Remote Access Policy

Summary

Access to campus resources from home, a hotel, or other remote locations is an attractive alternative to campus computing. To ensure confidentiality, integrity, and availability we must protect CSU information assets regardless of where the user is physically located. Due to the risk of viruses and information or identity theft from an unsecured connection, remote access presents a risk to the network and to the user.

Purpose

The purpose of this policy is to define the applications and data accessible from remote locations and the acceptable methods for connecting to the CSU network to retrieve that data.

For the purpose of this policy, "remote computer" is defined as a computer that is not connected directly to the CSU network (wired or wireless). Examples include a CSU laptop being used in a hotel room, a user's personal computer being used in their home, or a CSU computer housed at a CSU satellite office without a direct connection to the CSU network.

CSU has a number of web-based applications that, by design, allow access from any location with an internet connection. CougarNet, CougarNet E-Mail, Internet Native Banner (INB), PeopleSoft HRMS, and NetStorage are examples of web- based applications. In addition, many systems offer remote access methods for administrative activities. The majority of these systems provide some level of encryption.

Policy

Users must authenticate to the VPN prior to accessing sensitive data or conducting administrative tasks from a remote computer. As an added layer of security, all corresponding activity must take place inside of a Remote Desktop or similar session.

- Sensitive data includes student records, human resource records, and financial data
- Related applications include INB, PeopleSoft HRMS, and various administrative utilities
- Administrative tasks include systems, application, or network administration.

Users may also utilize the VPN and Remote Desktop to access applications that are not web-based, provided they follow the related procedures.

Procedures and Responsibilities

User responsibilities

- Users must get approval for remote access from their department head. The department head must submit the request via eQuest. The Information Security Officer is responsible for approving requests.
- Users must sign a VPN User Agreement prior to first use and must abide by all CSU policies and federal, state, and local regulations.
- Users must not store sensitive CSU data on remote computers or removable media such as jump drives.
- Remote computers must run Windows XP or higher for Remote Desktop functionality.
- Remote computers must have antivirus software with daily updates and full system scans enabled.
- Remote computers must have the current operating system security patches, including those for Internet Explorer and other web browsers.

UITS responsibilities

- UITS technicians must securely configure a designated campus computer, typically the user's office computer, to accept a Remote Desktop connection.
- UITS is responsible for providing the user with VPN and Remote Desktop usage instructions and troubleshooting connection issues. While UITS technicians may not be able to troubleshoot personally owned computers, they will make every effort to help the user connect successfully.
- UITS is responsible for proper configuration and operation of the VPN from a network perspective.

Related USG Policy

5.8 Endpoint Security

Last Update

4/17/2014

Responsible Authority

Chief Information Security Officer