Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to the Lawrence Technological University network. A Virtual Private Network (VPN) provides a secure encrypted network connection over the Internet between an individual and a private network. By utilizing the public Internet for transporting data, a VPN provides a low cost solution for secure remote access or connectivity. Use of VPN allows members of the Lawrence Technological University community to access Lawrence Technological University network resources as if they were on the campus.

2.0 Scope

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

3.0 Policy Statement

Lawrence Technological University students, faculty, employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties may utilize the benefits of the VPN to access University computing resources to which they have been granted access. Individual users are responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

1. It is the responsibility of employees and students with VPN privileges to ensure that unauthorized users are not allowed access to Lawrence Technological University internal networks.

2. All computers connected to Lawrence Technological University internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard and be up-to-date on available Operating System patches. This includes personal computers as well as university owned computers.

3. VPN users who have an idle connection will automatically be disconnected after 10 minutes. Users must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

4. VPN users who have an active connection will automatically be disconnected after 6 hours. Users must then logon again to reconnect to the network.

5. All individuals and machines using VPN technology, including university owned and personal equipment, are a de facto extension of Lawrence Technological University’s network, and as such are subject to the University’s computing policies.

6. Only VPN clients approved by the Lawrence Technological University Information Systems department may be used to access the Lawrence Technological University computing network.
7. VPN gateways are set up and managed by the Lawrence Technological University Information Technology department. No other department may implement VPN services unless approved by the Executive Director of Information Technology Services.

8. VPN software and support is available through the Lawrence Technological University Information Systems Help Desk.