UT System Procedure: IT7810-UTSA Information Technology Vulnerability Management Procedure	
Version 1	Effective Date: 03/01/2026

Purpose

This procedure establishes the required operational process for identifying, evaluating, prioritizing, mitigating, and remediating vulnerabilities affecting university-owned or managed servers. It provides a risk-based framework that enables campuses to consistently remediate vulnerabilities based on technical severity, exploit likelihood, asset criticality, and institutional risk.

This procedure supports the requirements defined in IT7810 and provides implementation guidance to ensure timely remediation and risk reduction.

I. Scope

This procedure applies to:

- All university-owned, managed, or hosted servers, including on-prem and cloud-hosted systems
- All operating systems and server-based applications
- All environments, including production, development, testing, and disaster recovery
- Network infrastructure devices
- Third-party, vendor-managed infrastructure, which is governed through contractual and vendor risk management processes

This procedure does not apply to:

- Workstations and end-user computing devices

II. Definitions

Common Vulnerability Scoring System v4 (CVSSv4) - provides an industry standard measure of technical severity, capturing exploitability, impact, and environmental factors across a 0.0–10.0 scale. Higher scores represent higher potential impact with lower attacker effort.

Compensating Control - A safeguard implemented when a patch is unavailable or cannot be immediately applied, which reduces the likelihood or impact of exploitation.

Exploit Prediction Scoring System (EPSS) - estimates the probability that a vulnerability will be exploited in the wild within 30 days, using machine learning models and real-world threat activity. Higher scores indicate a greater likelihood of exploitation.-learning models and

External System - A system accessible from untrusted networks, including the public internet, partner networks, or unauthenticated access.

Examples include:
- Public web servers
- Internet exposed applications or APIs
- VPN gateways
- Internet accessible cloud services

Internal System - A system accessible only from authenticated university networks or through internal-network access (e.g., VPN, zero-trust, private LAN).

Examples include:
- Application servers, internal administrative tools
- File servers, database servers, internal services
- Workstations or systems restricted to internal connectivity

Remediation - Actions taken to eliminate or sufficiently reduce risk associated with a vulnerability. Remediation may include:
- Vendor-supplied patches or updates
- Configuration changes
- Removal of vulnerable components
- Network isolation or segmentation
- Access restrictions
- Compensating or mitigating controls

Remediation is not limited to vendor patch application.

Vulnerability

A weakness in software, hardware, or configuration that could be exploited to compromise confidentiality, integrity, or availability.

III. Roles and Responsibilities

System Owners

Responsible for:

- Ensuring vulnerabilities are remediated within required timelines
- Coordinating remediation activities with system administrators
- Approving risk acceptance when remediation cannot be completed

System Administrators

Responsible for:

- Applying patches and remediation actions
- Implementing mitigating controls when patches are unavailable
- Verifying remediation effectiveness

Campus Information Security Office

Responsible for:

- Operating vulnerability scanning tools
- Validating vulnerability findings
- Risk prioritization and reporting
- Monitoring remediation timelines
- Escalating overdue vulnerabilities

Campus IT Leadership

Responsible for:

- Ensuring compliance with this procedure
- Supporting remediation efforts
- Accepting or rejecting risk exceptions

IV. Vulnerability Identification

Campuses must implement vulnerability identification processes, including:

- Automated vulnerability scanning using approved tools (e.g., Tenable, Qualys)
- Agent scans where technically feasible
    - Authenticated scans if agent scans are not feasible
    - Unauthenticated scans if agent or authenticated scans are not feasible

- Scanning frequency at a minimum of daily for all servers

Additional sources may include:

- Vendor advisories
- Security bulletins
- Threat intelligence feeds
- Penetration tests
- Security incident response findings

V. Vulnerability Severity Classification

Vulnerabilities must be classified using the Common Vulnerability Scoring System version 4 (CVSSv4).

Severity	CVSSv4 Score
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

CVSS provides technical severity based on exploitability and impact.

VI. Exploitability Consideration (EPSS)

The Exploit Prediction Scoring System (EPSS) must be used to prioritize remediation for externally exposed systems.

EPSS estimates the probability of exploitation within 30 days based on real-world threat intelligence.

Higher EPSS scores indicate a greater likelihood of active exploitation.

EPSS is used to accelerate remediation timelines for high-risk vulnerabilities.

VII. Remediation Timelines

Remediation timelines begin upon vulnerability discovery or publication, whichever is later.

