COMMUNITY LIVING
BRITISH COLUMBIA

Policy Number	Policy Section	Effective: January 9, 2013
QA7.110	Quality Assurance	**Amended**: November 24, 2016
Title: Information Incidents including Privacy Breaches Policy		**Executive Sponsor:** Director, Quality Assurance

1. PURPOSE

This policy describes how CLBC manages and responds to information incidents, including privacy breaches which are information incidents involving personal information. It is consistent with the policy of the BC government.

The *Information Incidents including Privacy Breaches Policy* is one of a suite of privacy policies described in the overarching *Organizational Privacy Policy*. The *Protection of Information Policy,* another policy of the privacy policy suite, describes how CLBC prevents and avoids information incidents.

2. DEFINITIONS

Information Incident: A single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the unauthorised 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, including, but 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

- 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, Quality Assurance 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 Director, Information Technology is CLBC's Information Security Officer.

3. POLICY

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.

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

Staff must also contain a privacy breach or other information incident if possible by recovering the information or records; suspending the activity that led to the breach, or correcting any physical or systems weakness that may have led to the breach.

CLBC staff provide information to service providers to clarify their contractual requirements to have appropriate information security procedures in place and to immediately notify CLBC in the event of unauthorized disclosure of personal information.

CLBC uses a four step process to manage privacy breaches and other information incidents in a consistent and appropriate way:

Step 1: Report

The key to successful management of privacy breaches or other information incidents is to take action as soon as possible. Reporting any actual or suspected information incident immediately is critical. Information incidents may be discovered and reported by employees

in the course of their work; by an audit or other investigation; or by an individual, family or service provider.

Step 2: Recover
Recovery is the first response to a report of a privacy breach or other information incident, designed to contain and/or lessen the impact for CLBC and/or for individuals, families or service providers who may be affected. This can involve recovering the actual information; suspending or isolating the activity that may have led to the information incident; and/or correcting any weakness in information security that may have led to the information incident.

Step 3: Remediate
It is important to determine the specifics, extent and impacts of the privacy breach or other information incident, including the precise information assets(s) involved, the individuals, families and/or service providers affected, and any foreseeable harm. This may require consultation with the Office of the Chief Information Officer. Some privacy breaches may require notification of affected individuals, families or service providers, and/or general public notification. Reporting on the resolution of incidents and the outcomes of investigations, including recommendations, is key for accountability and for preventing future incidents. Information incidents that may have been deliberate or that involve multiple public agencies or ministries may require reporting or liaison with other authorities such as the police or the Office of the Information and Privacy Commissioner.

Step 4: Prevent
CLBC promotes an organizational culture of keen awareness and diligence about the handling of information. This policy focuses on how CLBC responds to prevent future information incidents and privacy breaches after an incident has occurred Staff will also know about and comply with measures described in the CLBC *Protection of Information Policy*. The *Protection of Information Policy* provides direction on protecting personal and sensitive information and preventing information incidents and privacy breaches before they occur. CLBC staff ensures additionally that service providers are aware of their responsibilities under the *Terms and Conditions* of their contracts.

The CLBC Privacy Officer has overall responsibility for leading and coordinating this process, working collaboratively with Integrated Service Managers and staff; the Information Security Officer ; and the BC Office of the Chief Information Officer The Privacy Officer takes primary responsibility for managing the response to specific information incidents, except those involving CLBC's information technology systems, where the Information Security Officer takes primary responsibility and the Privacy Officer plays a supporting and consultative role.

CLBC assesses the extent and impact of the breach or information incident including the personal information involved, individuals affected, and foreseeable harm, in consultation with the Office of the Chief Information Officer as needed.

The impact of privacy breaches must be reviewed to determine if it is appropriate to notify individuals whose personal information has been affected by the breach. The Privacy Officer works with the Director, Regional Operations and Integrated Service Managers to notify affected individuals and their families if warranted by the circumstances. Considerations regarding notification are described in *Appendix One* of this policy.

4. PROCEDURES

The key to responding to information incidents including privacy breaches is to take action as soon as possible. The following procedures outline steps (report, recover, remediate and prevent) that staff follow for responding to information incidents.

4.1 All Staff:

- **Report** any actual or suspected privacy breach or other information incident immediately to your Integrated Service Manager or Director, Regional Operations or the Privacy Officer, if the Integrated Service Manager is not available;
- **Recover** the personal or sensitive information if possible, or otherwise contain the incident as directed by the Integrated Service Manager or Director, Regional Operations;
- **Remediate** the privacy breach or information incident by working with the Integrated Service Manager , Director, Regional Operations, Privacy Officer, Information Security Officer or others assigned to determine the specifics of the incident, to resolve it and, if directed, to notify affected individuals; and
- **Prevent** privacy breaches and information incidents by reviewing and making any needed changes to your processes, understanding your responsibilities, being diligent in the handling of sensitive or personal information and being an active participant in developing the culture of prudent information management as described in the *Protection of Information Policy*.

