Policy Owner: Chief Information Officer
Responsible Office: Information Technology Services
Origination Date: April 7, 2021
Last Revised: February 11, 2026

ACCESS MANAGEMENT

POLICY SUMMARY

This policy establishes a critical component of Northern Arizona University's strategic Identity and Access Management ("IAM") Program. It guides actions related to University Information and the Information Technology ("IT") Resources on which access to and the safeguarding of these resources depends. All University Community Members share the collective responsibility to protect access to University Information and IT Resources from harm through careful adherence to these requirements, which are designed to support the information-sharing needs of an academic culture.

REASON FOR THIS POLICY

University Information is a valuable asset that requires appropriate protection from unauthorized use, modification, loss, or disclosure in a manner consistent with industry best practices, applicable laws, and contractual obligations. Unauthorized use or disclosure of University Information could cause harm to the University or University Community Members. Clear policies and standards regarding access to University IT Resources contribute to mitigating these risks.

ENTITIES AFFECTED BY THIS POLICY

- All units that access or authorize access to the University's IT Resources or services
- Information Security Committee
- Identity and Access Management Team

WHO SHOULD KNOW THIS POLICY

- All employees who access or authorize access to the University's IT Resources or services
- Chief Information Officer ("CIO")
- Data Stewards
- Director, Information Security Services
- System Administrators and Technicians

DEFINITIONS

Access: the means or ability and permission to connect to, view, alter, obtain or distribute IT Resources.

Access Management: the process of identifying, tracking, controlling and managing authorized or specified users' permissions or access to a system, application or any IT instance or resource.

Account: a defined username with an associated Authentication Method that provides access to an IT Resource as the specified username.

Affiliate: a person who has truthfully identified themselves and their purposes or activities that further the University's mission who has an Affiliation of the type 'Affiliate'. Each Affiliate is associated with an Affiliation

Category and Affiliate Type. Affiliates are granted a default set of IT services and privileges based on their Affiliation Category.

Affiliation: a formal designation of an association between the University and certain persons, person categories, groups, or organizations that the University officially recognizes for purposes of administering IT services and privileges. Affiliations are usually, but not always, described in a written instrument that establishes certain entitlements. The University organizes its various Affiliations into Affiliation Categories.

Authentication: the means of verifying the authenticity of a Digital Identity assigned to an individual, service or device.

Authentication Methods: the technical process used to determine the validity or legitimacy of a Digital Identity, updated periodically to reflect best practices in security management. Security methods are approved by the CIO, or their designee, and documented as institutional IT procedures.

Authorization: a set of rules that determines what an authenticated Digital Identity has access to, or what actions it is approved to perform.

Data Steward: an official charged with controlling access to and properly curating University Information or data.

Digital Identity: a set of attributes stored as electronic data that represent or describe a person, device, or service. These attributes may include, but are not limited to, a name, an electronic mail address, login credentials, or similar identifying information that when taken together, unmistakably describe and identify the person, device, or service.

Information Security Standard: official criteria that establish the minimum requirements for administering, managing, protecting, or securing a particular aspect, function, or element of the University's IT Resources.

Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University, used to conduct University business, or connected to the University's IT networking or communication systems regardless of ownership, location, or access method. These resources are referred to herein as "IT Resources."

Privileged Access: An access right, role, or privilege assigned to an account elevating permission to perform operations in lieu of, or in tangent to, an administrator account.

Resource Manager: A designated individual or group responsible for access and management to an application, service, group, or other IT Resource.

Service Owner: A designated individual or group responsible for the management, maintenance, and integrity of an IT Resource.

System Administrators: University employees responsible for configuring, administering and maintaining University IT Resources for use by Authorized Users for authorized purposes.

Technicians: University employees who configure, maintain, or repair University-owned IT Resources

Unit: A Northern Arizona University campus, center, college, department, division, research facility, extended program or other official University organizational unit, its divisions, programs, senates, or associations[.]

University Community Members: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

University Information: all written or verbal data or information that the University or its employees, students, or designated affiliates or agents collect, possess, or have access to regardless of the medium on which it is stored or its format.

POLICY

A. Applicability

This policy, and its incorporated Access Management Standards, apply to all University Community Members and other users of University Information, wherever located, including all third-party individuals or entities granted access to University Information. Additionally, this policy applies to all University IT Resources, wherever located, all applications or data contained on those devices or systems, and all other devices, including privately owned devices, that connect to the University's information networks or data storage systems.

B. Information Security Services

At the direction of the CIO, their designee, and the Director of Information Security Services(ISS) administers the University's comprehensive Identity and Access Management (IAM) Program to help maintain the availability, confidentiality, and integrity of University Information. ISS provides IAM services, including password management, Authentication and Authorization systems, user lifecycle management, privileged Access management, incident response, guidance for complying with IAM controls, oversight of identity and access management activities, and other related services that comprise the University's IAM Program.

