# Remote Access Policy

## Overview

Today’s computing environments often require out-of-office access to information resources. Remote access refers to the process of connecting to internal resources from an external source (home, hotel, district, or other public area). The ability to securely and reliably connect to business resources from a remote location increases productivity.

## Purpose

This policy defines standards for staff to connect to the [LEP] network from a remote location. These standards are designed to minimize potential exposures including loss of sensitive information, and limit exposure to security concerns through a consistent and standardized access method.

## Scope

This policy applies to all [LEP] staff that access, configure, manage, and support remote connectivity to the [LEP] network.

## Policy

The following policies and procedures apply to staff managing and using remote access:

* Staff shall contact the help desk for approved methods and software to remotely connect to [LEP] systems
* Staff accessing systems remotely are responsible for ensuring their mobile device is compliant with applicable [LEP] policy
* All devices shall be inspected be the [LEP] help desk prior to use to ensure the device is up to date with all applicable security patches and virus/malware protection software
* Users with remote access privileges shall ensure that their remote access connection is used explicitly for work business and used in a manner consistent with their on-site connection to the [LEP] network
* Secure remote access shall be strictly controlled
* Information security shall determine the appropriate access methodology and hardening technologies up to and including two factor password authentication, smart card, or PKI technology with strong passphrases
* All user passwords shall be strong and follow guidelines and procedures in the [LEP] Access Control and Password Policy
* Staff shall ensure that devices used for work purposes are not shared in a multi-user capacity, violate AUP conditions, or used in any inappropriate activity
* Users shall bear full responsibility for any access misuse
* [LEP] users with remote access privileges shall ensure their remotely connected workstation, does not bridge or share another private or public internet connection
* A home routed and firewalled, internal private network using network address translation (NAT) technology is excepted from this clause provided said network is under the complete control of the user
* Personal equipment shall not be used to connect to the [LEP] network using remote connection software and exceptions require [Insert Appropriate Role] written approval

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of [LEP] day-to-day processes. Examples of controls and procedures for policy compliance are as follows:

* Anecdotal historical evidence supporting policy implementation including help desk ticketing logs, electronic mail, exceptions, authorizations and other appropriate documentation
* Remote access logs documenting user and secured remote access to the [LEP] network
* Group security policy associated with remote access

## 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.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/10/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |