Responsible Executive: Chief Information Officer
Responsible Office: Information Technology Services
Effective Date: August 19, 2022
Last Revised: Not Applicable

# AUTHENTICATION STANDARD

## STANDARD SUMMARY

In accordance with Northern Arizona

3. NAU ITS may temporarily suspend or permanently revoke passwords and passphrases, if necessary, to protect or maintain the integrity or security of the

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

iii. NAU is not responsible for helping with recovery or maintenance of any social media accounts used to access University IT Resour