Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
December, 2021
Policy Number:
ISO-1600
Responsible Unit:
Information Security Office
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Vulnerability and Patch Management Policy for the University of Arizona. This policy defines requirements for the management of information security vulnerabilities and the notification, testing, and installation of security-related patches on devices connected to University networks.

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 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.

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. **Vulnerability Management**
    a. The ISO is authorized to conduct routine scans of devices, systems, and applications connected to University networks to identify operating system and application vulnerabilities.
    b. Information Resource Owners must develop (or adopt) and adhere to risk-informed vulnerability management procedures.
        i. The procedures for the collection, monitoring, management, and review of device, system, and application vulnerabilities must meet the minimum standards specified in the University Vulnerability and Patch Management Standard [2].
2. **Patch Management**
    a. Servers, services, and applications must be maintained with current OS, application, or security patch levels, as recommended by the software manufacturer and informed by

risk, to protect University Information from known information security issues.

b. Information Resource Owners must develop (or adopt) and adhere to risk-informed patch management procedures.
    i. The procedures for the identification and management of information security patches for servers, services, and applications must meet the minimum standards specified in the University Vulnerability and Patch Management Standard [2].

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 any to 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 [3].

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 System Owners

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 [4]
- Information Security Risk Management and Security Planning Policy [5]
- Vulnerability and Patch Management Standard [2]
- University Information Resource Classification Standard [6]
- AWS Security Best Practices [7]
- Azure security best practices and patterns [8]
- Best Practices for Securing Active Directory [9]

Revision History*

04/25/2024: Updated link to Vulnerability and Patch Management Standard.

11/17/2023: Links updated.

03/15/2023: Non-substantive revisions to Policy Section, paragraphs A.1 and A.2 - for positioning and clarification purposes.

12/2021: Reference to Information System Owners responsibilities regarding patch management added to Policy Section A - All Classifications of University Information; revision to Tracking, Measuring and Reporting Section: ISO tracking and reporting responsibilities; Related Information Section updated; several hyperlinks updated.

01/24/2020: Non-substantive revisions.

03/19/2019: Replaces Interim policy.

Source
URL:https://policy.arizona.edu/information-technology/vulnerability-and-patch-management-policy

Links
[1] mailto:security@arizona.edu [2] https://emailarizona.sharepoint.com/sites/ISO-Communications/ISO%20Governance%20Documentation/Forms/AllItems.aspx?id=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D1600%20Vulnerability%20and%20Patch%20Management%2FISO%2D1600%2DS1%20Vulnerability%20and%20Patch%20Management%20Standard%2Epdf&parent=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D1600%20Vulnerability%20and%20Patch%20Management [3] 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 [4] https://security.arizona.edu/content/policy-and-guidance [5] https://policy.arizona.edu/information-technology/information-security-risk-management-and-security-planning-policy [6] https://emailarizona.sharepoint.com/sites/ISO-Communications/ISO%20Governance%20Documentation/Forms/AllItems.aspx?id=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D400%20Information%20Classification%20and%20Determination%2FISO%2D400%2DS1%2DInformation%2DResource%2DClassification%2DStandard%2Epdf&parent=%2Fsites%2FISO%2DCommunications%2FISO%20Governance%20Documentation%2FISO%2D400%20Information%20Classification%20and%20Determination [7] https://aws.amazon.com/architecture/security-identity-compliance/ [8] https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns [9] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory