Published on *Policies and Procedures* (http://policy.web.arizona.edu)

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:
May, 2019
Policy Number:
ISO-200
Responsible Unit:
Information Security Office
Phone:
(520) 621-6700
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Information Security Risk Management and Security Planning Policy for the University of Arizona. This policy manages University information security risk through the establishment of an information security risk management and security planning program.

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.

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 the owned University Information on behalf of the University and is 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 the owned Information Systems on behalf of the University and is 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.

Policy

ISO shall integrate information security and privacy assurances into University information technology and business practices using an information security risk management and security planning program.

Risk Management

Information Owners and Information System Owners shall, in coordination with ISO, integrate the following information security and privacy activities into their risk management processes:

1. **Categorize** the University Information and the Information Systems according to the level of impact from loss of confidentiality, integrity, or availability.
2. **Select** an initial set of baseline information security and privacy controls for the system and tailor the control baseline, as needed.
3. **Assess** the information security and privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the information security and privacy requirements for the system and enforcing those requirements.
4. **Authorize** the system by requiring a senior management official to determine if, based on the operation of a system or the use of common controls, the information security and privacy risk is acceptable as it pertains to organizational operations, assets, individuals, or other departments in the University.
5. **Monitor** the system and the associated information security and privacy controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting security and privacy impact analyses, and reporting the information security and privacy state of the system.

Security Planning

ISO shall develop, test, review, and maintain a comprehensive, University-wide Information Security Plan. Additionally, Information Owners and Information System Owners shall develop, test, review, and maintain, in coordination with ISO, information security plans for their Information Resources.

Each Information Security Plan shall:

- provide an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- include the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- reflect coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical);
- be approved by either the Information Owner or Information System Owner and by the office of the CISO for the University; and
- be treated as confidential.

The risk management and security planning program shall be constrained as follows:

- The information security risk management cycle must be repeated at least annually and any time changes occur in the classification, controls, environment, personnel, or operation of the covered system where said changes could impact the confidentiality, integrity, or availability of a University Information Resource.
- Information security plans shall be updated at least annually for Information Resources that store, process, or transmit University Information classified as Confidential or Regulated, as defined in the University’s Data Classification and Handling Standard, or every three years for all other Information Resources.
- Information security plans shall be updated any time changes occur in the classification, controls, environment, personnel, or operation of the covered system where said changes could impact the confidentiality, integrity, or availability of a University Information Resource.

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

ISO shall initiate mechanisms for tracking compliance with this policy and shall 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 information security policies (including this one) and related procedures. In cases where University resources are actively threatened, the CISO shall 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 information security policies (including this one) 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 shall 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 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.

Chief Information Security Officer

ISO shall, 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 shall 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 [2]

Data Classification and Handling Standard [3]

Information Security Incident Response Plan [4]

45 CFR 164.308(a)(1) [5][HIPAA Security rule: Administrative safeguards: Standard: Security management process]

16 CFR Part 314 [6] Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (''GLB Act'')

Revision History*

Replaces Interim policy of 3/19/19

Source URL:
http://policy.web.arizona.edu/information-technology/information-security-risk-management-and-security-planning-policy

Links
[1] mailto:security@arizona.edu
[2] https://security.arizona.edu/content/policy-and-guidance
[3] https://security.arizona.edu/data-classification-and-handling-standard
[4] https://confluence.arizona.edu/download/attachments/39782340/Incident%20Response%20Plan_v4.pdf?api=v2
[5] https://www.govinfo.gov/content/pkg/CFR-2009-title45-vol1/pdf/CFR-2009-title45-vol1-sec164-308.pdf

[6] https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf