THE UNIVERSITY OF ARIZONA

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

Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
December, 2021
Policy Number:
ISO-800
Responsible Unit:
Information Security Office
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Acceptable Use for System Administrators Policy for the University of Arizona. This policy establishes requirements and provides guidance to System Administrators for the ethical and acceptable use of their administrative access.

System Administrators manage, configure, and monitor the University Information Resources. In doing so, they are responsible for activity originating from their accounts. This policy establishes requirements for acceptable use of Elevated Access for System Administrators.

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.

Elevated Access: A level of access that is authorized to perform functions that ordinary Users are not authorized to perform.

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

System Administrator: A User with a level of access above that of a normal User, or with supervisory responsibility for Information Systems and Information Resources. Examples of System Administrators include, but are not limited to, a Database Administrator, a Network Administrator, a Central Administrator, a superuser, or any other privileged User.

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: Individual or group that interacts with a system or benefits from a system during its utilization.

Policy

A. All Classifications of University Information

1. Each Unit that is (or has an employee who is) an Information Resource Owner must have documented procedures for approving Elevated Access for System Administrators. The procedures should allow for risk-informed decisions regarding when to grant or deny such access (see Elevated Access Risk Analysis Guidelines [2] for guidance).
2. When a System Administrator's role or job responsibilities change, their Elevated Access must be evaluated and, if necessary, updated or removed according to Unit procedures.
3. Each System Administrator must:
   a. Restrict their use of accounts with Elevated Access to only official University business consistent with the System Administrator's University role, job responsibilities, and the purpose for which the access was granted. The permissible use of Information Systems for incidental personal purposes (as reflected in the Acceptable Use of Computers and Networks Policy [3]) does not extend to a System Administrator's use of this Elevated Access. System Administrators may not use their Elevated Access for any purposes outside of the scope for which such Elevated Access was granted.
   b. Never use Elevated Access to satisfy personal curiosity.
   c. Never expose or otherwise disclose information obtained through Elevated Access to unauthorized persons.
   d. Ensure that default passwords are changed using strong password methodologies, as defined in the University Password Standard [4], when an Information System is installed or implemented.
   e. Never share their own personal login credentials.
   f. Never gain or provide unauthorized access to an Information System. System Administrators must never give themselves or another User access to Information Systems that they have not been formally authorized to access.
   g. Take steps to ensure adherence to and compliance with all hardware and software license agreements entered and communicated by the University.
   h. In fulfilling the responsibilities that accompany the granting of Elevated Access, take all reasonable measures to protect the confidentiality, integrity, and availability of Information Resources.
   i. For those System Administrators responsible for secure architecture design, ensure that each individual or Unit is granted the minimum system resources and authorization that such individual or Unit needs to perform its function.

B. Restricted University Information

1. When Elevated Access is given to Information Systems that store, process, or transmit Restricted Information, as defined in the University Information Resource Classification Standard [5], the procedures must at least meet relevant minimum regulatory requirements, as established or communicated by the University office designated as responsible for enforcement of the relevant information security or privacy obligation (see Information Handling Guideline [6] for guidance).

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 [7].

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 [8]
- https://policy.arizona.edu/information-technology/acceptable-use-system-administrators-policy [9]
- Acceptable Use of Computers and Networks Policy [3]
- AWS Security Best Practices [10]
- Azure security best practices and patterns [11]
- Best Practices for Securing Active Directory [12]
- System Administrator—Security Best Practices [13]

Revision History*

11/17/2023: Updated links.

02/01/2023: Policy Section A, paragraph 1 - added new link to published guidance.

12/2021: Revisions to Policy Section A - All Classifications of University Information and Policy Section B – reference documents and hyperlinks added; revision to Tracking, Measuring and Reporting Section: ISO tracking and reporting responsibilities; several hyperlinks updated.

01/16/2020: Non-substantive revisions.

03/19/2019: Replaces Interim policy.

Source URL:https://policy.arizona.edu/information-technology/acceptable-use-system-administrators-policy

Links
[1] mailto:security@arizona.edu [2]
https://emailarizona.sharepoint.com/:b:/r/sites/ISO-Communications/ISO%20Governance%20Docume

ntation/ISO-800%20Acceptable%20Use%20for%20System%20Administrators/ISO-800-G1-Elevated-Access-Risk-Analysis-Guideline.pdf?csf=1&web=1&e=lIGGl1 [3]
https://policy.arizona.edu/information-technology/acceptable-use-computers-and-networks-policy [4]
https://emailarizona.sharepoint.com/:b:/r/sites/ISO-Communications/ISO%20Governance%20Documentation/ISO-800%20Acceptable%20Use%20for%20System%20Administrators/ISO-800-S1-Password-Standard.pdf?csf=1&web=1&e=95ZUqX [5]
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 [6]
https://emailarizona.sharepoint.com/:b:/r/sites/ISO-Communications/ISO%20Governance%20Documentation/ISO-400%20Information%20Classification%20and%20Determination/ISO-400-G2-Information-Handling-Guideline.pdf?csf=1&web=1&e=SCLWa6 [7]
https://emailarizona.sharepoint.com/:b:/r/sites/ISO-Communications/ISO%20Governance%20Documentation/ISO-100%20Information%20Security%20Program/ISO-100-P1-Information-Security-Office-Policy-Exception-Request-Procedure.pdf?csf=1&web=1&e=aWQXPv [8]
https://security.arizona.edu/content/policy-and-guidance [9]
https://policy.arizona.edu/information-technology/acceptable-use-system-administrators-policy [10]
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf [11]
https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns [12]
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory [13]
https://www.sans.org/reading-room/whitepapers/bestprac/system-administrator-security-practices-657