Responsible Executive: Chief Information Officer
Responsible Office: Affiliate Management Team,
Information Technology Services
Effective Date: December 3, 2012
Last Revised: August 19, 2022

Affiliate Management

Policy Summary

This policy sets forth the organizational structure used by Information Technology Services to administer the provision of information technology (“IT”) services to certain categories of users who interact or maintain a recognized relationship with Northern Arizona University in support of its educational and community missions. This policy also sets forth the University’s procedures for establishing IT-related status of Affiliate.

Reason For This Policy

Formalizing rules for the granting of IT services or privileges supports the efficient administration of the University’s IT resources while helping to mitigate institutional risk.

Entities Affected By This Policy

- Affiliate Management Office
- All entities who have the status of Affiliate
- All entities who seek the status of Affiliate
- Identity and Access Management Team
- Information Security Committee

Who Should Know This Policy

- All persons with Affiliate status
- All persons seeking Affiliate status
- Chief Information Officer (“CIO”)
- Director, Information Security Services
- External agents granted access to University Information
- University officials who wish to sponsor an Affiliate

Definitions

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.

Affiliate Sponsor: a University official of appropriate rank that presents a candidate for Affiliate status and advocates on the candidate’s behalf for the granting of certain IT services and privileges.

Affiliate Types: the Affiliations that have been established and are recognized by the University, as listed in the *Table of Affiliate Types*. Each Affiliate Type is associated with a parent Affiliation Category. Each Affiliate belongs to an Affiliate Type and associated 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.

Affiliation Category: classes of Affiliates that are granted pre-determined or default sets of IT services and privileges. The University's Affiliation Categories apply to all Affiliate Types and are described in the *Affiliation Category List*.

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

POLICY

A. Applicability

This policy applies 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 where the University considers granting IT services or privileges to any person, group, or category of persons or groups, whether internal or external, and wherever located. Use of the University's IT Resources is a privilege granted to Authorized Users, including all Affiliates; as such, the provisioning of an Affiliate account itself is a privilege granted to users in furtherance of educational opportunities or professional duties and responsibilities. The CIO 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.

B. Affiliations

Affiliations represent the relationship between a user and the University as is determined by their role within the University, including academic, administrative and third party relationships. For example, core affiliations as related to academic or administrative affiliations include: student, faculty, and staff, and the variations thereof, whereas, third party affiliations include: affiliate, with an additional affiliate category as defined in the *Affiliation Category List*.

C. Affiliate Program Administration

1. The CIO, acting through the Affiliate Management Office and supported by the NAU IT and Data Governance structure, is responsible for administering the University's Affiliate program in accordance with this policy and all other applicable requirements.

2. The default IT services or privileges granted to new Affiliation Categories will be specified in writing and approved in advance by the CIO in the manner set forth in the *How to Request a New Affiliate and the How to Request a New Affiliation Type* procedures that accompany this policy. The extension of IT services or privileges must comply with all applicable legal, policy, and contractual requirements, including software use licenses.

3. The CIO will create, in accordance with the NAU IT and Data Governance structures, appropriate review and recommended procedures concerning new Affiliate Type requests.

D. Affiliate Duties and Acknowledgements

In the same manner as its students and employees, the University's external Affiliates are required to comply with all applicable legal and policy requirements. In particular, all Affiliates are required to read and understand the *Appropriate Use of Information Technology Resources*, *Information Security*, *Data Classification and Handling*, and the *Information Security Awareness Training* policies. Acceptance of Affiliate status constitutes acknowledgement by the person granted such status that they have read, understood, and agree to abide by these and all University Policies, including the requirement to complete the University's online information security awareness training program.

