# Virtual Private Network (VPN) Policy

## Overview

Virtual Private Network (VPN) connections provide a convenient way for staff to access internal network resources remotely over the network. It also provides a mechanism for staff and vendors to provide support for applications and software remotely. Like any remote connection, they must be carefully managed and secured.

## Purpose

VPN connections are most commonly used for remote staff and vendor support functions. These connections provide secure tunnels allowing access to a remote network. This policy provides guidelines standards, and procedures for remotely accessing [LEP] internal network and systems.

## Scope

This policy applies to all [LEP] staff who access the network remotely using a VPN client.

## Policy

### GENERAL

Approved [LEP] staff may remotely connect to the [LEP] network and resources with appropriate approvals and business need. VPN technology provides an encrypted tunnel through a public network so information transmitted to and from systems are not easily readable by unauthorized parties.

Staff using VPN connections are responsible for their remote Internet Service Provider (ISP) and coordinating the installation of [LEP]-approved VPN software through [Insert Appropriate Department].

### REMOTE USER RESPONSIBILITIES

All staff using remote VPN access shall ensure the following operating environment and conditions:

* Staff using computers that are not [LEP]-owned equipment must configure the equipment to comply with [Insert Appropriate Department] policies as a condition of use
* Unauthorized users are not allowed access to [LEP] internal networks from the remote location
* Use is controlled using strong authentication mechanisms consisting of smartcard, two-factor, or a public/private key system with a strong passphrase
* Staff implementations force all traffic to and from the user workstation through the VPN tunnel and all other local and internet traffic shall be dropped
* Dual (split) tunneling is not permitted and only one network connection shall be allowed
* VPN gateways shall be set up and managed only by [Insert Appropriate Department]
* VPN users must understand that their personal machines are an extension of the [LEP] network, and as such are subject to the same rules and regulations that apply to [LEP]-owned equipment

### ADMINISTRATION AND MANAGEMENT RESPONSIBILITIES

[Insert Appropriate Department] shall ensure the following for all VPN users:

* All computers connected to via VPN or any other similar remote technology must use up-to-date [LEP] provided virus and malware protection software
* VPN users shall be automatically disconnected from [LEP] network after a specified period of inactivity.
* Support shall disallow pings or other artificial network processes to keep the connection open

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP]. Satisfactory examples of evidence and compliance include:

* Logs of authorized VPN users
* Anecdotal ticketing information showing compliance with this procedure
* Documented help and user documentation for remote VPN installations
* Archival communication documentation showing policy implementation

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff using, managing, or supporting VPN connections.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |