Vulnerability Management Policy

Document Number: ITS-0020 **Date Published(sys):** 3/13/2024

General Description

Purpose:

The purpose of this document is to set out the policy and controls to implement and maintain a sound vulnerability management program that covers the assessment and management of technical vulnerabilities within the IT environment, with the objective of proactively mitigating security risks associated with it.

This policy provides a consistent outline throughout the organization of the technology and procedures necessary for implementing a comprehensive, and integrated vulnerability management program to discover, assess, prioritize and remediate technical vulnerabilities affecting Trinity University systems, including but not limited to operating systems, applications, databases, web technologies, cloud resources, desktop software, mobile devices, network devices and hardware, to maintain appropriate levels of security.

This policy is complemented with the Trinity University Vulnerability and Patch Management Plan, which contains detailed implementation procedures of policy and controls stated in the current document.

Scope:

This vulnerability management policy applies to all systems, people and processes that constitute Trinity University's (TU) information systems, including staff, executives, faculty, and third parties with access to TU's information technology assets and called hereinafter as TU Workforce.

This vulnerability management policy applies to all systems, people and processes that constitute Trinity University's (TU) information systems, including staff, executives, faculty, and third parties with access to TU's information technology assets and called hereinafter as TU Workforce.

Exceptions:

In a few instances, Trinity systems may require to be exempted from the vulnerability management program due to possible technical difficulties or third-party contractual

obligations. Any such exceptions to the current policy must be documented and approved via Trinity's Exceptions Management Process.

Policy Content

① Vulnerability and Patch Management Plan

A vulnerability and patch management plan must be created, implemented, maintained, and enforced at Trinity University.

This plan must detail Trinity's vulnerability and patch management program, including the implementation of mechanisms to timely obtain information about technical vulnerabilities of information systems, the evaluation of the organization's exposure to such vulnerabilities and the implementation of appropriate safeguards to address the associated risk.

The plan must include supporting activities such as training and reporting metrics for effective implementation of the vulnerability and patch management program.

The plan must include roles and responsibilities of teams/roles for accomplishing all the activities of the vulnerability management program in a timely and effective manner.

② Create/Update a System Inventory

ITS must create a system inventory of IT resources in scope for the vulnerability management program to determine which brand, model and version of hardware equipment, operating systems, database, system, web server and software applications are used within the organization.

System inventory must be updated on an annual basis or whenever changes occur to IT resources to ensure that all the IT resources are covered in Trinity's vulnerability management program.

③ Monitor for Vulnerabilities, Remediations, and Threats

ITS must monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the IT resources within the system inventory.

ITS must establish procedures to obtain copies of the software updates electronically when they are issued by the vendor.

ITS must utilize authorized resources such as system vendor websites, third-party mailing lists and newsgroups, vulnerability management databases, and different tools for tracking the latest vulnerabilities.

In addition to the regular application of vendor-supplied software updates, ITS must conduct regular vulnerability scans at least monthly, and a penetration test assessment on critical infrastructure and systems at least annually. The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker.

The monthly vulnerability scans may be carried out in-house or by an external company or a combination of both. Those vulnerability scans should cover all the internal and external facing assets on the production network.

The annual penetration test must be commissioned as required, using external qualified specialists as part of a carefully planned exercise, The plan must address the scope of the assessment, the methods to use, and the operational requirements, in order to provide the most accurate and relevant information about current vulnerabilities, without affecting the operation of the organization.

④ Prioritize Vulnerability Remediation

ITS must prioritize the order and scheduling in which the organization addresses vulnerability remediation.

The scheduling of the installation of updates will depend upon several factors including:

The criticality of the systems being updated.

The expected time taken to install the updates (and requirements for service outages to users).

The degree of risk associated with any vulnerabilities that are being mitigated by the updates:

Trinity must evaluate and assign a rating to each vulnerability as critical, high, medium, low, informational, or trivial.

Coordination of the updating of related components of the infrastructure.

Dependencies between updates.

ITS must prioritize treatment of vulnerabilities based on their risk rating. Vulnerabilities with rating critical or high must be treated foremost. If patching is required for the vulnerability remediation, Trinity must comply with below minimum service levels.

Vulnerability Risk Rating	Service Levels

Critical	Less than 3 days
High	Less than 7 days
Medium	90 days
Low	180 days

All the exceptions to this rule must be approved by authorized personnel, based on the risk acceptance process.

