Overview

The UTHSC considers all electronic information transported over the UTHSC network to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as private and confidential. Any inspection of electronic files, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by University policies.

All mission critical servers and applications should have proactive monitoring tools installed to assure bandwidth, CPU usage, RAM, Disk Space, Virus Protection, etc.

Purpose

The purpose of this document is to outline the UTHSC policy regarding the monitoring, logging and retention of network packets that traverse the Campus Network Backbone.

The goals of this policy are:

A. To maintain the integrity and security of the University's network infrastructure and information assets

B. To collect information to be used in network design, engineering, troubleshooting, maintenance and usage-based accounting

C. Maximize uptime and maintenance of PHI and mission critical servers and applications.

Scope

This addendum applies to all users of UTHSC information resources over networks that cause traffic to traverse the Campus Network Backbone. The policy extends from the Network Access Point (NAP) to the end-user machine.

Policy

- ❑ Monitoring network traffic at the UTHSC will involve only the collection of packet header information, not the packet data, unless required to check for viruses, to monitor the improper release of confidential patient, employee or student information, or for intruder detection.

- ❑ Only the UTHSC Network Team is authorized to routinely monitor traffic on the network backbone.

- ❑ The use of sniffers or devices which operate in promiscuous mode are to be used only by the authorized UTHSC network administrator for diagnostic purposes of intranet traffic only.

- Users must respect other users' rights to privacy and must not intercept nor attempt
- to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

- Personnel authorized to analyze the network backbone will not disclose any information realized in the process without approval of appropriate authority.

- Operating system and third party monitoring tools shall be implemented on all servers and applications deemed mission critical and setup to proactively monitor critical processes.

Enforcement

Reference **Enforcement** in Acceptable Use document.

Additional Information

Any inquiries relating to this Monitoring Policy should be directed to the Security Director.