Network Devices Security

1.0 Purpose

This document describes a required minimal security configuration for all switches and other network devices connecting to a production network or used in a production capacity at Lawrence Technological University.

2.0 Scope

All switches and other devices connected to the Lawrence Technological University production network fall under the scope of this policy. Routers and switches within internal, secured labs, test or laboratory networks, shall not be connected to the Lawrence Technological University network without prior authorization from the Executive Director of Information Technology Services.

3.0 Policy Statement

The Information Technology Services Department (or any vendor approved by the Executive Director of Information Technology Services) has sole authority to access, and takes full responsibility for, all network devices and their configurations. Information Technology Services reserves the right to approve or remove any device connected to the Lawrence Technological University production network.

- All switches must be rack mounted.
- All access points must be wall or ceiling mounted with brackets.
- Switches left in public areas (by departments, faculty, etc.) will not be the responsibility of the Information Technology Services Department.
- Access to network devices will utilize Simple Network Management Protocol (SNMP) v1–3. This protocol utilizes a shared key encryption standard and is the current and preferred version. Legacy devices incompatible with SNMP v1–3 will not be covered by this protocol. These devices should be replaced within a reasonable timeline as departmental budgets allow.
- Firmware updates will be applied, within a reasonable time frame, as they become available and tested and will not cause other problems.
- Remote authorization will only be granted if specifically approved by the Executive Director of Information Technology Services.
- Each network device must have a Login Banner which states: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."
- All changes to routers must go through the Change Control process.