Responsible Executive:

Sensitive Information includes, but is not limited to, Level 3 ï Sensitive Data and Level 4 ï Highly Sensitive Data as defined in the Universityôs *Data Handling and Classification* policy.

University Information: all written or verbal data or information that the University or its employees, students, and 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 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. 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.

D. Compliance

System access privileges may be revoked for employees or other A

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 Universityôs 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-

Arizona Board ofofofofof9Tf1 0 0 [illegible] Tm [illegible] rg [illegible] RG