THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0120 - Secure Network Infrastructure	
Version: 2	**Effective Date: 10/01/2017**

IT0120 - Secure Network Infrastructure

Objective:

The University of Tennessee must protect its network infrastructure to accomplish its mission of teaching, learning, research, and public service. This policy provides the basis for the creation and maintenance of a secure network infrastructure.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee System 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 individual or position should be at a high enough organizational level to allow him/her/it to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program which 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 resources.

Policy:

1. General Policy
   a. The network infrastructure of each Campus is the responsibility of the position of authority for information technology (IT Authority) at that Campus.
   b. This policy covers the University network and all networks, devices, and services connected to the University network. Refer to the University Acceptable Use Policy for further restrictions and exceptions.
   c. This policy applies to construction and renovation projects involving network infrastructure, and the Campus IT Authority must be consulted for project related network requirements.
   d. Campuses may deploy standards, procedures, and controls to address specific or unique requirements.
   e. Each Campus must develop or adopt a disaster recovery and emergency response plan covering its critical network infrastructure. The development of the plan must include input from the information custodians and the Chief Business Officer at each Campus.
2. Network Wiring
   a. The connectivity infrastructure, wired and wireless, is the responsibility of each Campus' Information Technology organization and must only be

installed and maintained by or under the direct supervision of the Campus IT Authority.

b. Access to communications infrastructure must be limited to appropriate and approved personnel. Where reasonable, communications equipment should be housed in dedicated enclosures.
c. The requirements and design of appropriate space for data communication enclosures in new construction and renovations is the responsibility of the Campus IT Authority.
d. Data communications enclosures and infrastructure must be accessible to appropriate personnel 24x7x365.

3. Monitoring and Maintenance
   a. Network infrastructure components must be maintained at a reasonable operational and security level. Each Campus must develop or adopt a program for maintaining the hardware and software currency of these components including an equipment refresh cycle that is in accordance with industry standards related to end-of-life timeframes.
   b. Each Campus' information technology organization will monitor and maintain the availability and integrity of the network infrastructure.
   c. Each Campus must develop or adopt a network event logging and management strategy. Critical network components must log significant events.
   d. Each Campus must develop or adopt a sparing strategy that accounts for the critical network infrastructure.
   e. Each Campus must develop or adopt a strategy that provides sufficient time on a regular basis to maintain the communications infrastructure.
   f. Administrative access to network components must utilize secure access methods. In cases where insecure protocols must be used, documented compensating controls must be in place.
   g. All back-ups of network infrastructure devices must be secured at the same level as the primary device.

4. Related Services
   a. Each Campus IT organization will establish and maintain a program to control its Internet Protocol (IP) network address space including both dynamic and static addressing.
   b. Each Campus IT organization will establish and maintain a program to control its Domain Name System (DNS)..
   c. Each Campus IT organization will establish and maintain a process to evaluate requests for non-standard solutions.

References:

1. University of Tennessee Policy IT0110 – Acceptable Use of Information Technology Resources

Definitions: n/a

Last Reviewed: March 11, 2015