Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
December, 2021
Policy Number:
ISO-100
Responsible Unit:
Information Security Office
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Information Security Program Policy for the University of Arizona. This policy provides an outline to ensure ongoing compliance with policy and regulations related to the Program and positions the University to address future changes in the information security landscape, including new or amended regulations.

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 such Information on behalf of the University and is organizationally responsible for any loss associated with a realized information security risk scenario.

Information Resource Owner: Collective term used to refer to Information Owners and Information System Owners.

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

Information Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Information System or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of information security policies, information security procedures, or acceptable use policies.

Information Security Risk Manager: An individual designated by the supervisor of a Unit (e.g., a Vice President, Dean, Director, Department Head, or Head of a center or other office) to be responsible for managing an organization's information security risks and minimizing the adverse impact of losses on the achievement of organizational objectives.

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.

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

IT Security Manager: An individual designated by the supervisor of a Unit (e.g., a Vice President, Dean, Director, Department Head, or Head of a center or other office) to serve as the primary contact between the respective Unit and the ISO for all matters relating to information security.

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

A. All Classifications of University Information

1. Taking a University-wide approach and acting on behalf of the University, the CISO must develop and maintain an Information Security Program to preserve the confidentiality, integrity, and availability of University Information Resources. At the direction of the CISO, the ISO must:
    a. define information security policies, standards, processes, and procedures designed to provide insight into, and assurance of, the security posture of the University;
    b. support the University mission through appropriate information security governance and reporting;
    c. coordinate and oversee regular risk management and security planning activities for existing and planned Information Resources;
    d. implement Information Security Incident response planning, execution, and notification procedures; and
    e. enforce information security policy through a risk-informed, compliance validation program.
2. Each Unit must protect University Information Resources by adhering to, adopting, and implementing information security policies, standards, processes, and procedures as defined and developed by the CISO. All Units must meet the minimum standards appropriate to the information security risk of the Unit, including but not limited to:
    a. identifying the Information Resource Owners for each Information Resource for which the Unit has any responsibility;
    b. designating one or more Information Security Risk Manager(s) and IT Security Manager(s) within the Unit to work in collaboration with the ISO and on behalf of Information Resource Owners;
    c. empowering and enabling the Information Owners and Information System Owner to make risk tolerance decisions and risk handling decisions that are appropriate given the information security risk to the owned Information Resources; and
    d. ensuring Information Owners, Information System Owners, Information Security Risk Managers, and IT Security Managers, designated by the Unit, fulfill their respective obligations defined by ISO policy, standards, processes, and procedures.
3. Units are encouraged to adopt standards that exceed the minimum requirements for the protection of University Information Resources.

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

The ISO must develop, test, review, maintain, and communicate a representation of the University-wide information security posture to University leadership. The ISO is authorized to initiate mechanisms to track the effective implementation of information security controls associated with this policy and to produce reports measuring individual or Unit compliance to support University decision making.

Recourse for Noncompliance

The 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 must 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 [2].

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

Chief Information Security Officer

The 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 the ISO. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Related Information*

- ISO Website [3]
- Information Resource Classification Standard [4]
- Information Security Risk Management and Security Planning Policy [5]
- Information Security Incident Reporting and Response Policy [6]

Revision History*

11/17/2023: Updated links.

11/14/2023: Updated links.

02/01/2023: Revision to Definitions Section - added new defined term "Information Owner." Non-substantive grammatical revisions.

12/2021: Revision to Tracking, Measuring and Reporting Section: ISO tracking and reporting responsibilities; new hyperlink added to Exceptions Section; classification standard and various hyperlinks updated.

01/27/2020: Non-substantive revisions.

03/19/2019: Replaces Interim policy.

Links
[1] mailto:security@arizona.edu [2] https://emailarizona.sharepoint.com/sites/ISO-Communications/ISO%20Governance%20Documentation/Forms/AllItems.aspx?id=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D100%20Information%20Security%20Program%2FISO%2D100%2DP1%2DInformation%2DSecurity%2DOffice%2DPolicy%2DException%2DRequest%2DProcedure%2Epdf&parent=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D100%20Information%20Security%20Program [3] https://security.arizona.edu/content/policy-and-guidance [4] https://emailarizona.sharepoint.com/sites/ISO-Communications/ISO%20Governance%20Documentation/Forms/AllItems.aspx?id=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D400%20Information%20Classification%20and%20Determination%2FISO%2D400%2DS1%2DInformation%2DResource%2DClassification%2DStandard%2Epdf&parent=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D400%20Information%20Classification%20and%20Determination [5] https://policy.arizona.edu/information-technology/information-security-risk-management-and-security-planning-policy%E2%80%94interim [6] https://policy.arizona.edu/information-technology/information-security-incident-reporting-and-respon

se-policy%E2%80%94interim