Network Monitoring Policy

1.0 Purpose

The purpose of this document is to outline the Lawrence Technological University policy regarding the monitoring, logging and retention of network packets that traverse the University’s network or Internet connection.

The goals of this policy are:
1. To maintain the integrity and security of the University’s network infrastructure and information assets.
2. To collect information to be used in network design, engineering, troubleshooting, maintenance, planning and monitoring.
3. Maximize uptime and maintenance of mission critical servers and applications.

2.0 Scope

This policy applies to all users and devices connected to the Lawrence Technological University network that cause traffic to traverse the University’s network and Internet connection.

3.0 Policy Statement

Although the University does not generally monitor or restrict the content of material transported across networks, it reserves the right to access and review all aspects of its computing systems and networks, including individual login sessions and account files, to investigate performance or system problems, search for viruses and other harmful programs, or upon reasonable cause to determine if a user is violating a University policy or state or federal laws.

3.1 Guidelines

- All computer and communication devices connected to the Lawrence Technological University network are subject to this monitoring, whether or not they are owned or operated by the University.
- Only the Lawrence Technological University network team or parties approved by the Executive Director of Information Services are authorized to routinely monitor traffic on the University's network and Internet connection.
- Monitoring network traffic at the Lawrence Technological University will involve only the collection of information required to check for viruses, to monitor the improper use of computer resources, unauthorized access to sensitive data, or for intruder detection.
- The uses of sniffers or devices which operate in promiscuous mode are to be used only under the authority of the Lawrence Technological University network team for diagnostic purposes of university network traffic.
- 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 University network and Internet connection will not disclose any information realized in the process without approval of Executive Director of Information Technology Services.
Operating system and third party monitoring tools may be implemented on appropriate network equipment, servers and applications deemed mission critical and setup to proactively monitor critical processes.

Monitored data and usage logs will not be stored past the period of active investigation or needed for analysis. The network group stores incident related data as required. Unrelated monitored data may not be stored by anyone except as required by law. The network group may store aggregated data and usage logs for operational, compliance, and statistical purposes. Usage logs must be purged as per campus policies.