An updated release plan must be created and maintained to keep track of when various systems will be updated, taking into account the factors listed above. The plan must be managed through the change management process.

⑤ Create/Maintain Vulnerability Database

ITS must maintain a database of vulnerabilities gathered from multiple sources that require remediation and/or patching steps that need to be applied to Trinity systems.

The database must include vulnerability information, vulnerability analysis for prioritization, and vulnerability remediation plan.

⑥ Conduct Testing of Remediations

All the remediations must be tested before deploying the changes to Trinity systems. Failed remediations must be further examined for resolution.

⑦ Inform System Administrators and System Owners

All the vulnerabilities and respective remediation information must be informed to all the affected users, including system administrators, system owners, and end users.

⑧ Deploy Vulnerability Remediations

Only successfully tested vulnerability remediations must be deployed into production. Vulnerability remediation activities typically include security patch installation, configuration adjustment and/or software removal.

Where security patch installations and configuration changes are recommended to mitigate the vulnerabilities, these must be sent through the organization change management process so that appropriate controls are in place for testing, risks assessment and backout.

⑨ Verify Vulnerability Remediation

ITS must verify systems for vulnerability remediations.

Successful remediation of vulnerabilities must be tested through network and host vulnerability scanning, checking patch logs, penetration tests, and verifying configuration settings.

⑩ Cloud Service Providers/ Third Parties

For cloud services, the responsibilities of the cloud service provider (CSP) and ITS as the cloud service customer, must be defined and agreed upon. This may involve the CSP being responsible for vulnerability assessment and patching for some or all aspects of the service, depending on the cloud service model adopted (e.g. IaaS, PaaS or SaaS or similar service definitions).

ITS must ensure third parties comply with the requirements of our vulnerability management policy. Whenever possible, vulnerability management responsibilities are included in contracts with third parties.

⑪ Vulnerability Management Training

ITS must implement a training program for all participating team members on how to apply vulnerability remediations and best practices for effectively implementing the vulnerability management program, based on their roles in this process.

⑫ Vulnerability and Patch Management Metrics

ITS must consistently measure the effectiveness of its vulnerability and patch management program utilizing ‘vulnerability and patch management metrics’ and apply corrective actions as necessary.

On a monthly basis, these security metrics must be presented to the Information Security Governance Committee.

Performance Evaluation

Consequences of Policy Violation:

Users who violate this policy may be subject to disciplinary action, up to and including termination of employment or contract with Trinity University.

Trinity University cooperates with appropriate law enforcement entities if any user may have violated federal or state law. Instances of failure to adhere to this policy will be brought to the attention of the Chief Information Officer (CIO). The CIO may seek

consultation/advice from Human Resources.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Application	Any data entry, update, query, or report program that processes data for the user.
Configuration Adjustment	The act of changing an application's setup. Common configuration adjustments include disabling services, modifying privileges, and changing firewall rules.
Host	A computer or IT device (e.g., router, switch, gateway, firewall). Host is synonymous with the less formal definition of system.
Operating System	The master control program that runs a computer.
Patch	An additional piece of code developed to address a problem in an existing piece of software.
Remediation	The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application.
Remediation Plan	A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation.
Risk	The probability that a particular threat will exploit a particular vulnerability.
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operating environment. When not used in this formal sense, the term is synonymous with the term "host". The context surrounding this word should make the definition clear or else should specify which definition is being used.
System Administrator	A person who manages the technical aspects of a system.
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.
Threat	Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.
Vulnerability	A vulnerability is commonly defined as "an inherent weakness in an

Term:	Definition:
	information system, security procedures, internal controls, or implementation that could be exploited by a threat source.”

Related Documents

Related Content:

Trinity's vulnerability management policy is aligned with NIST Special Publication 800-40, creating a patch and vulnerability management program.

1. NIST Special Publication 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program: https://csrc.nist.gov/publications/detail/sp/800-40/version-20/archive/2005-11-16.
2. Vulnerability and Patch Management Plan: Link to Vulnerability and Patch Management Plan.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.0	4/27/2022 11:29 AM	Ben Lim
v3	1/27/2022 1:18 PM	Dan Carson
v2.0	8/21/2020 8:02 AM	Holly Warfel
v1.0	1/14/2020 2:46 PM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer