Community Connections Support Services - Policies and Procedures

Section	**Technology Policy and Procedures**
Subject	**Technology & Information Security (tp030)**
Applies To	**Employees**
Revised Date	**April 2026**

Policy: Community Connections Support Services will take appropriate measures to preserve the confidentiality, integrity and availability of information; to support information security within the organization; and to maintain a secure IT environment. The agency provides a safe and secure environment for the collection, storage, access and retrieval of information. CCSS employees are required to handle information assets responsibly within their respective roles and in accordance with this policy.

Scope:

This policy applies to all CCSS employees, including teleworkers, volunteers and anyone who has permanent or temporary access to our systems, hardware and information.

Procedures:

Access Management

Depending on an employee's role at the agency, each employee will be granted authorized access to CCSS technology and information systems necessary to do their job. Access to data and systems will be granted based only on 'need to know' principles and in accordance with applicable privacy legislation.

All users are responsible for:

- Taking appropriate measures to prevent loss, damage, abuse, or unauthorized access to information assets under their control
- Secure storage, archival, and disposal of confidential documents in paper and portable media format in their custody
- Looking after any physical device (phones, computers, laptops, etc.) and access articles (keys, system IDs, passwords, etc.) assigned to them for the purposes of performing their job duties
- Respecting the classification of information as established by the agency and provincial privacy legislation
- Complying with all security requirements defined in this document and all supporting standards. Guidelines should be followed whenever possible. Procedures should be

followed, when available, to help improve compliance with policies, standards, and guidelines.

Information Storage and Authorization

CCSS stores all agency data on a cloud-based server accessed by using the NextCloud utility. NextCloud is encrypted both ways to protect data; meaning, connection to the server via NextCloud is encrypted from any shared device and is also encrypted back to all shared devices. Information stored on the server is classified in the following ways:

- **Public** – Information that is available to all employees and subcontractors (eg. Policy and Procedures Manual)
- **Internal** – Information that is relevant to the work of each service area (eg. forms, templates, health & safety information, etc)
- **Restricted** – Information that is accessible only to members of the Management Support Team (ie. business records, contracts, employee files)
- **Confidential and Regulated** – Records for the persons supported (eg. ISPs, Medical and legal records, etc)

Authorization for access to information is determined by the agency Directors and is based on the roles, responsibilities and job requirements of each employee. Server files can only be accessed by an employee if Directors directly share files with that employee or their device or that employee / subcontractor is provided with a link to access specific files. Authorization is granted as below:

- Management Support Team Members will be provided with agency-issued technology equipment and will be authorized to have access to:
  - Public information
  - Internal information
  - Restricted information
  - Confidential and Regulated information

- Staffed Living Support workers will have access to agency-issued technology equipment at their specified work site. Those devices will provide them access to:
  - Public information,
  - Internal information – only that internal information that is relevant to their role (eg. Staffed Living Forms and Health & Safety Officer records)
  - Confidential and Regulated – only those records specific to the person(s) they support.

- Community Support workers will be authorized to have access to the following information using their personal devices:
  - Public information,

  - Internal information – only that internal information that is relevant to their role will be shared (eg. Community Support Forms)
  - Confidential and Regulated – only those records specific to the person(s) supported in the local program will be shared.

- Home Share Coordinators will be provided with agency-issued technology equipment and will be authorized to have access to:
  - Public information,
  - Internal information – only that internal information that is relevant to their role will be shared (eg. Home Share Forms)
  - Confidential and Regulated – only those records specific to the person(s) supported in the program will be shared.

- Home Share Providers will be authorized to have access to the following information using their personal devices:
  - Public information only (eg. CCSS policy and procedures manual and agency reports)

Deactivation or De-Authorization

CCSS has clear and detailed operational workflows to follow when an employee leaves the agency to ensure that all access to information is deactivated for that employee and any technological equipment issued to that employee by the agency is reclaimed by the agency at time of employee exit.

