THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT1318 - Information Technology Network Monitoring and Defense and Penetration Testing	
Version: 1	Effective Date: 01/23/2025

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to establish appropriate control mechanisms for securing the University Information Technology Networks and to create a Penetration Testing process.

II. IT Network Monitoring and Defense Policy

The Central IT Department must communicate the requirements and processes for IT Network monitoring and defense to the campus community annually to engage campus communities and individuals in the shared responsibility of secure monitoring and 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 associ ated process.

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 for IT Network monitoring and defense that includes:

a. Centralized security event alerting across the University's Assets for log correlation and analysis (IG2).

b. Deployment of a host-based intrusion detection solution on the University's Assets, where appropriate and/or supported (IG2).

c. Deployment of an IT Network intrusion detection solution on the University's Assets, where appropriate (IG2).

d. Traffic filtering between the University's IT Network segments, where appropriate (IG2).

e. The ability to manage access control for the University's Assets remotely connecting to the University's Resources (IG2) and determine amount of access to the University's Resources based on:

i. Up-to-date anti-malware software installed.

ii. Configuration compliance with the University's secure configuration process.

iii. Ensuring the operating System and applications are up to date.

f. Collect IT Network traffic flow logs and/or IT Network traffic to review and alert upon from the University's IT Network devices (IG2).

g. Deployment of a host-based intrusion prevention solution on the University's Assets, where appropriate and/or supported (IG3).

h. Deployment of an IT Network intrusion prevention solution, where appropriate (IG3).

i. Deployment of port-level access control. Port-level access control utilizes 802.1x, or similar IT Network access control protocols, such as certificates, and may incorporate User and/or device authentication (IG3).

j. Application layer filtering (IG3).

k. Tuning of security event alerting thresholds monthly at a minimum (IG3).

III. Penetration Testing Policy

The Central IT Department must communicate the requirements and processes for penetration testing to their campus community annually to engage in the shared responsibility of penetration testing. 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.

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 campus or institute CISO/DISL will establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the University (IG2). Penetration testing program characteristics include:

a. Scope, such an IT Network, web application, Application Programming Interface (API), hosted IT services, and physical premise controls.

b. Frequency.

c. Limitations, such as acceptable hours, and excluded attack types.

d. Point of contact information.

e. Remediation, such as how findings will be routed internally.

f. Retrospective requirements.

2. The campus or institute CISO/DISL will create a process to perform periodic external penetration tests based on program requirements, no less than annually (IG2).

a. External penetration testing must include University and environmental reconnaissance to detect exploitable information.

b. Penetration testing requires specialized skills and experience and must be conducted through a qualified party.

c. The testing may be clear box or opaque box with a clear box testing being a method that gives the tester access to the code of a product, while an opaque box testing method focuses on the external behavior of a product without considering its internal workings.

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

a. Remediate penetration test findings based on the University's policy for remediation scope and prioritization (IG2).

b. Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing (IG3).

c. Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box (IG3).

IV. 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 Network monitoring and defense and penetration testing as described in CIS Control 13 (Network Monitoring and Defense) and CIS Control 18 (Penetration Testing) 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. IT1516 – Information Technology Service Provider Management Application Software Security Management

l. IT4912 – Information Technology Secure Configuration 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/

____