Approved Solutions for Working Remotely

Executive Summary

Telecommuting & remote-access offer increased access, flexibility, and mobility for those authorized to work remotely. However, insecure and informally or improperly implemented means of working remotely can negatively impact the Columbia College Computing Community.

Columbia College seeks to enable remote work via well-designed solutions ensuring the continuity of access, authorization, integrity, and confidentiality controls established for use of a given computing resource.

This document sets forth approved solutions for working remotely including:

- Terminal Services
- Offline Caches of Files, Folders, and Application Information
- SSH
- University and College Issued Mobile Devices
- Virtual Private Networking (VPN)
- Web Interfaces

Terminal Services

Columbia College recommends Terminal Services as its primary remote access solution for users requiring a Windows environment.

Terminal Services allow one to establish a remote connection to the College's Windows-based computing resources from a wide range of computing devices including Windows PCs, Macintosh PCs, UNIX PCs, and some mobile devices. Using Terminal Services, one may work remotely from most computers so long as internet access is available.

Users of Terminal Services may logon from any computing device to securely access a Windows session resembling one's typical computing workspace; one's files, shared network folders, preferences, settings, and access privileges are all available.

Within Terminal Services, applications run inside the server and information is exchanged between the remote client and the server using a low-bandwidth, "thin" protocol. When using the Remote Desktop Client, all application logic executes on the server and only screen updates, mouse movements and keystrokes are transmitted.

Information exchanged between the server and the remote client is encrypted. No information is stored on the remote client. Terminal Services offers an additional degree of safety in working remotely: disconnected sessions may be accessed again without loss of work within a specified time period.

For more on accessing Terminal Services, see: http://ccit.college.columbia.edu/ts.php

Offline Caches of Files, Folders, and Application Information

Users of portable CCIT managed Windows computing systems (e.g. laptops) may use offline files & folders or the offline settings of applications supporting offline information caches so as to access information normally available only via networked systems without connecting to the network.

CCIT managed systems are designed to maintain access, authorization, integrity, and confidentiality controls so as to protect information stored away for use offline.

SSH

For remote access to its Linux systems, Columbia College offers authorized users secure shell (ssh) access. SSH allows for logging into and executing commands on a networked computer via a secure, encrypted communications channel.

SSH can additionally be used for tunneling, forwarding arbitrary TCP ports so as to secure non-secure protocols, forwarding X11 connections, and transferring files.

Staff members with accounts on College Linux Systems may obtain off-campus SSH access by approval of Senior Management.

University Issued Mobile Devices

University issued mobile devices include, but are not limited to, Blackberrys, Treos, iPhones, Mobile Phones, or other smartphone or networked PDA devices. They may be an approved solution for use in working remotely so long as the following criteria are met:

1. The wireless device is University or College issued.
2. The device maintains the access, authorization, integrity, and confidentiality controls established for use of a given computing resource.
3. The device maintains end-to-end encryption of information transmitted.
4. The device maintains appropriate access controls to information stored on the device.
5. The user has the approval and authorization of senior management to use specified computing resources via the device.

All University issued mobile devices must be password-protected as per CUIT's Password Policy for smartphones: http://www.columbia.edu/cuit/newsletter/staff/smartphones-081006.html

Virtual Private Networking (VPN)

Users of portable CCIT managed computing systems (e.g. laptops) configured for VPN may utilize Columbia College's Virtual Private Network (VPN) option.

VPN is a good remote access option when users require access to computing resources not available to them via Citrix. VPN is typically a less attractive remote access option when compared to Citrix due to bandwidth considerations, the distance information must travel, and the quality of the telecommunication infrastructure between a person and the campus systems to which they are connecting.

A VPN works by using the shared public infrastructure (e.g. the internet) while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. Additional security procedures include authenticating the user, authenticating the system the user is using to connect to the network (the client system), and ensuring that the virus definition and security patches of the client system are up to date.

Because a VPN connection opens a privileged connection to sensitive computing resources, VPN access will only be issued according to the following criteria:

1. The user requesting VPN access has a genuine need for such access unmet through other remote access solutions.
2. The user has the approval and authorization of senior management to use the College's VPN solution.
3. The user has been issued a CCIT-managed computing system for VPN access.

Web Interfaces

Many applications offered by the University and CCIT provide web accessible functionality (i.e. a web interface).

Such applications may be used for remote work so long as they are approved for remote access and appropriate procedures or safeguards are followed.

Prior to offering a web application, CCIT will document necessary procedures and safeguards.

Examples of such procedures may include directions regarding the following:

a) how to verify the identity of the remote host
b) how to ensure one's session will be secure
c) how to log out
d) how to erase information cached by the browser used to access the web interface
e) how to destroy cookies associated with the web interface

Concerns Regarding Non-CCIT Managed Systems

Although the approved options for remote access reasonably address many risks incurred by remote-access options, some of the above approved options permit access via non-CCIT managed systems.

Prior to working remotely on a non-CCIT managed system, users should ensure that the system is reasonably secure:

- Anti-virus software is installed & active, definitions are up-to-date, and virus scans are performed regularly.
- Anti-spyware software is installed & active, definitions are up-to-date, and scans are performed regularly.
- System updates and security patches are installed and up-to-date.
- The trust one confers upon the owner of the system can equally be conferred to their use of the system.
- Prior to stepping away from the system, you logoff and close any remote access solution opened.

Non-Approved Options for Working Remotely

Non-approved options for working remotely include mechanisms that do not ensure access, authorization, integrity, and confidentiality controls similar or superior to those established for use of a given computing resource on-campus.

Non-approved options for working remotely include, but are not limited to the following:

- USB storage devices, floppy disks, CDs, or DVDs for storage and transit of information between College systems and non-College systems.
- Access to College computing resources by non CCIT-managed computing systems via mechanisms other than Terminal Services, SSH, or approved Web interfaces.
- The transfer of computing resources from College computing systems to non-college computing systems for purposes of working remotely. (e.g. indiscriminate forwarding of emails, transfer of files to external accounts)
- Remote desktop software permitting direct access to one's on-campus computer workstation. (e.g. VNC, PC Anywhere, GoToMyPC)

Relationship to Other Computing Policies

Telecommuting and remote-access is governed by the University's Telecommuting policy available at the following URL:

http://www.hr.columbia.edu/hr/policies/telecommuting/telecommuting/index.html