Information Security

Two-factor authentication/Multi-factor authentication (2FA/MFA)

- 2FA/MFA is defined as requiring two or more independent factors to unlock a device or sign in: Something you know (password), Something you have (token, phone), or Something you are (biometrics)
- 2FA/MFA is required for all user accounts, including cloud-based services, VPNs, remote access, and systems handling sensitive data (e.g., financial, Personally Identifiable Information - PII).
- Authentication Methods & Requirements
  - Preferred Methods:
    - App-based push notifications: (e.g., Microsoft/Google Authenticator).
    - Hardware security keys: (e.g., YubiKey).
  - Permissible Secondary Factors:
    - Time-based one-time-password (TOTP) software tokens.
    - SMS/SMS-based codes (best used when stronger methods are not available).
  - Non-Preferred: Avoid relying solely on SMS for high-risk accounts.
- IT security must approve exceptions for systems that do not support 2FA.

Community Connections Support Services – Policies and Procedures

Server Security

- The CCSS server is encrypted;
- All server files are backed up using secure, offsite hard drives;
- The primary administrators are the Directors.
- There is a secondary external administrator to the server with full access, restore capability and capacity for IT support. Only when disaster recovery is necessary will the secondary administrator become active.

Keeping Emails Safe

Ensuring security of information sent or received via email is the responsibility of each employee. Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, employees must:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- Immediately delete any suspicious email.

Managing Passwords Properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should they be secure so they won't be easily hacked, but they should also remain secret. For this reason, employees are to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords semi-annually.

Transferring Data Securely

Transferring data introduces security risk. Employees must:

- Avoid transferring confidential and regulated data to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees must obtain authorization from the agency Directors prior to transfer.

- Share confidential data using the agency server, when possible.
- Password protect any document containing confidential and regulated information that is to be shared using email and only to authorized sources. The password to the document must be sent using a separate email.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies. All confidential and regulated data can only be shared after obtaining consent from the person to whom the data refers with the exception of CLBC and CCSS management.
- Temporarily store data on external media for purposes of transfer only with the authorization of CCSS management. External hard drives and other media such as personal laptop, USB flash drives, and CD/ DVDs are not appropriate storage locations for agency data beyond occasional and very short-term use. These devices are typically not enabled with the same safeguards as agency-issued devices and may be easily lost or compromised. Any and all information stored on temporary media must be deleted immediately after data transfer is complete.
- Report scams, privacy breaches and hacking attempts

Our agency needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the agency Directors. The Directors, or a designate will investigate promptly, resolve the issue and send an agency-wide alert when necessary.

Virus and Malware Protection

Up to date anti-virus software for the detection, removal and protection of suspected viruses should be installed on all servers, workstations, and laptops. Employees must follow their Continuous Quality Improvement (CQI) schedule activities and ensure that virus and malware protection is updated and scans are run monthly on any device that has access to CCSS information.

When installing or using software not provided by the agency, employees must ensure that the software is properly licensed. This also applies to copyrighted materials including music, pictures, videos, and movie files, as well as written media. If an employee installs software on an agency-issued device or uses external technology services, the employee must understand the associated risks (such as the trustworthiness of the author, download source, impact to information security, and system performance and reliability). The employee is responsible for managing these risks, including ensuring that the software or service is properly licensed and kept current with security patches. If the software has an auto-update function, it should be enabled.

Clear Desk; Clear Screen Practices

All employees are to adhere to clear desk; clear screen practices outlined below:

Clear desk

- Employees are required to ensure that all data in hardcopy or electronic form, including paper notebooks and printed sheets, and mass storage devices such as CDs, DVDs, and USB drives, must be removed from their desks or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access in their work area.
- This must be done at the end of the day and anytime an employee expects to be gone from their desk for an extended period (greater than 60 minutes) and when they vacate a meeting room or common area.
- Equipment is to be stored in a locked drawer/cupboard or a locked room to protect from unauthorized access. Employees are not to share or provide copies of keys to any unauthorized personnel.

Clear screen

- If the employee is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorization.
- PCs and tablets must be screen locked when a workspace is unoccupied.
- The workspace is to be locked if unoccupied for an extended period of time (longer than 60 minutes).
- File cabinets containing Confidential Data must be kept closed and locked when not in use or unattended.
- Keys for accessing drawers or filing cabinets should not be left on a desk.
- Passwords should never be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

Protection of shared facilities and equipment

- All whiteboards must be cleaned at the end of a meeting by the meeting facilitator.
- All waste paper which contains confidential and regulated data must be placed in the waste bin or shredded.
- Printers and fax machines should be treated with the same care under this policy:
  - Documents containing sensitive information must immediately be removed from printers, fax and copy machines.
  - When possible, the "Locked Print" functionality should be used.
  - All paperwork left over at the end of the work day will be properly disposed of.

