



Password Policy

Purpose:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Caledon Community Service's entire corporate network. As such, all Caledon Community Services staff, volunteers, program/student placements and including contractors and vendors with access to Caledon Community Services systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Policy:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Procedures:

All system-level (administrative) passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed once every 120 days. The third party IT provider will provide these passwords to Caledon Community Service's CEO and Director of Finance and Infrastructure. They must be provided in a non-electronic form and saved in a secure, prearranged location.

All user-level (employee level or unique login personnel) passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days and can be recycled after one year has lapsed. Each employee will be prompted to change their password 5 days before the scheduled 120 days. Failure to do so within the time allotted will result in the user (employee) being locked out. If this occurs, a troubleshoot request form must be completed to have the password reset.

Troubleshoot will be promptly notified of all voluntary/involuntary terminations of staff, volunteers, program/student placements from CCS to ensure immediate termination of access to CCS network/individual resources.

All volunteer and student level: the Manager will change the department generic user name and password at a minimum of every 90 days or when a current volunteer/student completes their work with CCS. The Manager will then verbally communicate new password to all remaining active volunteers/students.

All client login level: Remain unchanged.

Passwords must not be inserted into email messages or other forms of electronic communication.

All passwords must conform to the guidelines described below:

Do not use the same password for CCS accounts as for other non-CCS access (e.g., personal ISP account, option trading, benefits, etc.). Staff must have separate passwords for each CCS required login.

Do not share Caledon Community Services passwords with anyone; including your direct supervisor or with members of the Resource Coordination Team.

All passwords are to be treated as sensitive, confidential Caledon Community Service information.

Do not use “remember password” feature.

If an account or a password is suspected to have been compromised, contact Finance and Infrastructure immediately using the IT/Troubleshoot Request Form.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REFERENCES:

IT/Troubleshoot Request Form

Staff Troubleshoot Email Procedure

IT Employee Deactivation Termination Form

Date Revised: July 2015

Date Approved: November 2015