# Remote Access Policy

## Purpose

The purpose of this policy is to define standards for remotely connecting to Regent University's internal private network from either a host owned or managed by the university, or a privately owned host. These standards are designed to minimize potential exposure to Regent University from damages which may result from unauthorized use of Regent University resources. Damages include, but are not limited to the loss of sensitive or university confidential data, intellectual property, damage to public image, damage to critical Regent University internal systems, etc.

## Application

This policy applies to all Regent University faculty, staff, and other agents with a Regent University-owned or personally-owned computer or workstation used to connect to the Regent University network. Regent University provides remote access for the sole purpose of aiding remote faculty and staff in the completion of their Regent University employment responsibilities. This policy applies to remote access connections used to do work on behalf of Regent University including, but not limited to, reading or sending email, accessing files from private file servers, utilizing private/internal applications, and viewing other private/intranet resources. Remote access implementations governed by this policy include, but are not limited to, Virtual Private Network (VPN) clients and Secure Shell/Secure Copy/Secure FTP (SSH, SCP, SFTP) clients, etc.

Regent University provides remote access to authorized users only. Students, graduate assistants, vendors, contractors, temporary employees (full or part time), and other agents will not be provided access to Regent University’s internal private network for any reason without prior approval from both the petitioning party’s school dean or department head and the Vice President of Information Technology. Each request for access is reviewed on an individual basis. Regent University reserves the right to refuse access to any applicant at its sole discretion, without cause, and without regard to the applicant’s position within the university.

## Geographical Limitations

Any remote access user who desires to utilize their privileges from outside of the United States must receive prior approval before leaving the country. Each user is responsible for notifying, via Email or other written means, the IT Department of his/her plans no less than one week prior to departing. Within the written correspondence, users must include their travel destination, planned length of stay, and reasons for requiring remote access during international travel. Each case regarding remote access during international travel is evaluated separately. Regent University reserves the right to revoke remote access privileges for any user while the user resides, for any length of time, outside the United States. In cases where access has been revoked, the user’s access will be restored upon returning to the United States.

## Policy Provisions

It is the responsibility of Regent University faculty, staff, or other agents with remote access privileges to Regent University's private network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Regent University. As remote access is an extension of local systems access, all Regent University policies govern use from any and all remote connections.

Remote access users are prohibited from using Regent University as a primary Internet Service Provider (ISP). As such, remote connectivity to Regent University’s private network should be established on an ‘as needed’ basis. The Regent University faculty, staff, or other agent is responsible to ensure that unauthorized persons do not gain access to any device while remotely connected to Regent University’s private network. Remote users remain responsible to ensure that their use does not violate any Regent University policy, does not constitute illegal activities, or is not for the purpose of outside business interests. The Regent University faculty, staff, or other agent bears full responsibility for any consequences resulting from such misuse.

**Policy Enforcement**
Any faculty, staff, or other agent found to have violated any part of this policy or other university policies while having a remote connection will have their remote access immediately revoked and may be subject to disciplinary action, up to and including termination of employment and/or enrollment.

All users of Regent University's information systems, whether local or remote, may report university policy or law violations to their immediate supervisor, representative faculty or school personnel, or directly to the Information Technology Department at (757) 352-4076 or infosec@regent.edu.