Equipment or Physical Security

- Equipment must be protected, commensurate with its availability requirements, from power supply interruption and other disruptions caused by failures in supporting utilities.
- Power and telecommunications cabling must be protected from interception and damage.
- Equipment must be correctly maintained to enable continued availability and integrity.

- Equipment must be protected using security controls when off-site from the worksite. An example of a control could be that files or laptops are not to be left in unlocked cars or on seats where they are visible by passers-by.
- Information, records, and software must be protected against unauthorized disclosure during and subsequent to the reassignment or destruction of hardware and media.
- Equipment, information, or software belonging to or under the control of CCSS must not be destroyed without prior authorization from CCSS Directors.

Monitoring and Oversight

It is not the agency's regular practice to monitor electronic content, electronic communications, or system use. However, CCSS reserves the right to perform such monitoring as it deems necessary. Monitoring may be performed without notification to support activities such as, but not limited to, operational maintenance, auditing, and security. Upon request, employee's must surrender all agency-issued equipment.

Change Management / Updates

Changes to information systems and information processing are controlled by CCSS management. Establishment of changes to existing information systems or information processing components will require an assessment of security risks that are to be used to inform approval. All changes to technology and systems must be approved by the Directors.

Remote Access & Support

Technological and information management support is available to all employees from the CCSS management support team. The Directors are available for complex IT issues or support needs. The agency makes use of remote desktop software AeroAdmin to enable remote access to all agency-issued equipment to address and repair any issues.

Inventory Management

- An inventory of all IT assets (tangible or intangible) associated with information and information technology must be documented and maintained.
- Users must be designated for all assets associated with the processing and storage of information.

Decommissioning of Equipment & Destruction of Records

Where equipment is being disposed of, CCSS management must ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten. Where this is not possible, CCSS management will physically destroy the disk or tape. Inventory will be updated.

Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned. Prior to reassignment of hardware or media within the agency, the management support team must ensure:

- That the integrity of CCSS records is maintained;

- Information and software is erased using methods in accordance with best practices;
- Where information is erased by third parties there must be verification to ensure complete destruction of the information. Third parties must certify that destruction has occurred.

Training

All new and regular employees will receive annual training in technology use and cybersecurity.

References:

Canadian Partnership Against Cancer. (2015). Information and Information Technology Security Policy. Retrieved May 11, 2020, from https://www.partnershipagainstcancer.ca/wp-content/uploads/2017/11/information-information-technology-security-policy.pdf

Douglas College. (2020). Information Security Policy. Retrieved May 11, 2020, from https://www.douglascollege.ca/-/ media/C7E430BFFAD14ED8812A85EB7955A279.ashx

iCIMS. (2020). IT Security Policy. Retrieved May 11, 2020, from https://www.icims.ca/gc/IT-Security-Policy/

Isle of Wight NHS Trust. (2019). INFORMATION TECHNOLOGY SECURITY POLICY. Retrieved May 11, 2020, from https://www.iow.nhs.uk/Downloads/Policies/Information Technology Security policy.pdf

Paloalto Networks. (2020). What is an IT Security Policy? Retrieved May 11, 2020, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy

Resolver. (2020). Clear Desktop and Screen Policy. Retrieved May 11, 2020, from https://www.resolver.com/trust/policies/clear-desk-policy/

Royal Roads University. (2014, October 22). IT Services Information Security Policy Framework. Retrieved May 11, 2020, from https://policies.royalroads.ca/policies/it-services-information-security-policy

Workable. (2020, March 12). Company cyber security policy template: Workable. Retrieved May 11, 2020, from https://resources.workable.com/cyber-security-policy

Community Connections Support Services - Policies and Procedures

For further information on this policy or permission to reprint, please contact:
Vivienne Prather
Director – Strategic Management
Community Connections Support Services
Unit 236
9-3151 Lakeshore Rd.
Kelowna, BC V1W 3S9
ph. (250) 491-2907 fx.1-866-728-2938
viv@commconn.ca
www.commconn.ca