Responsible Executive: Chief Information Officer
Responsible Office: Information Technology Services
Effective Date: June 1, 2006
Last Revised: August 19, 2022

# APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES

## POLICY SUMMARY

Use of Northern Arizona University's information technology or "IT" resources ("IT Resources") must occur within the parameters defined by this policy and its accompanying standards of appropriate use. These IT Resources, which include computers, servers, networks, electronic mail and telephonic services, data and data storage systems, and mobile devices, may only be used for the advancement of the University's mission. All such use must comply with all applicable federal and state laws and regulations, Arizona Board of Regents and University policies, and the University's IT contracting and licensing agreements.

## REASON FOR THIS POLICY

Clear standards for the appropriate use of IT Resources promote institutional efficiency and effectiveness, enhance individual accountability for ethical and lawful use and help mitigate risk.

## ENTITIES AFFECTED BY THIS POLICY

- All units of the University community

## WHO SHOULD KNOW THIS POLICY

- All users of University IT Resources including faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, collaborators, volunteers, or members of the general public

## DEFINITIONS

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

**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 Chief Information Officer ("CIO") and documented as institutional IT procedures.

**Authorized Use**: utilization of the University's IT Resources by an Authorized User in a manner consistent with, or in furtherance of, the University's mission, as well as all applicable legal and policy mandates, standards, protocols, or other guidance and the University's IT-related contracting and licensing agreements.

**Authorized User**: a person who has truthfully identified themselves and their purposes and to whom the University has granted access credentials to permit their Authorized Use of the University's IT Resources, or a person accessing the University's public information services through a network connection open to the general public, for legitimate activity or purposes that further the University's mission.

**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 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."

**Sensitive Information**: all information that should remain private or confidential as designated by the University or as required by law, including, but not limited to, educational and student conduct records, social security numbers, credit card or banking information, regulated research data, and health care provider records. Sensitive Information includes, but is not limited to, Level 3 – Sensitive Data and Level 4 – Highly Sensitive Data as defined in the University's *Data Handling and Classification* policy.

**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.

## POLICY

A. Principles

The following six principles guide the appropriate, ethical and legal use of the University's IT Resources. The IT Resource appropriate use standards that accompany, and are a part of, this policy are organized according to these six principles.

1. Use only the IT Resources you are authorized to use
2. Only use the University's IT Resources for authorized purposes
3. Abide by all applicable laws, regulations, policies and contractual and licensing agreements
4. Take reasonable care to protect the integrity of the University's IT Resources
5. Respect the privacy and personal rights of others
6. Do no harm

B. Standards of Appropriate Use

The CIO will establish, revise, update, and republish, as needed, the University's Standards for the Appropriate Use of Information Technology Resources. These standards, which define appropriate and acceptable use of the University's IT Resources for all users, are designed to protect these resources and the University while promoting compliance with all applicable IT-related laws, regulations, policies, and contracts and licensing agreements. University IT Resource Authorized Users must affirm their knowledge of this policy and its associated standards of appropriate use at the beginning of their professional relationship with the University and periodically thereafter, as determined by the CIO.

C. Access Credentials

Each NAU Authorized User is responsible for using and maintaining their Digital Identity (as consistent with the requirements in the *Access Management* policy) in a safe and appropriate manner that protects the security of the University's IT Resources. Each NAU Authorized User is charged with protecting the integrity of their access credentials from loss or unauthorized use. The careless or intentional misuse of University access credentials is a serious violation of this policy that may result, as with other violations of applicable IT-related law or policy, in disciplinary sanctions up to and including termination of employment or, in cases of student misconduct, expulsion from the University.

D. Rights and Responsibilities

1. The University is committed to open discourse, the free expression of viewpoints and beliefs, and academic inquiry without unwarranted institutional intrusion. These core values must, at times, be balanced against or tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, and the stewardship of data, information, and State of Arizona resources.

2. Use of the University's IT Resources is a privilege granted to Authorized Users in furtherance of their educational opportunities or professional duties and responsibilities. The CIO, Human Resources, or the Office of 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. NAU Authorized Users must fully cooperate with any investigation of abuse or misuse of the University's IT Resources.

