University Policy: [*Director for Policy will assign code*]
Responsible Executive: Chief Information Officer
Responsible Office: Information Security Services
Effective Date: June 21, 2005
Last Revised: July 11,2018

INFORMATION SECURITY

POLICY STATEMENT

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 explusion or termination of employment, and civil and criminal liability.

REASON FOR THIS POLICY

The University's 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 or the unavailability of University Information 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
- Information Security Committee
- Information Security Services
- External entities granted access to University Information

WHO SHOULD KNOW THIS POLICY

- All University Community Members
- Chief Information Officer
- 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 Liaison: 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 Northern Arizona University or its employees, students, or designated affiliates collect, possess, or have access to regardless of the medium on which it is stored or its format.

University Community Members: all Northern Arizona University faculty, staff (including student employees), students, alumni, affiliates, contractors, consultants, and agents 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 Chief Information Officer 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 Chief Information Officer and the Director of Information Security Services, Information Security Services implements and oversees the University's comprehensive Information Security Program to help ensure the availability, confidentiality, and integrity of University Information. The office provides Information Security 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 any 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. Its 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 Chief Information Officer, in collaboration with the Director of Information Security Services and the Information Security Committee, establishes and revises as appropriate a comprehensive set of Information Security standards. 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

Information Security Standards that exceed these minimum requirements. After careful review, the Chief Information Officer may grant a written exemption to a particular Information Security Standard when doing so serves the best interests of the University. The University's Information Security Standards include:

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

Other Information Security requirements are outlined in the Information Security-related University Policies cross-referenced with this policy below.

F. Training and Implementation

This policy governs all data and information systems and devices owned by or under the University's control. It applies to all campuses, units, and University Community Members wherever located. The Chief Information Officer, 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. Violations and Enforcement

At the discretion of the Chief Information Officer, enforcement of this policy may include the removal of devices or systems from the University's networks or information systems until compliance with applicable requirements is achieved. Violations of this policy or its associated Information Security Standards may result in denial of access to University Information and/or University IT Resources. Willful violations may result in disciplinary action up to and including expulsion or termination of employment and civil and criminal liability.

H. Standard Information Security Contract Language

Information Security Services will provide 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. Contracting, 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.

RESPONSIBILITIES

Chief Information Officer: updates and republishes as necessary and appropriate the University's *Information Security Policy* and standards of appropriate use of the University's IT resources. Appoints and supervises the Director of Information Security Services.

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

Director of Information Security Services: reporting to the Chief Information Officer, 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. The Director of Information Security Services is responsible for working with individuals, departments, and administrators to implement and enforce this policy, and serves as the chairperson of the Information Security Committee.

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

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

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