Network and Wiring Closet Access Policy

1.0 Purpose

The purpose of this policy is to establish standards for securing the Lawrence Technological University network and wiring closets. Effective implementation of this policy will minimize unauthorized access to the University network and wiring closets and provide more effective physical access controls.

2.0 Scope

This policy applies to students, faculty, employees, contractors, consultants, temporaries, and other workers at Lawrence Technological University, including all personnel affiliated with third parties who require access to the Lawrence Technological University network and wiring closets.

3.0 Policy Statement

Access to the Lawrence Technological University network and wiring closets is restricted to the Information Technology staff and authorized personnel.

3.1 Ownership and Responsibilities

The Information Technology staff is responsible for the safety and security of the network equipment located in the network and wiring closets.

3.2 Guidelines

- Wherever possible network devices should be located in a secure and/or locked network and wiring closet. If this is not possible, then network equipment and wiring should be housed in a locked cabinet.
- Physical access to network and wiring closets should be restricted to authorized Lawrence Technological University personnel.
- Physical access to network cabinets is restricted to Information Technology staff or others approved by the Executive Director of Information Technology Services.
- Network and wiring closets should have appropriate environmental controls, including air handling, uninterruptible power protection (UPS) & conditioning, and fire suppression.