VPN – Connecting to Colleague from Remote Locations (Off Campus)

Purpose

The purpose of this policy is to clearly list the user and system requirements to have remote access to computer services hosted at Lesley University. This would be the requirements for the user and the physical device (computer) that would be utilized to connect to the Lesley University VPN service.

Motivation

In order to access computing resources hosted at Lesley University from off-campus, use of LU remote access services is required. A remote access connection is a secured private network connection built on top of a public network, such as the Internet. Remote access provides a secure, encrypted connection, or tunnel, over the Internet between an individual computer (such as a computer off campus) and a private network (such as LU's).

Allowing such connections is not entirely without risk. Remote access connections, by definition, allow an outside computer to connect directly to the LU network. This arrangement provides convenience for the remote worker, but bypasses any firewall restrictions that may be in place. This risk is particularly pronounced for remote access connections from privately owned computers, as the University cannot ensure the computer has sufficient protection configured (e.g. anti-virus, anti-spyware). The risk posed by LU-owned computers is still present, but to a lesser degree.

Responsibilities

The Information Technology department (IT) is responsible for implementing and maintaining the University's remote access services. Therefore, IT is also responsible for activities relating to this policy. Hence, IT will manage the configuration of the University's remote access service (VPN).

Policy for Remote Access

LU employees, and authorized third parties (vendors, etc.) may, under some circumstances, utilize remote access to access LU computing resources for which they have been granted access.

Regular, full-time LU faculty or staff employees that have a valid LU Domain User Account may request remote access to the LU network by completing a ***Colleague Access Request Form***. This access request form must be signed off by your immediate supervisor. Requests not signed/approved by a department director will be returned to the requestor as incomplete. A copy of the Colleague Access Request Form may be found in the Technology Requests section of the IT intranet website (https://intranet.lesley.edu/it/).

Guidelines for Access:

- Temporary Accounts shall not be granted remote access.
- Students shall not be granted remote access.
- Faculty and Administrative accounts may be granted remote access.
- Vendor Accounts may be granted remote access. Vendor accounts are setup specifically for vendors to access LU resources for support purposes. Vendor accounts must be sponsored by an LU employee/department. The account sponsor bears responsibility for the account and its use

by the vendor. If the vendor account does not already exist, a request to establish one must be made at the same time remote access is requested.

Operational Procedures

In order to use remote access, you need a connection to the Internet from your off-campus location. LU does not provide you with an Internet connection, your Internet Service Provider does. While dialup Internet connections may utilize a remote access connection, performance is very slow and is not recommended or supported.

- Remote access users will be automatically disconnected from the LU network after 15 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes to keep the connection open are prohibited.
- There is no support for individuals utilizing the VPN for remote access to Colleague via their personal computer.
- If you have any questions related to the use of LU remote access, please contact the IT Help Desk at 800.999.1959 extension 8770 or it@lesley.edu.

Remote Access Terms of Use

Any user found to have violated the terms of use may be subject to loss of privileges or services and other disciplinary action.

1. It is the responsibility of all LU employees and authorized third parties with remote access privileges to ensure that unauthorized users are not allowed access to internal University networks and associated content.
2. All individuals and machines, including university-owned and personal equipment, are a de facto extension of LU's network, and as such are subject to the University's Acceptable Use Policy.
3. All computers connected to LU's internal network via remote access or any other technology must use;
    a. properly configured, up-to-date operating system. Last updated within 2 months.
    b. anti-virus and anti-malware software whereby virus definition files are not more than 1 week old.; this includes all personally-owned computers.
    c. It is recommended to use Internet Explorer for this connection.

    These guidelines will be evaluated and enforced. If your personal computer does not meet the requirements you will be denied access and will be responsible updating your personal computer.
4. Redistribution of the LU remote access installers or associated installation information is prohibited.
5. All network activity during a remote access session is subject to LU policies.
6. All users of the LU remote access services shall only utilize resources for which they have been granted permission and rights to use.