THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT4912 - Information Technology Secure Configuration Management	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to establish configuration guidelines for University Assets, as well as cloud platforms deployed for University use.

II. Secure Configuration Management Policy

The Central IT Department must communicate the requirements and processes for secure configuration management to the campus community annually to engage campus communities and individuals in the shared responsibility of secure configuration 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. Configuration guidelines for creating secure configurations of the University's IT Assets for University Data must be developed by the Central IT Department based on either vendor-provided hardening requirements or industry standards. At a minimum the guideline will include:

a. Establishing a set of secure configurations for all operating Systems or applications before they are used by the University.

b. Establishing a set of secure configurations for all cloud or IT Service Providers before they are used by the University.

c. Establishing a set of secure configurations for all IT Network appliances before they are used by the University.

If configuration guidelines are not available for a particular technology required by the campus community, the Central IT Department must research appropriate security configurations to develop a configuration template for this technology before allowing their use at the University.

2. The Central IT Department will create a process for all the University's Assets deployed in the University's IT Networks to be appropriately configured and meet security requirements for their individual purposes.

a. Automatic session expirations must be configured with the period not exceeding 15 minutes for operating Systems and software Assets where supported.

b. All University hardware Assets, where technically capable, must utilize a host-based firewall or port-filtering tool, with a default-deny rule.

c. Servers must utilize either a virtual firewall, operating System firewall, or a third-party firewall agent enabled and appropriately configured in accordance with the University's standards.

d. Default accounts shipped with operating Systems and software, such as root, administrator, and other pre-configured vendor accounts must be appropriately disabled or configured to prevent unauthorized access (e.g., unauthorized password change). All pre-configured passwords on default or vendor accounts must be changed at first login.

e. Operating Systems, where technically possible, must be configured to automatically update using the University-approved mechanisms unless an alternative approved patching process is used.

f. Applications must be configured to automatically update, unless an alternative approved patching process is used.

g. All software authorized for use within the University must be currently supported by the developer and receiving security updates.

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

i. Configure access control lists on the University's Assets in accordance with the user's need to know. This includes laptops, smartphones, tablets, centralized file Systems, remote file Systems, databases, and all applications. The Data Owner and/or Data Steward must be consulted to determine the access control for the Data sets that they are responsible for.

ii. Ensure that detailed audit logging is enabled for User devices.

iii. Ensure that sufficient space is available on the University's Assets to collect and maintain audit logs.

iv. Disable autorun and autoplay functionality from executing on removable media for all University owned Assets must.

k. Opensource technology will be allowed by the Central IT Department for deployment on University-owned and non-University Assets used for University-related work or education unless there is an unmitigable critical vulnerability.

3. Every cloud platform and/or cloud service used by the University must be appropriately configured in accordance with University standards and CIS benchmarks or allow for vendor supplied

hardening guides if CIS doesn't have a benchmark for a specific IT service and must meet security requirements for their individual purpose.

a. The Central IT Department will create a process with guidance to:

i. Ensure cloud platforms enable detailed audit logging.

ii. Work with those approved companies to achieve the desired configuration for their platforms.

4. The Central IT Department will create a process to ensure that every IT Network appliance that is deployed is appropriately configured and meets the security requirements and industry hardening standards for their individual purpose. Examples of IT Network appliances include routers, switches, firewalls, etc.

5. The Central IT Department will create a process to ensure that:

a. Automatic session expirations must be configured for IT Network appliances.

b. Default accounts shipped with IT Network appliances, such as root, administrator, and other pre-configured vendor accounts must be appropriately disabled or configured to prevent inappropriate access (e.g., password change).

c. All ports, protocols, and IT services not required to support operations must be disabled where possible.

d. Domain Name System (DNS) filtering IT services must be used on all the University's Assets to block access to known malicious domains.

e. IT Network appliances have detailed audit logging enabled.

f. That sufficient space is available to collect and maintain audit logs.

g. All IT Network devices and other infrastructure are configured to automatically update, unless an alternative approved patching process is used.

h. Up-to-date IT Network management protocols (e.g., Secure Shell (SSH)) are used.

6. The Central IT Department will create a process for University owned securely configured technologies to be monitored to ensure they remain in compliance with approved configurations.

7. The Central IT Department will create a process to update the approved secure configuration guidance for a technology in a timely manner when a significant update occurs. In this context,

"significant" is defined by University standards and thresholds. All protocols and tools used to install, modify, or otherwise manage technology configurations must be approved by the Central IT Department.

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.

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

1. Uninstall or disable unnecessary IT services on all of the University's Assets, such as an unused file sharing service, web application module, or service function (IG2).

2. Configure trusted DNS servers on all of the University's Assets (IG2).

3. Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported (IG2). For the University's Assets, do not allow more than 20 failed authentication attempts.

4. Remotely wipe the University Data from University-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the University (IG2). The Data Owner and/or Data Steward must be contacted in these cases.

5. Ensure separate University workspaces are used on mobile end-user devices, where supported (IG3). Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate University applications and Data from personal applications and Data.

6. Update IT Network-based URL filters to limit the University' Assets from connecting to potentially malicious or unapproved websites (IG2).

7. Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications (IG2).

8. Implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards (IG2) that is set to reject.

9. Block unnecessary file types attempting to enter the University's email gateway (IG2).

10. Establish guidelines to deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing (IG3).

11. Establish and maintain a secure IT Network architecture (IG2). A secure IT Network architecture must address segmentation, least privilege, and availability, at a minimum.

12. Securely manage the University's IT Network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure IT Network protocols, such as SSH and HTTPS (IG2).

13. Establish and maintain architecture diagram(s) and/or other IT Network System documentation (IG2). Review and update documentation annually, or when significant University changes occur that could impact this Safeguard.

14. Centralize IT Network access, authorization, and authentications (AAA) (IG2).

15. Establish guidelines to use secure IT Network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) or greater) (IG2).

16. Establish guidelines to require users on remote devices to authenticate to the University-managed VPN and authentication services prior to accessing the University's Resources on end-user devices (IG2).

17. Establish guidelines to establish and maintain dedicated computing Resources, either physically or logically separated, for all administrative tasks related to IT Network management or tasks requiring administrative access (IG3). The computing Resources should be segmented from the University's primary IT Network and not be allowed internet access. An example would include a secure enclave.

III. 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 secure configuration management as described in CIS Control 4 (Secure Configuration of University Assets), CIS Control 9 (Email and Web Browser Protections), and CIS Control 12 (Network Infrastructure Management) 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.

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	cio@tennessee.edu or iso@tennessee.edu
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

[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

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. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

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