External Systems

Severity	EPSS Score	Remediation Timeline
Critical or High	EPSS ≥ 50 percent	14 days
Critical or High	EPSS < 50 percent	30 days
Medium	Any	60 days
Low	Any	90 days

Internal Systems

Severity	Remediation Timeline
Critical or High	30 days
Medium	90 days
Low	180 days

Emergency Remediation / Out-of-Band Patching

Vulnerabilities that present a high likelihood of active exploitation must not be deferred to standard patch cycles.

For Critical or High vulnerabilities affecting external systems with EPSS ≥ 50 percent, campuses must implement one of the following within the required remediation timeline:

- **Apply emergency (out-of-band) patching outside of normal maintenance windows, or**
- **Implement immediate compensating controls to reduce exposure**

Standard monthly or scheduled patch cycles do not supersede required remediation timelines for high-risk vulnerabilities.

Where emergency patching is not operationally feasible, compensating controls must be implemented immediately, and a formal exception must be submitted.

VIII. Remediation Requirements

Remediation timelines are risk-driven and may require action outside of standard maintenance or patch cycles for high-risk vulnerabilities.

Remediation must include one or more of the following actions:

- Applying vendor-provided patches
- Applying security updates or hotfixes
- Disabling vulnerable services or features
- Removing vulnerable software components
- Restricting network access
- Implementing firewall rules
- Implementing endpoint protection controls
- Segmenting systems
- Implementing vendor-recommended mitigations

When vendor patches are unavailable, compensating controls must be implemented within the same remediation timeline.

Once a vendor patch becomes available, it must be applied in accordance with the timelines defined in this procedure.

IX. Validation of Remediation

After remediation, validation must be performed by:

- Rescanning affected systems, or
- Verifying remediation through documented configuration review

Vulnerabilities must not be considered closed until validation confirms remediation effectiveness.

X. Exception, Mitigation Validation, and Risk Acceptance Process

A vulnerability is considered remediated only when the underlying vulnerability is eliminated through patching, upgrading, removal, or other permanent corrective action.

Mitigation measures such as firewall rules, network segmentation, disabling services, or access restrictions are considered compensating controls and do not constitute full remediation unless reviewed and approved by the Campus Information Security Office.

Exception Requirements

A formal exception is required when:

- The vulnerability remains present beyond the required remediation timeline
- A vendor patch is unavailable
- Remediation cannot be applied due to operational or technical constraints
- Compensating controls are used in place of full remediation

Exceptions are not required when the vulnerability has been fully remediated and validated.

Compensating controls must be reviewed and approved by the Campus Information Security Office to validate risk reduction. The exception remains active until the vulnerability is fully remediated.

Exception Approval and Review

Exception requests must include affected systems, justification, compensating controls, and a planned remediation timeline. They must include a defined expiration date not to exceed twelve months.

Exceptions must be approved by the System Owner and Campus Information Security Office and reviewed at least quarterly to validate that:

- Compensating controls remain effective
- Risk has not increased
- Remediation is still not feasible

Exceptions that persist beyond one year or exceed two consecutive review cycles without progress toward remediation must be escalated to Campus IT Leadership or a designated governance body (e.g., Risk Committee, CIO, or equivalent) for continued risk acceptance or direction.

XI. Reporting and Escalation

Campus Information Security Offices must:

- Track vulnerability remediation status
- Report overdue vulnerabilities to system owners and leadership
- Escalate unresolved Critical and High vulnerabilities

Regular reporting should include:

- Number of vulnerabilities by severity
- Remediation compliance rates
- Overdue vulnerabilities
- Trends over time
- Long-standing exceptions and overdue vulnerabilities must be included in regular reporting and escalated through established governance channels.

XII. Compensating Controls and Mitigation

When patches are unavailable, mitigation actions must be implemented, such as:

- Network isolation
- Firewall restrictions
- Disabling vulnerable features
- Increasing monitoring and logging
- Access restrictions

Mitigations reduce risk but do not eliminate the requirement to patch once available.

XIII. Continuous Improvement

Campuses should continuously mature vulnerability management programs by:

- Improving asset inventory accuracy
- Implementing asset criticality tagging
- Integrating vulnerability data with asset classification
- Prioritizing remediation based on risk context
- Improving remediation timelines and compliance rates

XIV. Compliance

Failure to comply with this procedure increases institutional risk and will be escalated to campus leadership. This failure will result in the suspension or revocation of network access, removal from sensitive or privileged roles, and/or disciplinary action up to and including termination in accordance with university HR policies.

XV. Procedure History

Version	Date
1	03/01/2026 - New Procedure

XVI. References

1. IT7810-Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy
2. Common Vulnerability Scoring System v4 (CVSSv4)
3. Exploit Prediction Scoring System (EPSS)