Policy Owner: Chief Information Officer
Responsible Office: Information Security Services
Origination Date: June 1, 2018
Last Revised: February 11, 2026

INFORMATION SECURITY AWARENESS TRAINING

POLICY SUMMARY

Northern Arizona University owns or controls, or acts as custodian for, a broad array of information, including Sensitive Information protected by law. To safeguard this University Information, this policy establishes information security awareness training requirements for all University employees (including student employees) and all other persons authorized to access this material.

REASON FOR THIS POLICY

All authorized users should gain a broad understanding of information security threats, risks, and best practices in order to assist the University in protecting the confidentiality, integrity, and availability of University Information and the University's Information Technology ("IT") Resources.

ENTITIES AFFECTED BY THIS POLICY

- All units that interact with University Information or IT Resources
- External entities authorized to access University Information or IT Resources
- Information Security Services

WHO SHOULD KNOW THIS POLICY

- All persons authorized to access University Information or IT Resources
- Chief Information Officer ("CIO")
- Director, Information Security Services

DEFINITIONS

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.

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."

Phishing: the fraudulent and malicious practice of sending electronic communications purporting to be from a reputable source in hopes of tricking or inducing the recipient to reveal sensitive or confidential personal information, such as passwords or credit card numbers.

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.

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. Information Security Awareness Training Program

Acting through the Director of Information Security Services, the CIO, or their designee, will establish and maintain an information security awareness training program that will include testing to assess and help ensure basic knowledge and comprehension of information security issues. To demonstrate basic competency in information security best practices, all faculty, staff, and other Authorized Users of University Information or IT Resources must complete this training as part of the onboarding process, annually thereafter, or as may be required by the CIO, or their designee. Information Security Services will:

- Develop or acquire appropriate information security training content and test materials
- Update and revise training content, test materials, and delivery methods annually to reflect current threats and emerging information security best practices
- Ensure a mechanism exists for feedback regarding the content and efficacy of the training program
- Track and record testing completion rates and other useful program statistics
- Report completion rates and follow-up with units not completing the mandatory training

B. Learning Objectives

The basic information security awareness training for all employees or agents will include:

- General information security awareness best practices
- Mobile device and wireless networking best practices
- Data confidentiality, integrity, and availability
- University IT Resource appropriate use and information security policies
- Individual employee information security roles and responsibilities
- Data classification and handling requirements, including the need to protect of Sensitive Information
- How to identify suspicious or risky activities
- Cybersecurity threat reporting requirements
- Insider threat detection and reporting
- IT security terms and definitions
- Authentication awareness and best practices

Additionally, role-based security training will be provided by subject-matter experts to employees and affiliates having unique, specific, or highly technical security responsibilities (such as roles involving financial transactions, health record processing, payment card transactions, and secure software development for web developers) as may be deemed appropriate for their roles or level of expertise. Students will have the option, but not the requirement, to complete the information security awareness training program.

C. Phishing

Employees whose accounts are found to be compromised by a successful Phishing attack may be required to retake and pass a specific Phishing security awareness training module.

Phishing simulations may be conducted up to 4 times per year or additionally at the direction of the CIO or their delegate.

D. Compliance

System access privileges may be revoked for employees or other Authorized Users (for whom training is required) who do not complete required information security awareness training within specified timelines, which shall not exceed thirty (30) days past onboarding, annually recurring, or other established training deadlines.

RESPONSIBILITIES

Chief Information Officer: ensure that appropriate and auditable information security awareness, training, and education controls are in place; has ultimate responsibility for the content of the security awareness program.

Information Security Services: determine the information security training content and enforce the training requirement with all units; annually review and update the training content as necessary or appropriate; maintain training statistics and report completion rates.

Director of Information Security Services: reporting to the Chief Information Officer, provide leadership in security awareness, training, and education, and develop and implement the University's information security awareness training program roles.

PROCEDURES

There are no procedures associated with this policy.

RELATED INFORMATION

Forms or Tools

Security Essentials Online Training Modules

Cross-References

Appropriate Use of Information Technology Resources

Data Classification and Handling

Information Security

Sources

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

APPENDIX

None.