Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
December, 2021
Policy Number:
ISO-600
Responsible Unit:
Information Security Office
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: Any irregular, adverse, or uncontrolled event that threatens the confidentiality, integrity, or availability of any University of Arizona information asset, system, network or storage media, or any violation or imminent threat of violation of any University of Arizona computer security policies, acceptable use policies, or standard security practices.

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.

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. All University-Related Persons must report, to the 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.
    a. Information Security Incident reporting and its timeliness must be determined by risk and regulatory requirements and in accordance with the procedures defined in the University Information Security Incident Response Standard [2].
    b. Unsuccessful security incidents are foreseeable and expected, are not required to be reported, but may be reported if any uncertainty exists. Unsuccessful security incidents include, but is not limited to, pings on a firewall, unsuccessful attempts to log onto a system with an invalid password or user name, unsuccessful attempts to load malware, denial-of-service attacks that do not result in a server being taken off-line, and other events that do not result in actual impermissible use, disclosure, access or acquisition of

University Information Resources or a substantial risk thereof.

2. The ISO must direct Information Security Incident responses and investigations in coordination and collaboration with the affected Unit(s).
3. The ISO must 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 counterparties, affected data subjects, or others.
    a. All Units and University-Related Persons are required to provide the ISO with any assistance the ISO requires for purposes of such coordination and reporting.

B. Restricted University Information

1. No action should be performed that is inconsistent with the University Information Security Incident Response Standard [2] when an Information Security Incident involves Restricted Information, as defined in the University Information Resource Classification Standard [3].

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 [4].

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 [5]
- University Information Resource Classification Standard [3]
- University Information Security Incident Response Standard [2]

Revision History*

11/17/2023: Updated links.

02/1/2023: Grammatical revisions throughout and in the Policy Section: paragraph A.1.a. - revised link name to include "University" and remove "Plan" and paragraph B.1. - added new link to the University Information Security Incident Response Standard.

12/2021: Information Security Incident defined term revised; substantive changes to Policy Section A - All Classifications of University Information; Policy Section B substantive changes; revision to Tracking, Measuring and Reporting Section: ISO tracking and reporting responsibilities; new hyperlink added to Exceptions Section; Related Information Section updated; various hyperlinks updated.

01/24/2020: Non-substantive revisions.

03/19/2019: Replaces Interim policy.

Source
URL:https://policy.arizona.edu/information-technology/information-security-incident-reporting-and-response-policy

Links
[1] mailto:security@arizona.edu [2] https://emailarizona.sharepoint.com/:b:/r/sites/ISO-Communications/ISO%20Governance%20Documentation/ISO-600%20Information%20Security%20Incident%20Reporting%20and%20Response/ISO-600-S1-Information-Security-Incident-Response-Standard.pdf?csf=1&web=1&e=UeydxX [3] https://emailarizona.sharepoint.com/:b:/r/sites/ISO-Communications/ISO%20Governance%20Documentation/ISO-400%20Information%20Classification%20and%20Determination/ISO-400-S1-Information-Resource-Classification-Standard.pdf?csf=1&web=1&e=yqfRXK [4] 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 [5] https://security.arizona.edu/content/policy-and-guidance