THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0134 - System and Communication Protection	
Version: 1	**Effective Date: 10/01/2017**

IT0134 - System and Communication Protection

Objective:

To establish policy for developing and maintaining a Systems and Communication Protection program to ensure compliance with minimally acceptable requirements.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee including its campuses, institutes, and administration (University and/or Campuses).

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program that demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

A Campus may apply more stringent requirements than those documented in this policy provided they do not conflict with or lower the standards or requirements established by this or any other University policy.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University IT resources.

Policy:

Each of the University's Campuses must develop or adopt and adhere to a formal, documented program to ensure that, commensurate with risk, the confidentiality, availability, and integrity of information assets both in storage and during transmission are protected.

The program must protect and monitor information transmitted or received by critical information systems, and employ architectural designs, software, development techniques, and engineering principles that promote effective information security.

All policy related standards and procedures must be consistent with applicable laws, regulations, and guidance. This policy and all associated standards and procedures as well as their implementation effectiveness must be reviewed periodically and updated as needed

Mandatory Controls:

Mandatory security controls for information systems are University-wide controls that are required to be consistently designed, implemented, monitored, and assessed by all Campuses.

1. **Policy and Procedures** (SC-1): Each Campus must develop or adopt and maintain a system and communication protection program for critical information systems that includes the implementation of this policy and associated controls, and an annual review of that program.
2. **Denial of Service Protection** (SC-5): Each Campus must assess the risk of denial of service attacks to critical information systems and ensure that those risks are adequately addressed.
3. **Boundary Protection** (SC-7): Each Campus must:
   a. Establish and monitor the external and key internal boundaries of critical information systems.
   b. Ensure that critical information systems deny network traffic by default and allow approved network traffic (i.e. deny all, permit by exception).
   c. Appropriately protect against the unauthorized release of information or unauthorized communication through the boundary protection mechanisms.
4. **Cryptographic Key Management** (SC-12): Each Campus must ensure that when encryption is required within critical information systems, cryptographic keys are appropriately protected.
5. **Collaborative Computing** (SC-15): Each Campus must ensure that critical information systems prohibit the remote activation of collaborative computing mechanisms (e.g. cameras, microphones, conferencing software, etc.) without an explicit indication of use to local users.
6. **Secure Name/Address Resolution Service (Authoritative Source)** (SC-20): Each Campus must ensure that the name/address resolution service provides appropriate additional data origin and integrity artifacts (e.g. digital signatures, etc.) along with the authoritative data it returns in response to queries.
7. **Secure Name/Address Resolution Service (Recursive or Caching Resolver)** (SC-21): Each Campus must ensure that name/address resolution services on the local clients of critical information systems perform data origin authentication and data integrity verification on resolutions received from authoritative sources.
8. **Architecture and Provisioning for Name/Address Resolution Service** (SC-22): Each Campus must ensure that the information systems that collectively

provide name/address resolution services are appropriately resilient (fault-tolerant).

Discretionary Controls:

Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

References:

1. NIST 800-53 "*Recommended Security Controls for Federal Information Systems and Organizations*"

Definitions:

1. **Flaw Remediation** - Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.
2. **Malicious Code** - Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography.

Last Reviewed: August 1, 2017