3. The University may be compelled to disclose an Authorized User's electronic records in response to various legal mandates, including, without limitation, search warrants, court orders, subpoenas, discovery rights related to litigation, and public records requests. The University reserves the right to monitor and inspect usage records or data—including Account activity, content, and devices—as necessary to fulfill its legal obligations or to effectively administer its IT Resources. The University may disclose the results of such monitoring or inspections to appropriate authorities in furtherance of meeting its administrative or legal obligations and may use such information in disciplinary proceedings.

4. When necessary to protect from an imminent threat to other Authorized Users or the University's IT infrastructure, or to prevent or respond to a violation of law or policy, the University may, without notice, take actions necessary to manage the threat and to preserve access to or the security of data. Such actions may include, but are not limited to, changing passwords, rescinding access rights, requiring multi-factor authentication, disabling or impounding computers, or disconnecting specific devices or segments of the University's networks. System Administrators will restore connectivity and functionality as soon as practicable after potential threats or legal or policy violations are effectively addressed or mitigated.

E. Partner and Affiliate Appropriate Use Requirements

Partners, affiliates, or other University collaborators may provide access to non-University IT resources or services governed by third-party appropriate use policies, statements, or standards. Authorized Users shall comply with these requirements, unless doing so would violate applicable law or University policy.

F. System Administrators and Technicians

System Administrators and Technicians are granted significant privileges and trust. Accordingly, they must use their IT Resources access authorizations appropriately and only for the intended purposes. As such, these employees bear the crucial responsibility of protecting the security, confidentiality, integrity, and availability of the University IT Resources entrusted to their care and supervision. At a minimum, System Administrators and Technicians shall:

- Respect and ensure the privacy rights of all Authorized Users to the maximum extent allowed by law and policy and strictly maintain the confidentiality of all Sensitive Information gained in the course of carrying out their professional duties, unless disclosure of such information is required by law or policy or is necessary to maintain the integrity and security of the University's IT Resources; and

- Report any potential, apparent, or perceived violation of law or policy of which they become aware to the appropriate supervisor or University office or department—such as the Northern Arizona University Police Department, the University Auditor, environmental safety officials, the Office of General Counsel, the Director of Information Security Services, the Associate VP of Information Technology Services (AVP), or the CIO—and cooperate, as necessary and appropriate, with all such authorized officials conducting legitimate investigations of security threats or wrongdoing.

G. Compliance

The University reserves the right to suspend network access and examine any Account pending review by University officials. Violators of the University's IT Resource appropriate use standards are subject to disciplinary action up to and including termination or expulsion. Misuse of IT Resources may result in the permanent revocation of access privileges and civil liability or criminal prosecution. Student misconduct will be reported to the appropriate instructor, chair, or dean and/or to the Office of the Dean of Students for potential

disciplinary action under the *Student Code of Conduct*. Employee violations will be reported to the appropriate supervisor.

H. Indemnification

Except for employees acting within the course and scope of their NAU employment, by virtue of using the University's IT Resources, Authorized Users agree to indemnify, defend, save and hold harmless the State of Arizona, its departments, agencies, boards, commissions, universities, and its and their officials, agents, and employees for, from, and against any and all claims, actions, liabilities, damages, losses, or expenses (including court costs, attorneys' fees, and costs of claim processing, investigation and litigation) for bodily injury or personal injury (including death), or loss or damage to tangible or intangible property to the extent caused, or alleged to be caused, by i) the Authorized User's negligence, acts or omissions; ii) a breach of this or other applicable policy, including this policy's accompanying *Standards for the Appropriate Use of Information Technology Resources*; or iii) a failure to comply with applicable law.

## RESPONSIBILITIES

**Authorized Users**: maintain the integrity and security of their Account; use all of the University's IT Resources in full compliance with all applicable law, regulation, policy, and contracts and licensing agreements; report suspected misuse of University IT Resources to the appropriate University officials.

**Chief Information Officer**: update and republish as necessary and appropriate the University's standards of appropriate use of the University's IT Resources.

**System Administrators and Technicians**: maintain the privacy and confidentiality of Sensitive Information seen or obtained in the normal course of their work, and report suspected violations of the University's IT Resource policies or standards to the appropriate University officials.

## PROCEDURES

There are no procedures associated with this policy.

## RELATED INFORMATION

### Forms or Tools

There are no forms or tools associated with this policy.

### Cross-References

Standards for the Appropriate Use of Information Technology Resources

Human Resources Policy 5.10 Regarding Lobbying and Political Activity

### Sources

Arizona Board of Regents Policy 6-905

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

## APPENDIX

None.