Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
May, 2019
Policy Number:
ISO-1600
Responsible Unit:
Information Security Office
Phone:
(520) 621-6700
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'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

Vulnerability

ISO is authorized to conduct routine scans of devices, systems, and applications connected to University networks to identify operating system and application vulnerabilities.

All Information System Owners are required to ensure routine review of the results of vulnerability scans of devices, systems, and applications for which they are responsible and to evaluate, test, and mitigate, where appropriate, identified vulnerabilities.

Vulnerability scanning and review shall be repeated as part of each annual risk assessment conducted pursuant to the Information Security Risk Management and Security Planning Policy, as well as each time a change is made that may introduce additional vulnerabilities. Information System Owners shall coordinate with ISO to schedule these scans and ensure timely (as determined by risk) review of findings.

Patch Management

ISO shall produce and maintain a Patch Management Standard that defines the minimum information security standards necessary to ensure the protection of University Information and Information Resources. The minimum standards shall include the following requirements:

- A risk-informed systems patch cycle for all server operating systems (OS) shall be scheduled, as appropriate, for Information Systems and related subsystems.
- Any emergency patching outside of the routine patching schedule shall be done according to level of risk, as determined by the Information System Owner in consultation with the ISO.
- Servers, services, or applications shall 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.

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 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 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 Risk Management and Security Planning Policy [4]

Patch Management Standard

Data Classification and Handling Standard [5]

AWS Security Best Practices [6]

Azure security best practices and patterns [7]

Best Practices for Securing Active Directory [8]

Revision History*

Replaces Interim policy of 3/19/19

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

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-risk-management-and-security-planning-policy
[5] https://security.arizona.edu/data-classification-and-handling-standard
[6] https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
[7] https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns
[8] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory