Approved 12/14/11

Virtual Private Network (VPN) Policy

Purpose 1
Scope 1
Terms and Definitions 1
Policy Statements 1
Enforcement 2
Related Documents 2

PURPOSE

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to access Texas Wesleyan's internal network. Texas Wesleyan's VPN server is designed to provide off-campus access to network resources available on the Texas Wesleyan campuses.

SCOPE

This policy applies to employees with demonstrated need to access resources internal to the university network.

TERMS AND DEFINITIONS

Virtual Private Network (VPN) is a method for accessing a remote network uses encryption and tunneling to connect users securely over a public network, usually the Internet.

POLICY STATEMENTS

VPN access will be enabled only via methods approved and managed by the Information Technology department.

All requests for VPN service begin with submitting a request to the Help Desk (helpdesk@txwes.edu) for installation.

By using the VPN technology, employees must understand that all VPN-connected devices are an extension of the Texas Wesleyan network, and as such are subjects to the same rules and policies that apply to university computers on campus.

Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any associated service issue. VPN services work best over broadband connections.

It is the responsibility of the employee with VPN privileges to ensure that unauthorized users are not allowed access to the Texas Wesleyan network.

All VPN services are to be used solely for the approved business/academic support purpose. All users are subject to auditing of VPN usage.

VPN users will be automatically disconnected from the Texas Wesleyan network after 30 minutes of inactivity.

All computers connected to the Texas Wesleyan network via VPN must use the university approved anti-virus software and are subject to scanning before establishing a connection.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

RELATED DOCUMENTS

Network Protection Policy