed and posted by authorized personnel. Content should be proofread to ensure that nonpublic information is not publicly accessible.

4.2 User Access Management

4.2.1 Unique User IDs and Passwords
All users must have unique user IDs and passwords for accessing endpoints, networks, systems, and/or data to establish accountability for actions performed under each user account. Shared, default or group user IDs must not be created or used. Users must be uniquely identifiable by their user IDs and must be responsible for all activity performed under their accounts. Users must not permit others to perform any activities under the context of their user IDs and must not perform any activity under the context of other users' user IDs.

Access to these accounts must be restricted using passwords or multi-factor access controls. These passwords must meet the minimum password requirements. If an account's initial password has been set on the user's behalf, a password change must be required upon the user's first successful login. Users' passwords must be unique and must not be re-used outside the University's endpoints, networks, and systems.

4.2.2 Non-Employee Accounts
All non-employee requests for access (including contractors, service providers, vendors, and third parties) must adhere to the access request and authorization requirements defined within this Standard.

Additionally, all non-employee access must be configured with a predetermined expiration date, or a default expiration date of ninety (90) days after the account's creation if the end date of the user's need is unknown.

4.2.3 Users Access Modifications and Terminations
Hiring managers and Human Resources must promptly report all significant changes in end-user duties and employment status to the Identity and Access Management team via an automated feed from the human resources management system to facilitate the modification and/or termination of users' access in a timely manner.

In the event a user is terminated, the termination must be reported via the human resources management system within twenty-four (24) hours of the user's termination, and the user's access must be effectively disabled within the following twenty-four (24) hours. In the event of emergency termination, the user access must be disabled immediately.

In the event a user changes job functions within the organization, the user's transition must be reported via an automated feed from the human resources management system within seven (7) business days of the user's transition.

4.2.4 Multi-factor Authentication
All users must supply two forms of authentication (something they know, have, or who they are) when accessing University network or systems from university owned and issued endpoints. Second forms of authentication, such as physical tokens, smart cards, certificates, etc. are to be uniquely assigned to each user, must be tracked (where applicable), and may not be shared between users. Privileged users (i.e., system administrators, super users, application owners, etc.) must have multi-factor authentication enforced when accessing university information systems.

4.2.5 User Access Reviews
Access to each system, application, or database must be reviewed at least annually by the respective business owner with the appropriate knowledge to determine whether each user's access is justified based on the user's job function. A system-generated access list must be used in the review process. The access list used in the review must contain the user's name, unique user identification (ID), and current access levels or permissions. Review documentation must be retained for at least three years.

4.2.6 Termination of Inactive Sessions
User sessions must be automatically suspended or terminated after periods of inactivity. The specific time periods must be defined based on system classification. Upon the suspension or termination of a session, a user must re-authenticate to the system to re-activate/initiate a session.

4.2.7 User Account Lockouts
User accounts must be automatically locked after ten (10) or more consecutive failed logon attempts within a defined period. Account lockouts shall last for a duration of one hour or until a system administrator has manually unlocked the account.

4.2.8 System Use / Logon Banners
Information systems must display an approved system use notification or banner before granting access to the system. These notifications/banners must disclose privacy and security notices that are consistent with applicable laws, regulations, and organizational policies. These notifications/banners shall disclose the following:

- The system's use information when appropriate
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties
- Use of the system indicates consent to monitoring and recording

The notification/banner shall remain on the logon prompt until users take explicit actions to acknowledge or consent to the notice and proceed in logging onto the information system.

University information systems, capable of displaying a notification banner, must use the approved default system use notification below OR a notification or banner which meets section 4.2.8 of this standard.

> **Default system use notification:** "These technology services, including all related equipment, network, and data systems, are provided solely for use authorized by the University of Nebraska. The use of these technology services constitutes consent to abide by the University of Nebraska's Policy for Responsible Use of University Computers and Information Systems. For more information, please see https://nebraska.edu/em16."

4.2.9 Inactive Accounts
Employee accounts within ninety (90) days or more and student accounts with one year (365 days) of inactivity must be disabled or otherwise reauthorized by the user's manager and/or the system's business owner.

