Router Security Policy

1.0 Purpose

This document describes a required minimal security configuration for all routers connecting to the Lawrence Technological University production network.

2.0 Scope

All routers connected to Lawrence Technological University production networks are covered under this policy. Routers within internal, secured labs are not affected.

3.0 Policy Statement

The Edward Donley Computer Center (EDCC) staff of the Information Services department is responsible for installing, managing, monitoring and auditing of all routers connected to the Lawrence Technology University production network. Information Technology Services reserves the right to remove any router connected to the Lawrence Technological University production network that was not installed by the EDDC staff.

Every router must meet the following configuration standards:

- The enable password on the router must be kept in a secure encrypted form.
- Disallow the following:
  - IP directed broadcasts
  - Incoming packets at the router sourced with invalid addresses such as RFC1918 address
  - TCP small services
  - UDP small services
  - All source routing
  - All web services running on router
- Use University standardized SNMP community strings.
- Access rules are to be added as business needs arise.
- The router must be included in the University enterprise management system with a designated point of contact.
- Firmware updates will be applied, within a reasonable time frame, as they become available and tested and will not cause other problems.
- 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.