LEE COLLEGE

Virtual Private Network (VPN) Policy: Information Technology

1.0 Introduction

In an effort to increase the security of Lee College's information technology systems, off-campus access to many information technology resources has been limited. Lee College offers Virtual Private Network (VPN) access for faculty/staff (hereinafter users) who need access to information technology systems that are not available to users from off-campus networks. Exceptions to the approved list of users will be considered on a case-by-case basis. The Supervisor and Cabinet Officer will approve the list of users.

2.0 Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to Lee College's internal network. Lee College's VPN server is designed to provide secure/encrypted access to network resources on the Lee College Network. Using the VPN server to access Internet resources external to Lee College is not recommended.

3.0 Policy

3.1 VPN access will be set up and managed only by the Lee College Information Technology Data Center Network Specialists.

3.2 Approved users' laptops will be configured with the VPN client software by Lee College Information Technology technicians.

3.3 Only VPN client software that is approved by and/or distributed by Information Technology networking services may be used to connect to the Lee College VPN concentrators.

3.4 By using VPN technology with personal equipment, users must understand that their machines are an extension of Lee College's network, and as such must comply with Lee College's Information Technology policies.

3.5 VPN provides secure access into the Lee College network. VPN does not, by itself, provide Internet connectivity. Users are responsible for providing their own Internet service.

3.6 Currently VPN software latest Microsoft Windows and Mac operating systems. Approved users are responsible for the installation of the VPN software. For assistance, contact the myLC Help Desk.

3.7 It is the responsibility of the users with VPN privileges to ensure that unauthorized persons are not allowed access to Lee College internal networks.

3.8 Lee College has configured the VPN service to not allow the bridging of networks (split tunneling). As a result, when connected to VPN, all network traffic from the users' computer will travel through the Lee College network, which will not allow communication back to a device on the private network other than the computer making the original connection.

3.9 All computers, including personal computers, connected to Lee College's internal networks via VPN or any other technology must use the most up-to-date anti-virus software.

3.10 VPN users will be automatically disconnected from Lee College's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes should not be used to keep the connection open.

3.11 VPN sessions are limited to a total connection time of twelve hours per session.

3.12 Only approved users with signatures from the Supervisor and Cabinet Officer with specific requirements for VPN access will be granted access to the resources.

4.0 Enforcement

Any user found to have violated this policy may be subject to loss of certain privileges or services, including but not limited to loss of VPN services.

By acceptance of VPN (virtual private network) access, I certify that I have read, understand and agree with the policy and procedures set forth in this document. Return signed document to the Information Technology office.

Requestor	Date
Executive Vice President	Date
Executive Director, IT / Chief Technology Officer	Date
Vice President, IT / Chief Information Officer	Date