CALEDON
community
SERVICES

Remote Access Policy

Purpose:

The Remote Desktop Program (RDP) is restricted to full time and part time staff of Caledon Community Services (CCS).   RDP access allows time-sensitive work to be completed outside of regular working hours or from an alternate location in the event of an emergency. CCS aims to minimize the potential exposure to damages, such as the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, which may result from unauthorized use of its resources.

Policy:

The purpose of this policy is to define the procedures for connecting remotely to Caledon Community Services' network.

This policy applies to all Caledon Community Services employee's with access to and use of CCS owned or personally-owned computer or workstation used to connect to the CCS network.

This policy applies to remote access connections used to do work on behalf of CCS. Remote access implementations that are covered by this policy include, but are not limited to: frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

Definitions:

Remote Access: Any access to CCS's corporate network or cloud based programs through a non-CCS controlled network, device, or medium.

VPN Virtual Private Network (VPN): A method for accessing a remote network via "tunneling" through the Internet.

Procedures:

- Secure remote access to CCS network or cloud based programs must be authorized by the staff, volunteer, program/student placement's direct supervisor and approved by the Director of Finance and Infrastructure.

- It is the responsibility of CCS staff with remote access privileges to CCS' network or cloud based programs to ensure that their remote access connection is given the same consideration as the user's on-site connection to CCS.

- General access to the Internet for recreational use by immediate household members through the CCS Network on personal computers is not permitted for employees.

- At no time should any CCS employee provide their login or email password to anyone, not even family members.

- CCS employees and contractors with remote access privileges must ensure that their CCS owned or personal computer or workstation, which is remotely connected to CCS' network or cloud based programs, is not connected to any other network at the same time.

- CCS employees and contractors with remote access privileges to CCS' network must not use non CCS email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct CCS business, thereby ensuring that official business is never confused with personal business. For larger files that will not send through CCS email, employees should utilize 'drop box'

- All hosts that are connected to CCS' internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

- Personal equipment that is used to connect to CCS' network must meet the requirements of CCS owned equipment for remote access.
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Date Revised: July 2015

Date Approved: November 2015