ITS POLICIES AND GUIDELINES
CATEGORY: Information Technology, Security
STATUS: In Review

POLICY TITLE: **Network Policy**

POLICY PURPOSE:
The purpose of network policy is to:

- Define a procedure that ensures secure, reliable, and sufficient network capacity to all campus users through a review of specialty devices prior to their deployment on the University network.
- Define a procedure to mitigate unauthorized network disruption, system failure, or data corruption on the University network.
- Define a common naming standard for all attached devices.

Truman's data network is a critical resource shared by all campus units: it provides the means to communicate both within the University and via the Internet to the rest of the world. The introduction of devices that might affect the behavior or performance of the network without proper planning for security and performance requirements has the potential of resulting in disruption of services to everyone on campus.

Additionally, connected devices are required to follow a common naming standard. This standard ensures that devices are properly identified and categorized, can be traced to a physical location, and are properly managed by University systems.

APPLIES TO:

- All members of the Truman State University community
- Anyone granted access to Truman State University data, systems or networks

---

CONTENTS:

POLICY STATEMENT:

Specialty Device Approval Process
The addition to the University network of specialty devices that could be foreseen to pose a threat to the network's performance or security must be approved prior to their introduction. In most circumstances this approval process will take place at the time of purchase as defined in the Hardware and Software Acquisition Review Policy.

Anyone planning to add a specialty device that alters the topology of the network or places unusually high demands on the network must submit a Help Desk request for approval to add the specialty device. The Technical Director will review the submitted request and reply to the Help Desk request, possibly with

stipulations about how the addition must be configured. If the request is approved, the device may be added to the network as approved, in accordance with Truman's Acceptable Use Policy.

Removal of disruptive devices from the University Network

The security, reliability, and performance of the University network are important to the accomplishment of the University's mission. Therefore, if any device on the network is found to compromise and affect any aspect of the network's operation, ITS must be able to quickly contact the appropriate campus unit or individual who can take action. If the disruption is an immediate security concern or is affecting other user's ability to use the network then ITS will notify the appropriate campus unit or individual and block the offending device immediately. If the disruption is not a security concern and is not affecting others, notification of the disruption will be sent to the campus unit or individual. If a response is not received within four hours indicating that the campus unit or individual is taking action to mitigate the disruption, the offending device will then be blocked or isolated until a response is received. In either case, ITS will work with the campus unit or individual to ensure that the device is properly configured. If a block (or isolation) has been put in place, it will be removed when ITS is assured that the device is up to accepted standards of operation.

Device Naming Standards

All devices connected to the University network are required to follow a common naming standard. ITS may notify campus units or individuals regarding misnamed devices. If a response is not received the device may be subject to removal from the University network.

The device naming standard is an eight to nine character code. The first two characters designate the building location. These codes are documented on the ITS Website in the Device Naming Standards and Building Code Document.

The next three or four characters are the office or room number. The device type designator follows this with L for a laptop, N for a netbook and P for a printer. The final two or three characters are the computer number. If there is only one device or computer in the room then the device number is 001. If there are multiple devices, the first device is 001, the next is 002, 003, etc. (if you have a 4 digit office number, use a 2 digit number here)

Device Naming Example: If you reside in Dobson Hall room 301 and both you and your roommate have computers, one should be named DH301001 and the other should be named DH301002.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Exclusions to the device naming standards may be granted for resources maintained by campus units that provide services to others within the unit or for devices that will have the name published or accessible to the office campus community. For example, a departmental research server that collaborates with off campus individuals may prefer to have a specific device name rather than publishing a name with the device's specific location. The Technical Director of ITS or their designate can grant these exclusions.

Appeals for Specialty Devices

If a request to deploy a specialty device is denied, the requestor may appeal the decision to the Chief Information Officer. The Chief Information Officer may seek the recommendation of the Information Technology Services Advisory Committee and may also consult with the users and the Technical Director and/or his designee(s).

Any exceptions to this policy must be approved in writing by ITS (see contact information below).

CONSEQUENCES:

By failing to abide by this policy or policy procedures, individuals may be subject to sanctions, up to and including the loss of computer or network privileges, disciplinary action, suspension, termination of employment, dismissal from the University, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

CONTACTS:

Responsible Executive:	Provost and Vice President for Academic Affairs
Responsible Office:	Information Technology Services
Contact:	Chief Information Officer 111 McClain 660-785-4163
APPROVED BY:	Truman State University President / Board of Governors
APPROVED ON:	July 11, 2012
EFFECTIVE ON:	July 11, 2012
REVIEW/CHANGE HISTORY:	
REVIEW CYCLE:	As Needed

DEFINITIONS:

ITS – Information Technology Services

Devices — Hardware components or software services running on common desktop or server machines that communicate over Truman's local area network

Specialty Device — A specialty device is defined as any non-standard device, any device that provides a dedicated networking function or provides a special service. These devices could include, but are not limited to networking switches, wireless access points, network attached storage devices, network attached cameras. These devices would not include standard configured computer systems.

Accepted Standards of Operation — Defines normal operating usage by a device on the University network. A device meeting any of the following criteria will be considered in violation.

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service.
- The unauthorized use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- Any device generating a significantly larger then normal amount of network traffic..

RELATED DOCUMENTS:

KEYWORDS: