Responsible Executive: Chief Information Officer
Responsible Office: Information Security Services
Effective Date: June 21, 2005
Last Revised: August 19, 2022

INFORMATION SECURITY

POLICY SUMMARY

This policy establishes the comprehensive security framework Northern Arizona University uses to protect its University Information and information technology ("IT") systems on which access to and the safeguarding of these resources depends. All University Community Members share the collective responsibility to help protect 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. Failure to comply with these standards and requirements may result in denial of access to University Information and/or IT Resources, disciplinary action up to and including expulsion or termination of employment, and civil and criminal liability.

REASON FOR THIS POLICY

The University's information and IT Resources are valuable assets that require 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 or the unavailability of University Information and IT Resources could cause harm to the University or members of the University community. Clear information security policies and standards contribute to mitigating these risks.

ENTITIES AFFECTED BY THIS POLICY

- All units that interact with University Information or IT resources or systems
- Contracts, Purchasing, and Risk Management
- External entities granted access to University Information
- Information Security Committee
- Information Security Services

WHO SHOULD KNOW THIS POLICY

- All University Community Members
- Chief Information Officer ("CIO")
- Director, Information Security Services
- External agents granted access to University Information acting for or on behalf of the University

DEFINITIONS

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."

Information Security: the protection of information systems and resources from unauthorized access, modification, disclosure, destruction, or loss. The three pillars of Information Security are *availability*, *confidentiality*, and *integrity*. *Availability* means that information is accessible when needed. *Confidentiality* limits information access to authorized users. *Integrity* protects information against unauthorized modification.

Information Security Liaisons: individuals who serve as the primary point of contact between Information Security Services and their respective business units to implement effective Information Security practices.

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

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.

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

POLICY

A. Applicability

This policy, and its incorporated Information Security 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 Program

In collaboration with the Director of Information Security Services and the Information Security Committee, the CIO oversees and directs a comprehensive Information Security Program to protect and preserve the availability, confidentiality, and integrity of University Information. The program shall support the University's compliance with all applicable statutory, regulatory, policy, and contractual guidance or requirements, and shall be shaped according to industry best practices. University administrators, including its senior executive leaders, deans, department chairs, principal investigators, and program or activity directors or managers, are each responsible for ensuring the effective implementation of, compliance with, and enforcement of the Information Security Program. These administrators shall be represented by and will work through the Information Security Liaison for their respective areas to develop and implement prudent Information Security practices, measures, and minimum requirements appropriate for each University area, unit, or activity.

C. Information Security Services

At the direction of the CIO and the Director of Information Security Services, Information Security Services administers the University's comprehensive Information Security Program to help maintain the availability, confidentiality, and integrity of University Information. Information Security Services provides services including network monitoring, vulnerability assessments and scanning, incident response, guidance for complying with Information Security controls, oversight of identity and access management activities, and other related services that comprise the University's Information Security Program.

D. Information Security Committee

The purpose of the Information Security Committee is to promote University-wide Information Security best practices. The Director of Information Security Services directs the committee's work and provides staffing support. The Committee's members, who are nominated by the University's senior executives and are representative of the University community, serve as Information Security Liaisons providing the primary point of contact between Information Security Services and their respective areas regarding Information Security matters.

E. Information Security Standards

The CIO, 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 Information Security

Standards listed below. All University units must meet the minimum applicable requirements established in each Information Security Standard for the protection of University IT Resources. Individual units may adopt additional Information Security Standards that exceed these minimum requirements. After careful review, the CIO may grant a written exemption to a particular Information Security Standard when doing so serves the best interests of the University. Other Information Security requirements are outlined in the Information Security-related University Policies cross-referenced with this policy below. The University's Information Security Standards include the following:

Auditing, Logging, and Monitoring

Data Backup and Disaster Recovery

Enterprise System Change Management

Information Technology Risk Assessment

Secure Data Center Physical Security

Software Patch Management

Vulnerability Management and Scanning

F. Training and Implementation

This policy governs all data and IT Resources owned by or under the University's control. It applies to all campuses, units, and University Community Members wherever located. The CIO, Director of Information Security Services, and the Information Security Committee are required to establish and revise the standards, policies, and controls identified herein. All units and University Community Members must adopt and follow the controls and policies set forth herein. Each of the University's senior executives is responsible for implementing Information Security Standards and all other applicable requirements within their respective areas of jurisdiction, and for providing all training that may be necessary or prudent.

G. Standard Information Security Contract Language

Information Security Services provides standard language (see item 16) to be used in all information technology contracts where third parties are granted or may receive access to University Information. Contracts, Purchasing, and Risk Management will request an Information Security Services review of product or service contracts when third-party access to University Information is requested.

H. Duty to Report

All University Community Members are obligated to immediately report any IT security threat or suspected or actual release or breach of Sensitive Data or Highly Sensitive Data as defined under the University's *Data Classification and Handling* policy. **Dial 928-523-3335 to make a report**. In collaboration with appropriate University stakeholders, Information Security Services is responsible for notifying all affected and responsible parties. The CIO will assemble an incident response team to investigate, preserve evidence, mitigate the situation, and analyze and report on the event. If health or safety may be a concern, the reporting party or Information Security Services shall immediately notify the Northern Arizona University Police Department and any other external entity or governmental agency as appropriate.

I. 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

Chief Information Officer: update and republish as necessary and appropriate the University's *Information Security Policy* and standards of appropriate use of the University's IT resources; appoint and supervise the Director of Information Security Services.

Contracts, Purchasing, and Risk Management: request review of product or service contracts by Information Security Services when access to University Information is involved or an exception to an Information Security Standard is requested.

Director of Information Security Services: reporting to the CIO, 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; serve as the chairperson of the Information Security Committee.

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.

University Community Members: promote the implementation of this policy within their respective areas of responsibility or jurisdiction and comply with the *Appropriate Use of Information Technology Resources* policy.

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

Access Management

Appropriate Use of Information Technology

Data Classification and Data Handling

Device Configuration Management

Electronic Mail

Information Security Awareness Training

Information Technology Incident Management

Sources

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

APPENDIX*

Information Security Program

*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.