Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
January, 2020
Policy Number:
ISO-1000
Responsible Unit:
Information Security Office
Phone:
(520) 621-6700

Purpose and Summary

This document establishes the Device and Media Protection Policy for the University of Arizona. This policy defines information security requirements that ensure device and media protection during the storage, transport, and disposal of Information Resources.

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 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'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

A. All Classifications of University Information

1. Information Resource Owners must ensure University Information, Information Systems, and related resources of any classification, as defined in the University's Data Classification and Handling Standard [1], are protected in proportion to their security risk by establishing processes that meet the following minimum requirements:
    a. **Storage**
        i. Information Resources must be stored in a safe and secure environment to prevent damage, loss, and/or theft.
        ii. University Information stored solely on media and devices that are vulnerable to degradation over time (e.g., unique information with no redundancy stored on magnetic tapes, CDs, DVDs, etc.) must be transferred to fresh media every five (5)

years or prior to the media's predicted life expectancy, whichever occurs earlier.

b. **Transport**
    i. University Information and any devices or media on which it is stored or transported must be protected against unauthorized access, misuse, and/or corruption during transport.
c. **Disposal**
    i. Information Resources must be disposed of securely in accordance with the requirements defined in the University's Procedures for Disposal of Computer/Electronic Surplus Property [2], except for CDs and DVDs, which may be rendered unusable by breaking or shredding the discs without utilizing the foregoing IT disposal procedures.

B. Confidential and Regulated University Information

1. Information Resource Owners with responsibility for University Information and any devices or media that store, process, or transmit University Information classified as Confidential or Regulated, as defined in the University's Data Classification and Handling Standard [1], 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:
    a. **Storage**
        i. All such Information, devices, and media must be encrypted with cryptographic modules that meet industry best standards and Information Security Office standards.
    b. **Transport**
        i. All such Information, devices, and media must be shipped by a tracked carrier with a recipient signature required. The encryption key must only be released after the package and confirmation signature have been received.
    c. **Disposal**
        i. At the time of disposal, all such Information, devices, and media must be sanitized according to NIST's Guidelines for Media Sanitization [3].

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

ISO must initiate mechanisms for tracking compliance with this policy and must 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 all information security policies and related procedures. In cases where University resources are actively threatened, the CISO should 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.

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.

Responsibility

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 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 ISO. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Related Information*

- ISO Website [4]
- Data Classification and Handling Standard [5]

- Procedures for Disposal of Computer/Electronic Surplus Property [2]
- Federal Information Processing Standards PUB 140-2 [6]
- NIST Guidelines for Media Sanitization (800-88 rev. 1) [3]

Revision History*

Nonsubstantive revisions January 24, 2020

Replaces Interim policy of 3/19/19

Links
[1] https://security.arizona.edu/content/data-classification-and-handling-standard
[2] https://pacs.arizona.edu/surplus_department_main
[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[4] https://security.arizona.edu/content/policy-and-guidance
[5] https://security.arizona.edu/data-classification-and-handling-standard
[6] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf