Policy Contents

- Purpose and Summary
- Scope
- Definitions
- Policy
- Compliance and Responsibilities
- Related Information*
- Revision History*

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
January, 2020
Policy Number:
ISO-500
Responsible Unit:
Information Security Office
Phone:
(520) 621-6700
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Information Security Awareness Training Policy for the University of Arizona. This policy ensures security awareness and training controls that protect the confidentiality, integrity, and availability of the University's Information Resources.

Scope

This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of the University. All University-Related Persons with access to University Information or computers and systems operated or maintained on behalf of the University are responsible for adhering to this policy.

Definitions

CISO: The senior-level University employee with the title of Chief Information Security Officer.

Elevated Access: A level of access that is authorized to perform functions that ordinary users are not authorized to perform.

Information Owner: The individual(s) or Unit with operational authority for specified University Information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This individual or Unit is responsible for making risk tolerance decisions related to such Information on behalf of the University and is organizationally responsible for any loss associated with a realized information security risk scenario.

Information Resources: University Information and related resources, such as equipment, devices, software, and other information technology.

Information System: A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

Information System Owner: The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

ISO: The University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

Unit: A college, department, school, program, research center, business service center, or other operating Unit of the University.

University Information: Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.

University-Related Persons: University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University, and third-party contractors engaged by the University and their agents and employees.

User: Individual or group that interacts with a system or benefits from a system during its utilization.

Policy

A. All Classifications of University Information

1. ISO, on behalf of the University, must define and ensure the implementation of an information security awareness training program to increase Users’ awareness of their information security responsibilities in protecting the confidentiality, integrity, and availability of University Information Resources.
2. Employee and DCC Security Awareness Training

    a. All University employees (including student employees) and Designated Campus Colleagues (DCCs) with access to University Information Resources must complete security awareness training within the first 30 days from date of hire. Information Security Refresher Training must be completed annually, within 60 days of the anniversary of the previous instance of such training.
3. Role-Based Security Awareness Training
    a. Additional role-based security awareness training must be required for employees and DCCs whose responsibilities require Elevated Access, including access to Regulated or Confidential Information, as defined in the University's Data and Classification Handling Standard [2] (e.g., information subject to additional requirements under HIPAA, PCI-DSS, FISMA, ITAR/Export Control, NIST 800-171), and related Information Systems. Role-based training must be completed on an annual or periodic basis, as required by the relevant regulatory or contractual compliance programs.

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

ISO must initiate mechanisms for tracking compliance with this policy and must produce reports representing these measures to support University decision making.

Recourse for Noncompliance

ISO is authorized to limit network access for individuals or Units not in compliance with all information security policies and related procedures. In cases where University resources are actively threatened, the CISO should act in the best interest of the University by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the CISO is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, the University may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

Exceptions

Requests for exceptions to any information security policies may be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the CISO for review and approval pursuant to the exception procedures published by the CISO.

Frequency of Policy Review

The CISO must review information security policies and procedures annually, at minimum. This policy is subject to revision based upon findings of these reviews.

Responsibilities

University-Related Persons

All University-Related Persons are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.

Information Owners and Information System Owners

Information Owners and Information System Owners are also responsible for implementing processes and procedures designed to provide assurance of compliance with the minimum standards, as defined by ISO, and for enabling and participating in validation efforts, as appropriate.

Regulatory and Contractual Compliance Programs

Regulatory and Contractual Compliance Programs that are responsible for ensuring appropriate treatment of Regulated or Confidential Information must establish additional role-based security awareness training modules specific to their program, along with accompanying periodicity requirements.

Chief Information Security Officer

ISO must, at the direction of the CISO:

- identify solutions that enable consistency in compliance and aggregate and report on available compliance metrics;
- develop, establish, maintain, and enforce information security policy and relevant standards and processes;
- provide oversight of information security governance processes;
- educate the University community about individual and organizational information security responsibilities;
- measure and report on the effectiveness of University information security efforts; and
- delegate individual responsibilities and authorities specified in this policy or associated standards and procedures, as necessary.

Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers

All Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers must take appropriate actions to comply with information technology and security policies. These individuals have ultimate responsibility for University resources, for the support and implementation of this policy within their respective Units, and, when requested, for reporting on policy compliance to ISO. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Related Information*

- ISO Website [3]
- Information Security Policy (IS-100) [4]
- Data Classification and Handling Standard [5]
- Designated Campus Colleague Quick Reference Matrix [6]

Revision History*

Nonsubstantive revisions January 24, 2020

Replaces Interim policy of 3/19/19

Source URL:
https://policy.arizona.edu/information-technology/information-security-awareness-training-policy

Links
[1] mailto:security@arizona.edu
[2] https://security.arizona.edu/content/data-classification-and-handling-standard
[3] https://security.arizona.edu/content/policy-and-guidance
[4] http://policy.arizona.edu/information-technology/information-security-policy
[5] https://security.arizona.edu/data-classification-and-handling-standard
[6]
https://hr.arizona.edu/sites/default/files/hr/Workforce-Systems/uaccess-resources/dcc/DCC_Srvc_Matrix.pdf