Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
May, 2019
Policy Number:
ISO-1100
Responsible Unit:
Information Security Office
Phone:
(520) 621-6700
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Information System Audit, Accountability, and Activity Review Policy for the University of Arizona. This policy ensures consistency in the creation and management of Information Systems activity logs and in the approaches used to analyze Information Systems activity.

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 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 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.

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

Policy

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 develop (or adopt) and adhere to risk-informed auditing and reporting procedures. These procedures, for the collection, monitoring, management, and review of system, application, network, and User activity, must meet the minimum standards specified by this policy. Auditing procedures must be of the appropriate level and type based on associated risk. ISO shall prepare common procedures that may be adopted by those Information Owners and Information System Owners who do not require a customized plan.

The appropriate hardware, software, or procedural auditing collection and management mechanisms must be implemented and, at a minimum, provide the following information:

- Date and time of the activity
- Origin of the activity
- Identification of the User, service, or process performing the activity
- Description of the attempted or completed activity

At a minimum, the following activities must be monitored by the Information Owner or Information System Owner:

- Privileged account usage
- Information system resource start-up or stop
- Failed authentication attempts
- General login activity
- Password change activity
- Data modification (where required for regulatory compliance)

The review of system, application, network, and User activity shall be done via a documented process which, at a minimum:

- Identifies the person or persons responsible for reviewing activity records
- Defines "significant" activity
- Describes the steps taken when exceptions or anomalies are identified
- Determines which activity records need to be archived and for how long
- Sets forth Information Security Incident reporting criteria
- Establishes procedures for preserving records of significant activity

Whenever possible, employees shall not be assigned to monitor or review activity originating from their own User accounts.

Audit records and reports must be retained in accordance with University retention requirements, as defined in the University of Arizona Common Records Retention and Disposition Schedule, and standards and procedures must be consistent with applicable laws, regulations, and guidance.

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]

Information Security Incident Response Plan [3]

Information Security Incident Reporting and Response Policy [4]

Data Classification and Handling Standard [5]

University of Arizona Common Records Retention and Disposition Schedule [6]

University Retention Schedule Policy [7]

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://confluence.arizona.edu/download/attachments/39782340/Incident%20Response%20Plan_v4.pdf?api=v2
[4] https://policy.arizona.edu/information-technology/information-security-incident-reporting-and-response-policy
[5] https://security.arizona.edu/content/data-classification-and-handling-standard
[6] https://rmaa.arizona.edu/sites/rmaa/files/inline-files/common_retention_schedules.pdf
[7] https://rmaa.arizona.edu/retention