C. Access Management Standards

The CIO, or their designee, in collaboration with the Director of Information Security Services and the Information Security Committee, establishes and revises, as necessary or appropriate, the comprehensive set of Access Management Standards listed below. All University Units must meet the minimum applicable requirements established in each Access Management Standard for the protection of University IT Resources. Individual Units may adopt additional Access Management Standards that exceed these minimum requirements. After careful review, the CIO, or their designee, may grant a written exemption to a particular Access Management Standard when doing so serves the best interests of the University. The CIO, or their designee, may also enforce stricter access controls on systems or users that represent elevated risk to the University. Other IAM requirements are outlined in the Access Management-related University policies cross-referenced with this policy below. The University's Access Management Standards include the following:

Authentication Standard

Standard and Privileged Access

User Account Types

D. Single Sign-On

1. At the direction of the CIO, or their Designee, all University purchased, leased, licensed, or supported applications and software are required to utilize an institutionally approved Single Sign-On (SSO) solution wherever supported by the product. Any software or service offering SSO capability must enable, procure, or collaborate with Information Security Services (ISS) to implement the SSO components prior to production use. Exceptions may only be approved by the CIO or their appointed designee, and must be reviewed and updated on a periodic basis.

E. Digital Identities

1. A Digital Identity is usually stored in a directory system that is referenced from applications. A Digital Identity is represented or thought of as an Account, but it should be noted that a single Digital Identity can have multiple Accounts across many different systems.

2. Northern Arizona University will grant access for University Community Members to IT Resources and services mainly through Digital Identities represented as Accounts. These Accounts will primarily be represented by a username known as NAU User ID ("NAU UID"). Alternative Accounts may be issued as needed to authorize access to IT Resources that do not use a NAU UID.

3. All Digital Identities must be assigned to a University Community Member or associated with a responsible party.

4. Digital Identities may be secured at the discretion of ISS upon suspicion of compromise, including observation of the Identity clicking on suspected or compromised links or interacting with known or suspected malicious entities.

5. At no time shall a group, shared Account, or other digital reference conflict with any NAU digital identity schemas or other reserved named space.

6. Levels of authorized Access will be based on University-defined attributes such as, but not limited to, type of Affiliation, employment status, academic status, or group membership. Access granted to an Account may change if a University Community Member's attributes change.

7. Authorized Access must be approved through a documented request process like the Affiliate Account Request process, Electronic Peoplesoft Administrative Security System ("ePASS") request, other automated workflow requests, supervisor approval, or automatic entitlements based on job position or Digital Identity attributes.

8. Periodic reviews of access levels, group memberships, sponsored Affiliates, and role assignments must be performed by Affiliate sponsors, employee supervisors, Data Stewards, System Administrators, Technicians, and the IAM team to ensure eligibility. Reviews and audits may be performed by the University Internal Audit team.

9. University Community Members who are no longer actively employed with NAU may be subject to a review after departure. Upon completion of this review privileges and access may be revoked.

F. Duty to Report Access Violations

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 explicitly granted to that individual's current role at the University is expressly prohibited.

RESPONSIBILITIES

Chief Information Officer: in collaboration with the Director of Information Security Services, update as necessary and appropriate and enforce the University's *Access Management Standards*.

Data Stewards: perform periodic reviews of access levels, group memberships, sponsored affiliates, and role assignments to ensure eligibility.

Director, Information Security Services: reporting to the CIO, or their designee, is responsible for working with the roles identified herein to develop and implement security policies, procedures, protocols, and standards in support of this policy and the Information Security Program; is responsible for working with individuals, departments, and administrators to implement and enforce this policy and serves as chair of the Information Security Committee.

Information Security Services: review and enforce access policies, standards, business rules and systems that manage and grant access to IT Resources; perform periodic reviews of access control systems to ensure existing granted accesses are still appropriate.

System Administrators and Technicians: ensure the effective implementation of this policy; maintain the privacy and confidentiality of sensitive information seen or obtained in the normal course of their work; report suspected or actual violations of the University IT policies to the appropriate University authority; perform periodic reviews of Access levels, group memberships, sponsored Affiliates, and role assignments to ensure eligibility.

University Community Members: familiarize themselves to and implement, within their respective areas of responsibility of jurisdiction, these policies and standards to protect University IT Resources.

PROCEDURES

Affiliate Account Request

Electronic Peoplesoft Administrative Security System (EPASS)

RELATED INFORMATION

Forms or Tools

Standard and Privileged Access

User Account Types

Cross-References

Affiliate Management

Appropriate Use of Information Technology Resources

Authentication Standard

Information Security

Standard and Privileged Access

User Account Types

Sources

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

APPENDIX

None.