

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

## SECTION 1. Policy Statement

### I. Objective

This policy provides guidance and structure for the University to establish sound processes for performing Vulnerability Management, for performing threat and vulnerability monitoring, for creation and maintenance of audit logs, and for installation of anti-malware software on all University Assets.

### II. Vulnerability Management Policy

The Central IT Department must communicate the requirements and processes for Vulnerability Management to the campus community annually to engage campus communities and individuals in the shared responsibility of Vulnerability Management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

1. The Central IT Department will create a process for performing Vulnerability Management that meets the following:
  - a. At a minimum, the Vulnerability Management process must be reviewed by the Central IT Department on an annual basis or following changes that affect the operability and/or security of the System.
  - b. Monitoring of vulnerability announcements and emerging threats applicable to the University's Assets, Systems, and Resources that includes establishing clear lines of communication regarding threat intelligence between the vendor(s) and the University.
  - c. Validation that all cloud-based services have a documented Vulnerability Management program.
  - d. Ensures that identified vulnerabilities are prioritized with higher risk vulnerabilities addressed first.
  - e. Ensures that all the University's Systems connected to the University IT Network are scanned for vulnerabilities.
2. The Central IT Department will create a process for remediating identified Vulnerabilities that meets the following:
  - a. Review of the process occurs at a minimum annually by the Central IT Department.

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

- b. Ensures that operating Systems are configured to automatically update, unless an alternative approved patching process is used.
  - c. Ensures that applications are configured to automatically update, unless an alternative approved patching process is used.
  - d. Requires that all Users of the University's Assets install updates for the University's Systems and applications in a timely manner.
  - e. Ensures that all required reboots occur within a reasonable timeframe to ensure updates are properly installed.
  - f. Ensures that high risk vulnerabilities are mitigated within 14 days.
  - g. A separate process for exceptions such that vulnerabilities that cannot be remediated are submitted through this process. The exception process ensures that all false positives for vulnerabilities are documented.
3. The Central IT Department will create a process for performing threat and vulnerability monitoring that meets the following:
- a. Subscription to a threat information service to receive notifications of recently released patches and other software updates.
  - b. Notification of the decision-making authority if vulnerabilities are not mitigated in a timely manner.
  - c. A monthly report containing the status of all known vulnerabilities within the University that is presented to the CISO for review.

#### Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

1. The Central IT Department will create a process(es) to:
  - a. Perform automated vulnerability scans of the internal University Assets on a quarterly basis (IG2). This includes conducting both authenticated and unauthenticated scans and using a Security Content Automation Protocol (SCAP)-compliant vulnerability scanning tool.

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

- b. Perform automated vulnerability scans of externally exposed University owned Assets using a SCAP compliant vulnerability scanning tool (IG2). This includes performing scans, at a minimum, monthly.
- c. Remediate detected vulnerabilities in software through processes and tooling monthly, based on the remediation process (IG2).

### III. Audit Log Management Policy

The Central IT Department must communicate the requirements and processes for audit log management to the campus community annually to engage campus communities and individuals in the shared responsibility of audit log management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

All of the University's Assets are required to comply with the University audit logging procedures.

- 1. The Central IT Department will create a University-wide strategy to establish and maintain an audit log process. The strategy must adhere to the following:
  - a. Follow a risk-based approach for determining the logging information that is retained.
  - b. Documentation must be updated at a minimum annually.
  - c. The contents of logs must be specified within the Secure Configuration Policy.
  - d. Audit logging must be enabled on all the University's Assets, as is practical.
  - e. Audit logs must not be disabled on the University's Assets.
- 2. The Central IT Department will create a process to move the process defined logs from the University's Assets to an audit log datastore. The process will include the following:
  - a. This relocation of the logs may be done manually or via electronic means.
  - b. Access controls must be used to prevent audit logs from being modified in an unauthorized manner.

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

3. The Central IT Department will create a process to collect audit logs from the University's Assets. The process must include the following:
  - a. Sufficient storage space must be allocated for audit logs for the period required for analysis and retention.
  - b. Sufficient space must be allocated to store audit logs on all the University's Assets.
  - c. Sufficient space must be allocated to store audit logs on any centralized audit log datastore.
4. All high-risk events must be acted upon in accordance with the audit log management process.
5. The Central IT Department will create a process for all audit logs to be stored for a period of a minimum of 12 months. The process must include the following:
  - a. Archived logs must be available for analysis.
  - b. Disposal of audit logs should be in accordance with the University Data management process and/or any applicable statutory requirements.

#### Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

1. The Central IT Department will create a process(es) to:
  - a. Ensure configured detailed audit logging for the University's Assets containing Protected University Information (IG2) that will include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
  - b. Collect DNS query audit logs on the University's Assets, where appropriate and supported (IG2).
  - c. Collect URL request audit logs on the University's Assets, where appropriate and supported (IG2).
  - d. Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals (IG2).
  - e. Centralize, to the extent possible, audit log collection and retention across the University's Assets (IG2).

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

- f. Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat (IG2). Conduct reviews on a weekly, or more frequent, basis.
- g. Collect IT Service Provider logs, where supported (IG3).

#### IV. Malware Defense Policy

The Central IT Department must communicate the requirements and processes for malware defense to the campus community annually to engage campus communities and individuals in the shared responsibility of secure malware defense. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

- 1. The Central IT Department will create a process to install anti-malware software on all the University's Assets where appropriate.
  - a. Users must not disable anti-malware software on the University's Assets.
  - b. Users must not modify the update frequency specified as part of System-wide Policy: IT4912 - Information Technology Secure Configuration Management.
- 2. The Central IT Department will create a process(es) to:
  - a. Configure anti-malware software to automatically update. The Central IT Department must ensure that anti-malware signatures are kept up to date as they become available via an automatic update process.
  - b. Ensure that anti-malware software is functioning properly on all the University's Assets.
  - c. Escalate the presence of unauthorized software and high-risk alerts on the University's Assets.
  - d. Ensure that all cloud-based services have a malware defense program.

#### Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

The Central IT Department will create a process(es) to:

1. Configure anti-malware software to automatically scan removable media (IG2).
2. Enable anti-exploitation features on the University's Assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™ (IG2).
3. Provide centrally managed anti-malware software (IG2).
4. Provide behavior-based anti-malware software (IG2).

#### V. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

---

#### SECTION 2. Reason for the Policy

This policy establishes the requirements for information technology Vulnerability Management, audit log management, and malware defense as described in CIS Control 7 (Continuous Vulnerability Management), CIS Control 8 (Audit Log Management), and CIS Control 10 (Malware Defenses) for the University of Tennessee in support of System-wide Policy: IT0001 - General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

---

#### SECTION 3. Scope and Application

This policy applies to all Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

---

#### SECTION 4. Procedures

Each campus/institute will adopt procedures related to this policy.

---

#### SECTION 5. Definitions

See IT0001 - General Statement on Information Technology Policy for definitions of terms.

<b>System-wide Policy:</b>	
<b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

**SECTION 6. Penalties/Disciplinary Action for Non-Compliance**

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

**SECTION 7. Responsible Official & Additional Contacts**

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	<a href="mailto:cio@tennessee.edu">cio@tennessee.edu</a> or <a href="mailto:iso@tennessee.edu">iso@tennessee.edu</a>
Policy Training	System Chief Information Security Officer	(865) 974-0637	<a href="mailto:iso@tennessee.edu">iso@tennessee.edu</a>

[Text Wrapping Break]

**SECTION 8. Policy History**

Revision 1:

**SECTION 9. Related Policies/Guidance Documents**

- A. University Policies
  - a. IT0001 – General Statement on Information Technology Policy
  - b. IT0002 – Acceptable Use of Information Technology Resources
  - c. IT0003 – Information Technology Security Program Strategy
  - d. IT0004 – Information Technology Risk Management
  - e. IT0005 – Data Categorization
  - f. IT0014 – Security Awareness Training Management

<b>System-wide Policy:</b> <b>IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy</b>	
<b>Version: 1</b>	<b>Effective Date: 01/23/2025</b>

- g. IT0017 - Information Technology Incident Response Management
- h. IT0102 - Information Technology Asset Management
- i. IT0311 - Information Technology Data Access, Management, and Recovery
- j. IT0506 - Information Technology Account and Credential Management
- k. IT1318 - Information Technology Network Monitoring and Defense and Penetration Testing
- l. IT1516 - Information Technology Service Provider Management Application Software Security Management
- m. IT4912 - Information Technology Secure Configuration Management

B. Center for Internet Security Critical Security Controls Navigator

<https://www.cisecurity.org/controls/cis-controls-navigator/>

---