LENOIR-RHYNE UNIVERSITY

Policy and Procedure

Title: Virtual Private Network Policy

Division/Department: University Wide

Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to Lenoir Rhyne University's internal network. Lenoir Rhyne University's VPN server is designed to provide secure/encrypted access to network resources on the Lenoir Rhyne University Network. Using the VPN server to access Internet resources external to Lenoir Rhyne University is strongly discouraged.

Policy

Institutional data is information that supports the mission of Lenoir Rhyne University. Institutional data is considered a vital asset and is owned by the University. Due to the essential nature of institutional data, its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity. This policy sets forth the university's standards with regard to the handling and storing institutional data.

Procedure

- VPN gateways will be set up and managed only by the Office of Information Technology.
- Approved users laptops will be configured with the VPN client software by the Office of Information Technology.
- Only VPN client software that is approved by and/or distributed by the Office of Information Technology may be used to connect to the Lenoir Rhyne University VPN concentrators.
- By using VPN technology with personal equipment, users must understand that their machines are an extension of Lenoir Rhyne University's network, and as such must comply with Lenoir Rhyne University's Office of Information Technology Policies http://policies.lr.edu/administration-finance/IT.
- VPN provides secure access into the Lenoir Rhyne University Network. VPN does not, by itself, provide Internet connectivity. Users are responsible for providing their own Internet service via dial-up, cable modem, DSL, or other means to be able to use Lenoir Rhyne University's VPN service.
- It is the responsibility of the users with VPN privileges to ensure that unauthorized persons are not allowed access to Lenoir Rhyne University internal networks.
- Lenoir Rhyne University 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 Lenoir Rhyne University network which will not allow

communication back to a device on the private network other than the computer making the original connection.

- All computers, including personal computers, connected to Lenoir Rhyne University's internal networks via VPN or any other technology must use the most up-to-date anti-virus software approved by the University.
- VPN users will be automatically disconnected from Lenoir Rhyne University's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes should not be used to keep the connection open.
- Only one active VPN connection is allowed per user and the VPN concentrator is limited to a total connection time of 8 hours per user in one session.
- Enforcement - Any user found to have violated this policy may be subject to loss of VPN services.

Author of Policy:
Chief Information Officer

Individuals Affected:
All employees of the university

Reviewed By/Concurrence From

Chief Information Officer
VP for Finance and Administration

Approval

Chief Information Officer

1/8/2010

Approval Date

Developed On: 01/08/2010
Revised On: 01/26/2012

Note: Please review the policies available online at http://policies.lr.edu/ to confirm that this is the most recent version of the policy.