Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
May, 2019
Policy Number:
ISO-300
Responsible Unit:
Information Security Office
Phone:
(520) 621-6700
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Identity and Access Management Policy for the University of Arizona. This policy defines information security requirements for the identity and access management processes relevant to 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 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 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: An individual or group that interacts with a system or benefits from a system during its utilization.

Policy

A. All Classifications of University Information

Information Owners and Information System Owners with responsibility for Information Resources that store, process, or transmit University Information of any classification, as defined in the University’s Data Classification and Handling Standard, must establish or adopt documented

procedures. Procedures must be appropriate to the level of information security risk to prevent unauthorized digital or physical access and meet, at a minimum, the following requirements:

- Use of unique usernames assigned to identify a specific individual.
- Usernames must not be reassigned or transferred, even when the individual originally assigned is no longer affiliated with the University.
- Use of multi-factor authentication for any access authorized to modify University Information shall be preferred, where feasible, over single-factor authentication.
- Supervision for individuals without the need to access Confidential or Regulated Information who work in or have access to areas where Confidential or Regulated Information is accessible.

B. Confidential and Regulated University Information

Information Owners and Information System Owners with responsibility 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, must establish or adopt additional documented procedures to augment those defined in Paragraph A (above). These additional procedures must meet, at a minimum, the following additional requirements:

- Workforce clearance to determine that access of an individual to Confidential or Regulated Information is appropriate, that the individual has a “need to know” based on job responsibilities, and that the results of a screening process have been reviewed.
- Each individual or role is granted access to the minimum amount of information and system resources needed to perform their job function.
- Annual review of authorization decisions.
- Periodic review, at least quarterly, of exception reporting for actual User-level or role-level access. Exception reporting must, at a minimum, report any inconsistencies between authorized access and actual access.
- Where feasible, use of role-based authorization schemes (as opposed to individual authorizations), including required use of such role-based authorization when appropriate to the level of information security risk.
- Termination procedures to remove access when employment ends and/or when the access is no longer appropriate, which require at a minimum:
    - a notification mechanism to appropriate personnel;
    - rescission of all forms of access to University Confidential and Regulated Information;
    - disabling of the User’s access to relevant Information Systems; and
    - a process to record and maintain the dates, times, and descriptions of actions taken pursuant to such termination procedures.
- Control procedures to prevent the unintended flow of Confidential or Regulated University Information into systems not approved for storing, processing, or transmitting Confidential or Regulated University Information.
- User access to relevant University Information and Information Systems is restricted pending User completion of information security awareness trainings required by ISO Policy and relevant regulations, as defined by the relevant regulatory offices.

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

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