



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

[Home](#) > Information Security Incident Reporting and Response Policy

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-600

Responsible Unit:

Information Security Office

Phone:

(520) 621-6700

Email:

security@arizona.edu [1]

Purpose and Summary

This document establishes the Information Security Incident Reporting and Response Policy for the University of Arizona. The purpose of this policy is to define the requirements and responsibilities in reporting and responding to Information Security Incidents or events in a manner that minimizes negative impacts to the confidentiality, integrity, and availability of University Information Resources and University Information.

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 Resources: University Information and related resources, such as personnel, equipment, funds, and 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 security policies, security procedures, or acceptable use policies.

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'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

All University-Related Persons must report, to ISO, any Information Security Incident or event that has the potential to negatively impact the confidentiality, integrity, or availability of University Information or any Information System that stores, processes, or transmits University Information.

Information Security Incident reporting and its timeliness shall be determined by risk and regulatory requirements and in accordance with the procedures defined in the Information Security Incident Response Plan. Additionally, no action shall be performed that is inconsistent with the Information Security Incident Response Plan when an Information Security Incident involves Confidential or Regulated Information, as defined in the University's Data Classification and Handling Standard.

ISO shall direct Information Security Incident responses and investigations in coordination and collaboration with the affected Unit(s).

ISO shall be responsible for coordinating with appropriate University departments, such as the Office of General Counsel and University Marketing and Communications; any required external

reporting of Information Security Incidents, such as to regulators, state attorneys general, contractual counter-parties, affected data subjects, or others. All Units and University-Related Persons are required to provide ISO any assistance it requires for purposes of such coordination and reporting.

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]

Revision History*

Replaces Interim policy of 3/19/19

Source URL:

<http://policy.web.arizona.edu/information-technology/information-security-incident-reporting-and-response-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