Policy Number	Policy Section	Effective: January 9, 2013 Amended: July 9, 2025
IT5.190	Information Technology	
Title: Information Incidents Including Privacy Breaches Policy	**Executive Sponsor:** Vice President, Information Technology and Project Services	

SUMMARY

This policy explains what happens when CLBC collects, uses, stores or shares information in a way that is not allowed by law. This could mean somebody's personal information is not handled properly and their privacy is affected.

There is also a document called the "Information Incidents Including Privacy Breaches Procedures Guide" that explains what CLBC workers have to do when this happens.

1. PURPOSE

The *Information Incidents including Privacy Breaches Policy* explains how Community Living British Columbia (CLBC) manages and responds to all types of information incidents, including privacy breaches which involve personal information. It establishes processes to ensure timely and effective handling of these incidents in order to safeguard personal information and sensitive data and minimize potential harm to individuals and CLBC.

The *Information Incidents Including Privacy Breaches Policy* is part of CLBC's Privacy Policy Suite established in the overarching *Organizational Privacy Policy*. It ensures CLBC requirements align with BC government standards and best practices in information management. It should be reviewed with the *Information Incidents Including Privacy Breaches Procedures Guide* and applied together as a set of standardized requirements.

2. DEFINITIONS

See *Appendix – Definitions* for relevant definitions.

3. POLICY

3.1 Information incidents, including privacy breaches, occur when unwanted or unexpected events, such as theft, loss or unauthorized disclosure, threaten the security or privacy of personal or sensitive information. Information incidents may happen while handling or transmitting information using hard copy, data storage devices, fax, email or voicemail; in the course of a personal or phone conversation; or while using CLBC information technology systems. Compliance with the *Collection of Personal Information Policy*, the *Confidentiality and Information Sharing* Policy, and the *Protection of Information Policy* helps

to safeguard personal and sensitive information and prevent information incidents from occurring.

3.2 The CLBC Privacy Officer is responsible for managing the response to specific information incidents. This work is done collaboratively with the relevant manager or supervisor, the relevant staff, the Information Security Officer, and/or the BC Office of the Chief Information Officer as appropriate to the specific circumstance. When information incidents involve CLBC's information technology systems, the Information Security Officer takes primary responsibility, and the Privacy Officer plays a supporting and consultative role.

3.3 All staff must report an actual or suspected information incident immediately, including incidents reported by individuals, family or service providers.

3.4 Staff work with their manager or supervisor, and with the Privacy team to contain and mitigate the impact of an information incident, when possible, by recovering the information or records; suspending the activity that led to the incident, or correcting any physical or systems weakness that may have led to the incident.

3.5 The Privacy Officer assesses the extent and impact of the information incident including the personal information involved, individuals affected, and foreseeable harm, in consultation with the Office of the Chief Information Officer as needed

3.6 The Privacy Officer reviews the impact of privacy breaches to determine if it is appropriate to notify individuals whose personal information has been affected by the breach. The Privacy Officer works with the Service Area Managers and Service Delivery Managers, or relevant managers to notify affected individuals and their families if warranted by the circumstances. See the *Information Incidents Including Privacy Breaches Procedures Guide* for the Breach Notification Process.

3.7 CLBC staff ensure service providers are aware of their contractual requirement to have appropriate information security procedures in place and to immediately notify CLBC in the event of unauthorized disclosure of personal information. See *Service Terms and Conditions – Schedule E: Privacy Protection* for more information.

3.8 Managers and Supervisors ensure documentation of all information incidents and related investigations is completed. Reports are submitted using the *Information Incident Form*.

3.9 Managers and supervisors work with the Privacy Officer to establish and maintain a culture of prudent information management. This includes implementing recommendations from investigations and audits.

3.10 The Privacy Officer and Information Security Officer must ensure documentation of all privacy breaches, information incidents, related investigations and audits is maintained centrally.

3.11 When an information incident includes the personal information of an Indigenous person, staff contact the Privacy team. The Privacy team, Indigenous Relations team, and Policy and Government Relations team will work collaboratively with the regional staff to ensure cultural safety considerations are addressed.

4. REFERENCES

Collection of Personal Information Policy

Confidentiality and Information Sharing Policy

Freedom of Information and Protection of Privacy Act

Information Incident Form

Information Incidents Including Privacy Breaches Procedures Guide

Organizational Privacy Policy

Protection of Information Policy

Service Terms and Conditions for Contracts between CLBC and Service Providers

Appendix - Definitions

Information Incident: A single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the unauthorized collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate.

Privacy Breach: Information incidents are called privacy breaches when they involve collection, use, disclosure, access, disposal, or storage of **personal** information, whether accidental or deliberate, that is not authorized by the *Freedom of Information and Protection of Privacy Act.*

Personal Information: Information recorded about an identifiable individual, other than contact information. Personal information may include but is not limited to:

- Name, address, telephone number, email;
- Race, national/ethnic origin, colour, religious or political beliefs or associations;
- Age, sex, sexual orientation, marital status;
- Identifying number or symbol such as social insurance number or driver's license number;
- Fingerprints, blood type, DNA prints;
- Health care history;
- Educational, financial, criminal, employment history; and
- Anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else

Personal information also includes separate pieces of information that may seem unrelated, but when put together would allow someone to accurately infer information about an individual.

Sensitive Information: Information or data that is confidential or critical to the functioning of CLBC, or which CLBC is obliged under law or by government to maintain and keep confidential, and any other information or data that could harm CLBC or individuals, if compromised.

Privacy Officer: A designated position within CLBC with overall responsibility and accountability for CLBC privacy policies and related compliance with the *Freedom of Information and Protection of Privacy Act*. The Manager, Information Management is CLBC's Privacy Officer.

Information Security Officer: A designated position within CLBC with overall responsibility for policies and compliance related to the security of information contained in and related to CLBC information technology systems. This position is also sometimes called the information custodian. The Vice President, Information Technology and Project Services is CLBC's Information Security Officer.