E. Sponsorship

1. University officials, including academic chairs, department directors, or positions of equivalent or higher rank may sponsor a new Affiliate account when doing so is consistent with or would promote the University's mission or a related public purpose, as set forth below:

   a. The President and Vice Presidents only may approve unique or longer-term Affiliate relationships or Affiliation Types that require especially significant resources to establish or maintain. When such approvals involve external entities, a compelling University mission-related justification should be present.

   b. Deans, Department Chairs and Department Directors (or equivalent officials) may request reasonable Affiliation Types involving outside agencies or groups of individuals that are deemed beneficial to the University in support of student or departmental goals. Examples of these Affiliation Types include, but are not limited to, the Library 2+2 arrangements with Community Colleges, The College of Education Gear UP grant, and contract employees.

2. Where the extension of the University's IT services or privileges to new Affiliates or supplemental Affiliation Type would entail substantially new or additional costs, the Affiliate Sponsor will be responsible for identifying the source of funds necessary to accommodate the additional services.

3. When considering granting new Affiliate status or creating additional Affiliation Types, the security of the University's IT resources must be a primary concern. Extending IT services or privileges beyond the student and employee population entails greater risk that the Affiliate Sponsor must justify.

4. When there is a change in an Affiliate's status or point of contact, the Affiliate Sponsor or their department is responsible for notifying the Affiliate Management Team within a reasonable amount of time based on the Affiliate's level of access. The Affiliate Sponsor is also responsible for responding to any related security or usage concerns and for reviewing the individual Affiliate accounts they sponsor at expiration.

F. Compliance and Enforcement

When necessary to protect the integrity or security of its IT Resources or information systems and the University Information they contain, the University may suspend access to its networks or devices and may examine any user account. At the discretion of the CIO, enforcement of this and related IT policies may include the removal of devices or systems from the University's information networks until compliance with applicable requirements is achieved. Violations by a University Community Member of the duty and responsibility to protect the University's data, IT Resources, and information systems in accordance with applicable policies, standards, or requirements may also result in denial of access to University Information and/or University IT Resources. Further, such violations may result in the temporary or permanent revocation of access privileges and possible civil liability or criminal prosecution. In cases where full compliance with the requirements of this policy may not be immediately achievable, the unit's leadership must consult with Information Security Services to develop a plan for achieving compliance as soon as possible.

RESPONSIBILITIES

Affiliate Management Office: review all Affiliate requests to determine validity and to ensure all required information is provided; execute all Affiliate requests, including, but not limited to, Affiliate renewals and inactivations; ensure all Affiliate accounts receive the appropriate security privileges based on the Affiliation Category associated with the Affiliate's account; review annually the list of Affiliate Types to determine which Affiliate Types can be inactivated or updated.

Affiliate Sponsors: sponsor a new Affiliate account by submitting or approving the submission of an Affiliate request form, approve or deny an extension for an Affiliate request, notify the Affiliate Management Office when contact information for an Affiliate or a sponsor changes, and assist in the regular review of Affiliate access levels.

Chief Information Officer: in collaboration with the Affiliate Management Office and supported by the Information Security Committee and the Identity Governance Committee, update as necessary and appropriate and enforce the Affiliate Management program.

Identity and Access Management Team: 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; provide oversight of the Affiliate Management program in coordination with the Identity Governance Committee.

Identity Governance Committee: provide oversight of the Identity and Access Management and Affiliate Management programs as set forth in its charter and serve as part of the University's IT and Data Governance structure as a part of the Information Security Committee. It is comprised of members representative of the University community.

Information Security Committee: provide oversight of the Information Security Program as set forth in its charter and serve as part of the University's IT and Data Governance structure. It is comprised of members representative of the University community.

PROCEDURES

Requesting a New Affiliate

Requesting a New Affiliation Type

RELATED INFORMATION

Forms or Tools

Information Security Training Modules

Table of Affiliation Categories

Table of Affiliate Types

Cross-References

Appropriate Use of Information Technology Resources

Information Security

Data Classification and Handling

Information Security Awareness Training

Sources

There are no external sources associated with this policy.

APPENDIX*

Family Educational Rights and Private Act Information and Training Materials

Information Security at NAU

Service Access After Leaving NAU

*Disclaimer: all documents, links, or other materials included in this policy's appendix are provided solely for the user's convenience and are not part of official University policy.