4.2.10 Privacy Statement
Online services and websites must display a link to the University of Nebraska System online privacy statement.

4.3 Privileged Access Management

4.3.1 Privileged Access Management

Access to administrative or highly privileged user accounts must be limited to the minimum number of staff required to perform administrative duties. Access to administrative or highly privileged accounts must be approved in advance by the user's immediate supervisor, the Service Owner, and the Chief Information Security Officer or the Chief Information Officer.

Privileged account credentials for University systems and networks must be secured using an ITS approved privileged access management system. Any other means of managing credentials for privileged accounts must be approved in accordance with the **Policy Exception Standard**.

4.3.2 Designated Administrative Accounts in IT Systems

All privileged users must be issued two (2) accounts if they are also expected to perform non-privileged, day-to-day tasks in the given system. The user must have an account that provides privileged access, with privileged actions being logged, and another account for non-administrative, normal use. Privileged or administrative tasks must only be performed using designated administrative accounts. Such accounts must only be used for these purposes, and must not be used for non-administrative, day-to-day activities.

Passwords for privileged administrative accounts must be unique, randomly generated, 30 characters or greater, and changed annually. If a privileged administrative account password is the only authentication factor, the password must be changed every 90 days. Exceptions must be documented and approved in accordance with the **Policy Exception Standard.**

4.3.3 Administrative Access in End User Computing Environments

End users shall not possess administrative access to their assigned University endpoints unless warranted by a documented and justified business need. All exceptions must be documented, tracked, and approved in accordance with the **Policy Exception Standard**. Such users must be informed of the risks associated with administrative rights and must exercise due care when installing software.

Administrative Access in End User Computing Environments applies to users and information systems in scope with (a) federal security-related laws and regulations, (b) state and local security-related laws and regulations, and (c) contractual requirements.

4.3.4 Services Accounts for IT Systems

Service Accounts for University information systems must be authorized by the Service Owner and Information Security. Unique Service Accounts must be established for specific information systems and functions, following the Principle of Least Privilege. An inventory of Service Accounts must be maintained and include, at minimum, the specific function of the account, where it is used, and authorized individuals with access to the account password.

Service Account passwords must be unique, randomly generated, 30 characters or greater, and changed annually or upon a personnel change in the group of authorized individuals with access to the password. Plain text Service Account passwords must not be embedded or hard-coded into applications or scripts. Passwords and certificates for Service Accounts must be stored separately using secure encryption or access controls. Exceptions must be documented and approved in accordance with the **Policy Exception Standard.**

Service Account credentials must not be shared with individuals that are not authorized.

4.4 Remote System Access

4.4.1 Remote Access Mechanisms

External access to internal information system resources must be facilitated through the use of an ITS approved Virtual Private Network (VPN) connection, Virtual Desktop Infrastructure, or managed Remote Access System. Any other means of remotely accessing internal resources must be approved in accordance with the **Policy Exception Standard**.

4.4.2 Remote Access Authorizations
External access to internal information system resources utilizing the approved access mechanisms must only be granted to authorized University users.

Remote access to the environment by contractors, third-parties, vendors, or business partners must adhere to the authorization requirements defined in this Standard, must only be activated when needed, and must be immediately deactivated after use.

4.4.3 Multi-factor Authentication for Remote Access
All users must supply multiple forms of authentication (something they know, possess, or who they are) when accessing University systems remotely, or from outside the University network. Second forms of authentication, such as physical tokens, smart cards, certificates, etc. are to be uniquely assigned to each user, must be tracked (where applicable), and may not be shared between users.

4.5 Network Access

4.5.1 Network Authentication
Endpoints connecting to University network services must be authenticated prior to gaining network access. The network shall segment endpoints logically by risk, and access will be configured after evaluating the user's identity and the endpoint's security posture. Conference rooms, public computer labs, or other areas used to host guests shall not have access to internal University services without authorization by a University identity.

Endpoints incapable of 802.1x user authentication may be permitted to leverage machine authentication with the authorization of Information Security. All non-authenticated endpoints shall be considered guests, limited to the external internet and public University services.

4.5.2 Wireless Network Access and Encryption
Access to the wireless network must be regulated by credential-based authentication controls to restrict access to authorized users only. All wireless networks in use at University facilities must be protected by WPA2-Enterprise with AES encryption, WPA3-Enterprise with AES-CCM-128 encryption, or WPA2-Personal using a Multi Pre-Shared Key (MPSK). If these authentication protocols cannot be implemented, the use of the WPA2-Personal protocol, with a single Pre-Shared Key (PSK), is strictly prohibited unless approved in accordance with the **Policy Exception Standard**. In such exceptions, the wireless network PSK must be changed on an annual basis, or upon a personnel change in the group of individuals with access to the PSK.

Non-authenticated guest wireless shall be limited to the external internet and public University services.

4.5.3 Rogue Networking Equipment
The attachment of wireless routers, access points, switches, or hubs to University networks or operating network services is strictly prohibited unless approved in accordance with the **Policy Exception Standard**.

At minimum, on a quarterly basis, Information Security shall scan the network and reconcile all identified network equipment against a list of authorized equipment. Any discrepancies shall be investigated and remediated by quarantining and removing the equipment from the network.

4.6 Authentication and Authorization

4.6.1 Users Authentication
All User access to networks, information systems, and data must be authenticated through an automated access control system using unique ID and must be regulated by authentication controls to restrict access to authorized users only.

4.6.2 Authentication Obfuscation
To prevent the compromise of authentication information (such as passwords) during the authentication process, the information system must obscure the password feedback when typed into the system.

4.6.3 Replay Resistant
For all network access of privileged and non-privileged accounts, authentication sessions between the authenticating client and the application server validating the user credentials must not be vulnerable to a replay attack.

4.6.4 Identifier Management
The University must manage user and system identifiers by:

- Establishing credentials that uniquely identify each user accessing an information system
- Verifying the identity of each user at login
- Receiving authorization to issue a user identifier is received from an appropriate member of management or other organization official and in accordance with policy and procedures.
- Ensuring that the user identifier is issued to the intended party or device identifier to the intended device in accordance with policy and procedures.
- Disabling the user identifier within 24 hours when the termination is mutual. In case of non-voluntary separation, the user identifier is disabled immediately
- Reviewing the user identifier when a user is transferred
- Disabling the employee user identifier after two years of inactivity
- Disabling the student user identifier after 365 days of inactivity; and
- Prohibiting the reassignment of user identifiers for a minimum of 365 days

4.7 Passwords Requirements

4.7.1 Password-based Authentication Control
Access to networks, information systems, and data must be regulated by authentication controls to restrict access to authorized users only. All password-based authentication controls must adhere to the password requirements.

4.7.2 Null Passwords
Access to networks, information systems, and data must be regulated by authentication controls to restrict access to authorized users only. The use of null passwords must be systematically prohibited.

4.7.3 Cryptographic Protection
Passwords must be encrypted when at-rest and in-transit. Passwords must never be transmitted or stored in plain text.

4.7.4 Initial Passwords
Passwords generated on a user's behalf must be unique for each user and must be changed by the user upon their first successful login. Where possible, systems and applications must be configured to systematically require a password change upon the user's first successful login.

4.7.5 Password Complexity
All passwords must be 10 characters or greater and follow the guidance within NIST 800-63B section 5.

4.7.6 Password/Credential Change or Compromise
If an account's credentials are changed, exposed, or an account compromise is detected, all secrets for the impacted identity must be invalidated.

4.7.7 Default Information System Passwords
Vendor-supplied default passwords and encryption keys must be changed immediately upon initial configuration of an information system.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-63-3
NIST 800-162
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	03/12/2024
Approved by:	Bret Blackman	IT CIO	03/12/2024

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	02/09/2023	Added the default notification banner language to section 4.2.8
1.2	03/12/2024	Updated Sections 4.3, 4.4, 4.5, and 4.7