

Secure Network Equipment and Wiring Policy IT0120

This document describes guidelines for creation and maintenance of a secure information systems infrastructure

FINAL DRAFT – 8/7/2007

Objective

Protection of the network infrastructure at the University of Tennessee is necessary in order to assist the university in effectively achieving its mission of teaching, learning, research, and public service. This policy provides the requirements for creation and maintenance of a secure information systems infrastructure, including both wired and wireless technologies, necessary to protect the confidentiality, integrity, and availability of the university's information and information systems. These requirements include technical, administrative, maintenance, computer systems refresh, and operations solutions for information technology (IT) network infrastructure security.

This best practice applies to all students, faculty, staff, and others, referred to as "users" throughout this policy, while accessing, using, or handling the university's IT resources. In this policy, "users" includes but is not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities that are granted access as defined in Acceptable Use of Information Technology Resources Policy (IT0110).

Definitions

Position of Authority for Information Systems for Each Respective Campus, Institute, School, Division, or Unit (The POA list can be found at <http://security.tennessee.edu/>) – The person assigned by each respective campus chancellor or institute vice-president as the information systems authority for that respective location. As a part of being the information systems authority, this position is responsible for the creation of procedures and guidelines that define the implementation of information systems security policies and best practices at the respective location. The Position of Authority for Information Systems at each respective location will include a representative from each of the following university campuses/institutes:

- Chattanooga Campus
- Health Sciences Center
- Knoxville Campus
- Martin Campus
- Institute of Agriculture
- Institute for Public Service
- Space Institute

Network Infrastructure – Refers to the physical architecture in terms of equipment and connections that comprise a network. It includes fixed equipment consisting of wireless transceivers, routers, antennas, switches, cabling, management information systems, and other equipment. This does not include workstations, printers, or file, print, or application servers.

Policies and Best Practices

University policies mentioned in this document can be found from the *University of Tennessee System Policy Search Page* at <http://www.tennessee.edu/policy/>. Best practice documents are referenced from the *Information Security Office* home page at <http://security.tennessee.edu/>.

Compliance

Individual areas (e.g. campuses or institutes, departments, colleges and divisions) within the university system may define specific IT security requirements, guidelines, and standards as long as the documents do not detract from the university's Information Technology Security Strategy, policies, or best practices. The university's Information Technology Security Strategy, policies, and best practices will supersede such documents where inconsistencies exist.

Any non-compliance of the university's Information Technology Security Strategy, policies, or best practices must be reported to the ISO. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. Reference the Information Technology Acceptable Use of Information Technology Resources Policy (IT0110) for information concerning the escalation of non-compliance issues.

Exceptions

Policies and best practices are management instructions indicating a course of action. Compliance with the university's Information Technology Security Strategy, policies, and best practices are mandatory. In some instances, exceptions to policies and best practices must be made due to extenuating circumstances. Such exceptions must be documented and approved prior to implementation. To provide for "a standard way of doing non-standard things", the university will provide a process for reviewing and approving/disapproving requests for exceptions. This process shall be created and maintained by the ISO for the University of Tennessee. Instructions for requesting an exception can be found at <http://security.tennessee.edu/>.

General Policy

1. The entire network infrastructure of each campus or institute will be the responsibility of the POA or their designee.
2. The Information Security Office (ISO) will be responsible for validating the secure design of the university's network infrastructure. The ISO will also

monitor the network infrastructure and provide information to the POA or their designee concerning all vulnerabilities.

3. All network infrastructure components should be maintained at an optimal operational and secure level. Components that are older and have out-of-date revision levels are a high security risk and operate at a suboptimal level. The POA or their designee should develop a plan that meets the needs of each respective campus or institute for maintaining a reasonably recent version of these components. An equipment refresh cycle should be developed by the POA or their designee in conjunction with the lead financial entity at the respective campus or institute that is in accordance with industry standards as well as IT security best practices related to the end-of-life timeframes of network infrastructure components.
4. This policy covers all wiring and electronic devices from the wall outlet inward to the campus or institute core network. In addition, certain devices outside the wall-outlet-to-core region including all university subscribed services (e.g., dial-in servers, DSL, and cable modems for example) are also subject to this policy.
5. Wireless networks are an important part of the network infrastructure and have specific security requirements. These requirements are to be defined in the Secure Network Infrastructure Best Practice.
6. A customized network infrastructure plan that defines technical, operational, and security elements should be presented, maintained, and updated prior to each major upgrade of the network infrastructure by the POA or their designee. This plan will serve as the blueprint for implementation and budget purposes.
7. A disaster recovery and emergency response plan should be in place for all critical elements of the network infrastructure for each campus or institute. The development of the plan should include input from the information custodians and the lead financial entities at each campus or institute.
8. This policy applies to all planning for facility construction projects involving network infrastructure components, whether new facilities or remodeling of existing facilities. The POA or their designee should be consulted concerning specific network infrastructure requirements in all cases.

Network Wiring

9. Due to the sensitive nature of the wiring required for information systems, installation and maintenance of all wiring is the sole responsibility of the central information systems entity at each respective campus or institute. Wiring should not be installed by divisional faculty, staff, or students. Wiring should not be installed by third party contractors hired by a unit without the express consent of, and under the direct supervision of, the POA.
10. It is the responsibility of the campus or institute, college, or department to provide appropriate space for the data communications closet in the design of any new building and renovations of existing facilities. Dedicated, secure

communications closets are critical to the physical security of the campus or institute network. Due to the critical nature and physical security protection requirements of the equipment, all existing data communication closets must be dedicated to data communications, monitoring, telephone equipment, and electrical panels already installed in this space. The space must not be used for housekeeping, storage space, or any other use.

11. All new wiring installations, including those involved in renovation of building(s), must adhere to low voltage industry standards as specified in the **BUILDING INDUSTRY CONSULTING SERVICE INTERNATIONAL (BICSI)** practices.
12. The POA or their designee will oversee the installation of unique locks for data communications closets to limit unauthorized access to this space and to prevent unauthorized personnel from making wiring changes.

Monitoring, Maintenance, and Repair of Defective Components

13. The POA will maintain all active network infrastructure components. This will allow for expeditious problem detection and the repair or replacement of failing devices as well as the review of potential security incidents.
14. After-hours access to data communications closets must be provided to selected information systems personnel so that failing components can be repaired or replaced and/or the resolution of security incidents can be expedited.
15. A defined plan for spare components should be created and implemented by the POA for all critical components of the network infrastructure.
16. All network infrastructure devices should be maintained at the most recent stable code levels that provide the highest required level of security. The POA should be consulted if assistance is required to determine the appropriate code level for network infrastructure devices.
17. There should be a pre-determined maintenance window established for all network infrastructure devices that provides a defined time to maintain the hardware and software updates.

Related Services

18. The POA will control network address management at each respective campus or institute. This should be done via a dynamic assignment process with static addressing provided as necessary.
19. The POA will control Domain Name System (DNS) management at each respective campus or institute.

Network Infrastructure Device Control

21. All network infrastructure devices should have logging capabilities enabled for administrative and management access to record all access attempts, both successful and unsuccessful.

22. All network infrastructure devices should have a secure password methodology for access that is based on the Password Best Practice. All network infrastructure devices must be designed, tested, and controlled to prevent the retrieval of stored passwords.
23. All network infrastructure devices should be restricted to secure communications protocols for administrative and/or maintenance access. In cases where insecure protocols must be used, compensating controls must be in place and documented by the POA or their designee. The ISO will be the approving authority for the appropriate compensating controls for access to network infrastructure devices.
24. All back-ups for network infrastructure devices must be secured at the same level as the primary device.