UNT SYSTEM™
Information Technology

INFORMATION TECHNOLOGY STANDARD

VULNERABILITY AND PATCH MANAGEMENT

Purpose and Benefits

Employees of the UNT System Enterprise (Enterprise) must adhere to all regulations, policies, and standards related to Vulnerability and Patch Management. The remediation of vulnerabilities and timely patching of systems, to reduce the risk to the security of information at the Enterprise, must occur in accordance with standards set by UNT System IT Cybersecurity and IT Compliance.

Security patch management (Patch Management) is a practice designed to proactively prevent the exploitation of IT vulnerabilities existing within an organization. Through the application of security related software or firmware updates (patches) we reduce or eliminate vulnerabilities that present potential for exploitation, thereby reducing time and financial expenditures on compromised assets.

Information systems owned by or operated by the Enterprise must be kept current and protected from the exploitation of vulnerabilities leading to damage, loss, or unauthorized disclosure of data or compromised information systems.

This standard applies to all employees, contractors, and vendors of the Enterprise and establishes Vulnerability and Patch Management requirements for all Enterprise information resources that store and/or process Enterprise data.

Authority and Requirements

The Configuration Hardening and Patch Management section of the UNT System Information Security Handbook (Page 34) serves as the Enterprise authority for this standard and requires the following:

1. Prioritization of patches and system updates;
2. Specification that patches are to be applied at regular intervals;
3. Aligned maintenance windows with vendor patch and update release schedules;
4. Patch monitoring for correct installation;
5. Problems shall be addressed as they occur;
6. Contingency plans for handling emergency or critical updates; and
7. End-of-life procedures to address older systems using one or more of the following approaches:
   a. Decommission system;
   b. Upgrade to latest platform;
   c. Migrate to another platform; or
   d. Manage risk through use of compensating controls.

The Vulnerability and Patch Management standards herein satisfy the control requirements of SI-2 in the Texas Department of Information Resources Security Controls Standards Catalog (Page 165).

Definitions

Patch. "Patch" means an update to an operating system, application, or other software issued to correct specific problems or vulnerabilities.

Information Security Program. "Information Security Program" means the policies, Information Security Handbook, control catalog, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions.

User. "User" means an individual or automated application authorized to access information or information resources in accordance with the Information Owner-defined controls and access rules.

Vulnerability. "Vulnerability" means a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

General Implementation

Asset Management

All Enterprise information resource assets must be inventoried and labelled as to their criticality to business operations and to the sensitivity of the data they store and/or process. Inventories shall include hardware, software, and data assets.

Labelling of assets shall follow the criticality classification listed below.

Criticality	**Characteristics**
High	• Assets critical to operations • Assets critical to infrastructure • Assets exposed to the internet • Assets storing Confidential information • Assets under contractual requirements such as DFARS/CMMC/PCI • Assets with end users as system/device administrators • Assets not managed by Information Technology personnel
Moderate	• Assets used as standard workstations • Assets managed by Information Technology personnel • Assets that do not store Confidential information
Low	• Assets as development environments • Assets with limited functionality • Image based assets or constantly refreshed systems

Configuration Management

Information systems and devices must be configured with the secure baseline configurations adopted by UNT System IT Cybersecurity and IT Compliance. UNT System IT Cybersecurity and IT Compliance have adopted the Center for Internet Security (CIS) benchmarks as secure baseline configurations. Variances of configuration from the appropriate benchmarks require formal security exceptions approved by the Chief Information Security Officer or their delegate.

Systems for which no CIS benchmarks exist shall be configured using vendor or industry best practices for secure configuration, as agreed on and approved by the Chief Information Security Officer or their delegate.

Scanning and Detection

UNT System IT Cybersecurity and IT Compliance are responsible for conducting scans of Enterprise networks, systems, or services owned by or operated on behalf of the Enterprise and systems, or services operated using domains owned by or operated on behalf of the Enterprise. Information System/Application Owners must make information resources available for scanning using methods which may include, but are not limited to:

- Discovery scans on Enterprise networks to enumerate information systems and resources;
- Agent-based scans using deployed agent software to systems as available and applicable;
- Credentialed scans requiring authentication to the systems using preconfigured credentials;
- Policy-based scans comparing device/software configuration against benchmarks or standards;
- Web-based application scans using tools to test for vulnerabilities; and
- Third-party services authorized by the Chief Information Security Officer to detect vulnerabilities on external-facing systems.

Information System/Application Owners must not prevent the scanning of networks, systems, or services by blocking or filtering scanning functionality.

Monitoring and Reporting

UNT System IT Cybersecurity and IT Compliance will make available results of vulnerability and patch scanning to appropriate IT support groups, information system Custodians, and/or the Information System/Application Owners at regular intervals and only provide dashboard vulnerability data, trends, and metrics to support personnel based on business justification and as necessary. UNT System IT Cybersecurity and IT Compliance will report on and monitor vulnerabilities discovered and/or reported by external providers.

Vulnerability and patch compliance data is considered Confidential as disclosure of the information has the potential to result in harm to Enterprise networks, systems, and services.

UNT System IT Cybersecurity and IT Compliance will report key performance indicators and other metrics to Enterprise IT, institutional, and departmental leadership at regular intervals.

Prioritization of Patching and Vulnerability Remediation

Software patching and vulnerability remediation should be prioritized based on the level of risk posed to the Enterprise and the criticality of the systems to business operations. Vulnerabilities should be addressed using the Priority Matrix below:

Vulnerability Level	**CVSS Score Ranking**	**Maximum Time to Remediate**
Emergency	Risk Based	3 Business Days
Critical	10.0 – 9.0	30 Days
High	8.9 – 7.0	30 Days
Medium	6.9 – 4.0	45 Days
Low	3.9 – 0.1	Risk Management Decision

Remediation of vulnerabilities and patching must use vendor/industry resolutions or vendor provided patches to mitigate risks or patch networks, systems, or services. The use of a ‘Ring’ model is suggested where deployment occurs to increasingly larger ‘rings’ of systems/end users to effectively measure and respond to possible issues caused by the remediation or patch.

Information System/Application Owners and Custodians should establish separate maintenance windows at regular intervals to address both software and hardware vulnerability remediation and patching.

Information System/Application Owners and Custodians must follow Change Management standards and procedures when remediating vulnerabilities or patching systems.

Information System/Application Owners must manage the System Currency of information systems to avoid the use of end-of-life (EOL) systems. Information System/Application Owners must address EOL systems as follows:

1. Patch or update to the latest supported version of the system;
2. Pursue extended support from the vendor of the system, if possible;
3. Migrate to another product or platform;
4. Decommission or stop all use of the system; or

5. Address the risk presented by using the EOL system through compensating controls and a documented security exception.

Exceptions and Compensating Controls

Exceptions to Information Security policies and this standard may be approved by the Chief Information Security Officer or their delegate when accompanied with sufficient justification and compensating controls, in accordance with the UNT System Information Security Program.

The Chief Information Security Officer may revoke an exception at any time.

References and Notes

DIR Security Controls Standards Catalog
UNT System Information Security Regulation 06.1000
UNT System Information Security Handbook

Approvals and Revision History

Date	Approved By	Version	Notes
7/1/2024	Rich Anderson	1.0	New Vulnerability and Patch Management Standard