Policy Owner: Chief Information Officer
Responsible Office: Information Technology Services
Origination Date: August 19, 2022
Last Revised: February 11, 2026

AUTHENTICATION STANDARD

STANDARD SUMMARY

In accordance with Northern Arizona University's Access Management policy, the Chief Information Officer ("CIO"), or their designee, updates and revises, as necessary and appropriate, a set of Access Standards. These standards establish acceptable practices for accessing the types of Accounts referenced in the User Account Types standard. The standards apply to all University Community Members and to Accounts on all University-owned IT Resources. Contact the CIO, their designee, or Information Security Services ("ISS") with any inquiry or feedback regarding these standards. Capitalized terms used herein are defined in the *Information Security* policy or *Data Classification and Handling* policy. Questions regarding the *Information Security Standards* should be directed to ISS.

STANDARD

1. **Responsibilities**
    a. University Community Members must report any compromise or other unauthorized Access to any NAU Account to NAU Information Technology Services ("ITS").
    b. University Community Members must not reutilize their NAU Account information, including passwords, passphrases, or personal identification numbers ("PINs"), for Authentication to non-University affiliated systems and services, including, but not limited to, third party software applications.
    c. University Community Members are responsible for actions conducted using NAU Accounts where they are responsible for the authentication credentials, including, but not limited to, their NAU User Account or other account types as defined in the *User Account Types* standard.

2. **Authentication Mechanisms**
    a. Passwords and Passphrases
        i. Complexity
            1. Passwords and passphrases must be a minimum of 12 characters in length and no longer than 127 characters.
            2. Passwords and passphrases may have superseding requirements as defined in the *User Account Types* standard of the *Access Management* policy.
            3. Passwords and passphrases must not include individuals' personally identifiable information ("PII"), including, but not limited to name, NAU User ID, phone number, employee ID, social security number ("SSN"), or address.
            4. Passwords and passphrases must not contain academic information, including, but not limited to, semester, course, or program information, or other University data that may be used to gain Access to an NAU Account.
            5. Passwords must not be of a known compromised state or listed within a known password dictionary.
            6. Passwords may contain standard characters including: A-Z, a-z, 0-9, spaces, and ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/.
        ii. Expiration
            1. Actively used passwords and passphrases may not have a set expiration during their continued use. Upon inactive use, passwords and passphrases may be expired by NAU to protect the University and IT Resources.
            2. Passwords and passphrases that are or presumed to be compromised may be expired as determined by NAU ITS.

3. NAU ITS may temporarily suspend or permanently revoke passwords and passphrases, if necessary, to protect or maintain the integrity or security of the University's IT Resources or data.

iii. Lockout
1. Passwords and passphrases will be locked out after six consecutive incorrect authentication attempts.
2. Passwords and passphrases may be unlocked after a period of 30 minutes or upon administrative action.

b. PIN
i. Complexity
1. PINs should be a minimum of 8 alpha, numeric, or alpha-numeric characters.
2. PINs may not include repeating or sequential character sets.
3. PINs should not include PII including, but not limited to, SSN, NAU User ID, date of birth, or employee ID.

ii. Expiration
1. Actively used PINs may not have a set expiration during their continued use. Upon inactive use, PINs may be expired by NAU ITS to protect the University and IT Resources.

iii. Lockout
1. PINs may be blocked after six consecutive incorrect attempts or after exceeding limitations imposed by hardware or device manufacturers.
2. PINs may be unlocked after a period of 30 minutes or after successful authentication of another authentication method, including a password or passphrase.

c. Multi-Factor Authentication ("MFA")
i. MFA is required for all active and current University Community Members and users with Privileged Access accounts.
ii. MFA may be implemented via DUO, Microsoft Authenticator, or other hardware authentication mechanisms.
iii. MFA may be completed via the phone application or a random number generating token issued by NAU ITS, FIPS certified hardware token, or biometric authentication.
iv. Upon accessing a secure network that requires MFA, additional MFA prompts may not be required for standard resources.
v. When elevating Access beyond the bounds of a standard account, operation may require additional or alternate MFA requirements.
vi. MFA will be locked out after six consecutive incorrect authentication attempts and may be automatically unlocked after a period of 30 minutes.

d. Biometric Authentication
i. Biometric authentication may be used in addition to passwords, passphrases, or PINs after a successful authentication utilizing one of the aforementioned authentication methods.

e. Certificate Based Authentication
i. Certificates must be issued by a trusted Certificate Authority, as approved by NAU ITS, prior to being used for Authentication to University IT Resources.
ii. Certificate Based Authentication should be protected by another Authentication Method, including, but not limited to, a password, passphrase, or PIN.

f. Hardware Authentication
i. Hardware Authentication tokens may be issued by an NAU approved source to facilitate the roles or responsibilities of a University Community Member.
ii. Loss, damage, or theft of hardware authentication, including, but not limited to, a Digital JacksCard, plastic JacksCard, or YubiKey must be reported immediately to the proper issuing authority.

g. Social Authentication
i. University Community Members must be in full control and the sole user of any social media account used to Access, recover, or claim an official NAU account.
ii. University Community Members are solely responsible for the social media account(s) they use to Access University IT Resources, including account recovery, maintenance, and liability associated with misuse or loss of the Account.

iii. NAU is not responsible for helping with recovery or maintenance of any social media accounts used to Access University IT Resources.
iv. University Community Members are responsible for securing the social media account(s) they use to access any University IT Resources and ensuring that the social media accounts are not used to change, modify, or update university data without direct Authorization.
v. University Community Members are responsible for securing the social media accounts they use to access University IT Resources. Users must notify NAU ITS in the event of suspicious activity, compromised Account, or reasonable belief that unauthorized Access to University IT Resources has occurred.

3. Authentication Impersonation

Impersonation, in the context of this policy, refers to the act of assuming the identity of another University Community Members to gain Access, privileges, or assignments available to a specific University Community Members, outside those provided as part of a delegated assignment.

a. ISS or a University Community Member designated by ISS may grant specific users or groups permission to impersonate other University Community Members in non-production environments on a limited time basis for approved business needs.
b. Impersonation of users with sensitive or privileged, such as the President, CIO, or other users with elevated Access, access may only happen for limited, specific use cases with the explicit permission of the CIO, or their designee.
c. Impersonation of user Accounts may only be done using methods pre-authorized by the ISS.
d. Only Authorized Users with permission from the CIO, or their designee, may impersonate other University Community Members in any production environment on a limited time basis for approved emergency business needs.
    i. Members may not use this privilege to escalate, impersonate, and complete tasks as any supervisor, manager, or other leadership.
e. Authorized Users with permission to use impersonation are required to only use it in execution of their duties.
f. Members may not use Impersonation to Access sensitive or restricted information outside their area of responsibility.
g. Impersonation that could knowingly lead to a conflict of interest, such as impersonating family members or friends, must be avoided where possible. Members are directed to the CERT Standards and Expectations of Conduct.

4. Compromised Authentication Mechanisms

a. NAU reserves the right to require any University Community Member or University IT Resource to reset the authentication mechanisms associated with an NAU account at any time when there is reasonable suspicion of Account compromise.
b. NAU may reset University Community Members' authentication mechanisms, including, but not limited to, passwords, passphrases, PINs, or MFA if it is suspected that these credentials have become compromised.