ACCESS MANAGEMENT STANDARD – STANDARD AND PRIVILEGED ACCESS

The capitalized terms used herein are defined in the Access Management policy.

In accordance with Northern Arizona University's Access Management policy, the Chief Information Officer ("CIO") establishes, updates, and revises as necessary and appropriate, a set of Access Management Standards. This standard establishes acceptable practices for accounts with standard and privileged or elevated access as defined in this document. It applies to all University Community Members and all user accounts used to access any University owned IT Resource or network. Contact the CIO or the Identity and Access Management team with any inquiry or feedback regarding these Access Management standards.

Section I. – Standard Access

1. Digital Identities

1.1. NAU User Account

A digital identity known as a NAU User ID or NAU UID is assigned to a University Community Member~~s~~ when that individual receives an official University affiliation status. These official affiliations within the University identity management system include:

1.1.1. Applicant: an individual with a current application in the student information system.

1.1.2. Student: an individual who is enrolled and pursuing a valid academic program.

1.1.3. Employee: an individual with a current, active (non-terminated) job record in the Human Resources system of record, which includes current and future faculty, staff, and student employees.

1.1.4. Affiliate: an individual who has been sponsored by a University Community Member or has retired from the NAU system and has been granted a valid time-based affiliation.

1.1.5. Recent or Former Student: an individual who has previously attended a class at the University and has active access to student email resources.

1.2. Multiple Digital Identities

Some members of the University community may be granted multiple Digital Identities (also referred to as persona accounts) to support their role(s) at the University. These accounts must be associated with the user's primary NAU User Account and must be deprovisioned upon the University Community Member no longer holding an active affiliation or upon a role change that no longer authorizes the utilization of the provisioned digital identity.

2. Ownership and Responsibilities

2.1. Account Management

2.1.1. University Community Members must not share their NAU User Account password, passphrase, PIN, or other authentication credentials with any other person.

2.1.2. Supervisors, administrators, or other University Community Members must not request or require anyone to share authentication information for NAU User Accounts.

2.1.3. University Community Members must report any compromise or other unauthorized access to any NAU User Account to NAU ITS.

2.1.4. University Community Members must not reutilize their NAU User Account information including their NAU User ID and password for authentication to non-university affiliated systems and services.

2.2. Access Management

2.2.1. Supervisors and service managers are responsible for maintaining up-to-date and accurate group and access management controls for access to University IT Resources.

2.2.2. It is the responsibility of each individual University Community Member to report access that is not associated with their current role, position or affiliation at the University to the appropriate Data Steward, service manager, or the IAM team. The utilization of access that is not expressly granted to that individual's current role at the University is prohibited.

2.2.3. Student Employee Supervisors are responsible for maintaining the separation of duties for their student employees' academic access and employee access.

3. Least Privilege

3.1. University Community Members must employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with the data classification policy.

3.2. Access rights must be configured to provide user privileges as low as possible, while still maintaining operational functionality of the University community.

3.2.1. Standard, day-to-day user access for performing general University business functions should be performed with the user's NAU User ID account, which has been provisioned based on the user's affiliation and areas of responsibilities.

3.2.2. When administrative privileges are required, the utilization of Privileged Access accounts should be utilized.

3.3. Separation of Access is a concept used to describe the breakdown of functions that an individual can perform prior to access elevation. The objective is to separate access rights for administrative functions, away from standard access accounts.

3.3.1. Privileged Access should be maintained on, and performed with, a separate account with separate credentials.

3.3.2. Separation of Access may involve the utilization of persona accounts, Student Employee access group, or a Service Account as described in this standard.

3.3.3. Standard functions should only be completed with a non-administrative or non-Privileged Access account.

4. Auditing and Review

4.1. The University will perform periodic reviews of access rights associated with University Community Members.

4.2. Supervisors, Services Owners, and Resource Managers are expected to review access controls to IT Resources on at least a yearly basis.

4.3. The Information Security team will run periodic reviews to maintain the highest level of compliance and security without impeding business operations.

5. Violations and Enforcement: The CIO, after consulting with General Counsel, may temporarily suspend or permanently revoke an individual's access to the University's IT Resources if necessary to protect or maintain the integrity or security of the University's IT systems or data – in such cases notice to the affected user will be provided. Enforcement may include removal of systems from the NAU network, or removal of access privileges to NAU IT Resources, removal of Internet Connectivity, or removal of access to the NAU User Account.

Section II. – Privileged Access

1. Definition and Description

1.1. Privileged Access, often referred to as "administrator," "admin," "root," or "service" accounts or access exist in all operating systems, databases, and applications. Privileged Access is commonly used for running specific services or processes that typically have elevated privileges that allow for modifications to the operation of an IT Resource, and full or elevated access to files, logs, and other user account privilege levels.

1.2. Due to the nature of the high level of access, accounts associated with these rights are targeted by attackers seeking to compromise and use them for unauthorized access. The compromise of a Privileged Access account poses significant risk and harm to the University, including data loss, creation of attacker-controlled accounts, and continued control of IT Resources.

2. Issuance and Management

2.1. A system administrator or designee must approve the granting of administrative or Privileged Access to systems or applications which they administer and for which they are responsible.

2.2. Administrator level, or Privileged Access may be associated to a single individual, service, group, or team of individuals, and should remain active only while there is an identified business need for these access rights.

2.3. Administrative access and privileged accounts should be reviewed periodically by the appropriate System Administrator, Data Steward, group owner, supervisor, or the IAM team. This review is required for systems where Sensitive or Highly Sensitive Data resides, is transmitted, or processed.

2.4. When a user with administrative access separates from the University, a system administrator or designee must revoke that individual's administrative or Privileged Access to University IT Resources.

3. Responsibilities and Usage

3.1. All Privileged Access usage must be logged and monitored for anomalous activity. Anomalous activity associated with Privileged Access should be automatically alerted with notifications to the Information Security Services team and/or the IAM team.

3.2. Privileged Access must not be used for day-to-day operations or non-security functions that can be accomplished by a non-Privileged or elevated account including, but not limited to:

- Browsing the web
- Email, instant messaging, or other electronic communications
- Opening of attachments

3.3. Privileged Access shall not be used for purposes beyond facilitating operations of the intended IT Resource and may be used to perform job duties including, but not limited to:

- Installing, upgrading, or troubleshooting system or application software
- Relocating an individual's files

- Performing repairs necessary to return an IT Resource to normal operations
- Running security programs

- Managing system backups
- Monitoring and fine-tuning an IT Resource to ensure continuity of operations, reliability, and security

3.4. Privileged or elevated access may be used to grant, deny, or change access or privileges to another individual for authorized account management actions. Examples include, but are not limited to:

- Disabling or removing an account suspected of misuse or attempting to compromise privileged accounts, such as root or administrator
- Disconnecting an IT Resource from the network when suspected compromise or security incident is reported
- Accessing files for law enforcement authorities or other third parties with a valid subpoena