

STCC Remote VPN Access Policy

Purpose:

The purpose of this policy is to regulate/restrict remote (off-campus) access to personally identifiable information (PII), sensitive, protected and/or non-public data on STCC administrative systems in order to protect such information from unauthorized disclosure.

Scope:

A Virtual Private Network (VPN) is a technique used to create a private and secure path from a remote computer located on a public network into a private network such as STCC's campus data network. The VPN service is limited to full-time staff and faculty who have obtained appropriate approvals and have met the provisions listed below. This policy applies to all approved network users desiring a VPN connection at the College.

General Provisions:

Employees granted VPN access privileges must use a college-owned computer that is configured, maintained and managed by the IT department and, configured with the STCC provided VPN application. Personally owned computers will not be allowed secure access to the College's IT resources that require VPN software.

Secure access to both GroupWise and Datatel WebAdvisor are currently available via the Internet without the need for VPN software and may be accessed from any computer. Use of any other third party services or software (e.g. GoToMyPC, PC Anywhere, etc.) to access the college's networks or computers is not permitted. Users must not attempt to bypass or circumvent any security mechanisms put in place by the IT Department and must protect all passwords/procedures involved in the remote access process. Employees will not allow unauthorized individuals (i.e. non-STCC employees, family members, etc.) to use college-owned equipment and/or to access secure STCC resources. Users must disable their STCC VPN session when it is not actively in use and must not store locally (save) sensitive information unless absolutely necessary and the data have been encrypted. Employee access will be reviewed/ renewed annually.

Use of the STCC VPN service is a privilege that comes with responsibilities for the user, including best practices outlined in the Family Educational Rights and Privacy Act of 1974 (FERPA), Mass. Regulation 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, the Payment Card Industry Data Security Standard (PCI DSS), and Gramm-Leach-Bliley Financial Services Modernization Act (GLB) guidelines.

Approval Process:

Access to the STCC VPN will be issued based on the ability to demonstrate work-related need and its use is limited to work-related purposes. Convenience alone will not be considered adequate justification. In addition to a completed STCC Property Pass, the IT Department also requires a VPN Request Form on file, signed by the employee/ vendor and their Dean or VP acknowledging the requirements/restrictions and penalties set forth in the policy.

Responsibilities of IT:

- Provide the VPN client software and instructions for using the VPN client on the employee's computer.
- Provide a method for granting employees access to the VPN service.
- "Scan" for unauthorized VPN connections and disable access of those devices.
- Provide end-user support for VPN issues only during normal business hours.
- IT will not support home computers.

Responsibilities of Users:

- VPN service is limited to those needing secure VPN remote access to resources located on the college's network.
- All users must utilize the STCC provided VPN service and the associated VPN client software.
- Any remote systems must have the VPN client's firewall feature enabled.
- A dedicated (employee is the only person who logs onto the machine) college-owned computer must be used in order to access the VPN.
- Authorized users with VPN privileges must ensure that their remote VPN access connection complies with the STCC Policy on Use of STCC Information Technology Resources (E-mail, Internet, and Related Hardware and Software) and treat it with the same consideration as an on-site connection to the college.

Users shall immediately notify Campus Police and the IT Department should any college-owned computer be lost or stolen or, should an employee suspect that a computer or other technology resource has been compromised in any way.

Additional Provisions for Vendors:

The College recognizes that at times a vendor under contract with the College, requires access to the College's systems for maintenance and/or upgrades. In such instances, special VPN access privileges will be granted, on a short-term basis. A unique VPN profile will be created with limited access, in order to complete required tasks. Upon completion of the tasks, the access will be terminated.

Any violation of this policy may result in the termination of secure remote access privileges and, depending upon the severity of the violation, may further result in disciplinary and/or legal action.

IT Steering Group reference: FY07-001 Remote Access Policy, completed date 06/26/2009