4.2 Integrated Service Managers:

In addition to the same responsibilities as all staff, Integrated Service Managers:

- **Receive** reports about actual or suspected privacy breaches or information incidents from employees, service providers or other persons and provide direction on assessing the incident;
- **Report** actual or suspected privacy breaches or information incidents to the Privacy Officer and where an incident involves CLBC information technology or systems, also ensure it is **reported** to the Information Security Officer;
- **Recover** the personal or sensitive information immediately if possible, or otherwise contain the incident to lessen the impacts for CLBC and individuals. Determine if the personal or sensitive information can be recovered locally, or if the loss/disclosure can otherwise be contained locally. Further actions depend on circumstances but may include locating information, records or equipment, correcting physical security issues, and

isolating the activity that led to the incident. (Note: If the incident involves information technology, seek the direction of the Information Security Officer before taking any containment steps directly;

- **Remediate** the incident by working collaboratively with the Director, Regional Operations and the Privacy Officer or Information Security Officer as needed, to determine the specifics of the information incident or privacy breach , to implement the steps to resolve it and, if instructed by the Privacy Officer or the Director, Regional Operations , to notify affected individuals;
- **Prevent** information incidents by:
    - Implementing recommendations from investigations;
    - Ensuring that employees know and understand how to handle personal and sensitive information;
    - Participate in the development of a culture for the prudent management of information, including providing training;
    - Ensure employees understand their responsibility in reporting all actual and suspected privacy breaches and information incidents and contain the loss and/or recover the information as described in the *Protection of Information Policy*; and
    - Provide information to contractors and service providers to clarify their responsibilities under the *Terms and Conditions; Schedule E: Privacy Protection* of their contract.

4.3 Director, Regional Operations

In addition to the same responsibilities as Integrated Service Managers, Director, Regional Operationss:

- Ensure Integrated Service Managers and staff are aware of and adhere to their responsibilities under this policy if an information incident occurs;
- Make decisions about notifying affected individuals if the Privacy Officer is not available and the decision is urgent;
- Informs the Communications Department where an information incident may result in adverse media attention (e.g. loss of sensitive budget materials, individual files lost in dumpster);
- Advise the Privacy Officer of any systemic concerns or issues they become aware of;
- Work collaboratively as needed with the Privacy Officer and Information Security Officer during investigations of breaches of privacy and other information incidents; and
- Support audit activities initiated by the Privacy Officer and/or Information Security Officer.

4.4 Privacy Officer:

CLBC's designated Privacy Officer has overall responsibility for ensuring CLBC maintains adequate systems for preventing and responding to privacy breaches and information incidents. As part of this role, the Privacy Officer:

- Maintains a log and provides a summary report to the Senior Management Team annually;
- Receives reports of breaches of privacy and other information incidents from Directors, Regional Operations and Integrated Service Managers unless the breach involves CLBC information technology or systems;
- Develops procedures for investigating and remediating breaches in collaboration with the Information Security Officer;
- Investigates or supports the investigation of privacy breaches and information incidents in collaboration with the Information Security Officer;
- Provides consultation to Integrated ServiceManagers and Directors, Regional Operations regarding expectations and practice for responding to privacy breaches and information incidents whether internal or external; (e.g. responding to service providers);

- Makes decision about whether to notify affected individuals in cases of privacy breaches;
- Informs the Communications Department where an information incident may result in adverse media attention;
- Receives reports about the management of incidents from the Directors, Regional Operations;
- Receives status reports and the final investigation reports, distributing them as necessary;
- Coordinates information incident communication and updates internally;
- Liaises with Office of the Chief Information Officer and with other government ministry information officers in multi-ministry incidents;
- Assists in reviewing and rectifying existing procedures, where necessary;
- Ensures that the regions implement the recommendations of investigations;
- Initiates audits as needed; and
- Reports investigation, implementation or audit results as needed to the Chief Executive Officer.

4.5 Information Security Officer:

The Information Security Officer takes the lead in preventing and responding to incidents involving IT systems and assets. The Information Security Officer:

- Receives reports of information incidents including privacy breaches where the incident involves CLBC information technology or systems;
- Develops procedures for investigating and remediating privacy breaches and other information incidents in collaboration with the Privacy Officer;
- Investigates privacy breaches and other information incidents as needed, in collaboration with the Privacy Officer; and
- Carries out additionally the same responsibilities as the Privacy Officer, where the incident involves information technology.

5. DOCUMENTATION

5.1 Documentation of an investigation of an information incident should include:

- What happened, when, and who was involved
- How and when it was discovered
- Information assets involved and scope of the incident
- Who was interviewed in the investigation
- Whether the incident has been contained and any information recovered
- Who has been notified
- Remedial action taken
- Recommendations, including further action that needs to be taken
- Involvement of other ministries or authorities

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

6. PRACTICES

6.1 CLBC staff refer to the CLBC *Protection of Information Policy* for further guidance and direction on prevention of information incidents and privacy breaches.

6.2 Information incidents may happen while handling or transmitting information using hard copy, data storage devices, fax, email or voice-mail; in the course of a personal or phone conversation; or while using CLBC information technology systems.

6.3 Good practice around notifying affected persons relies on a balance of harms approach. For instance, a person who potentially faces harm as a result of an information incident may not be notified, if it is determined that the harm resulting from notifying them would outweigh the benefit to be gained. Refer to *Appendix 1* for more information regarding notification decisions and process.

6.4 Practice guidance regarding the notification of individuals, families or service providers affected by a privacy breach is included in *Appendix 1*.

7. REFERENCES

CLBC Privacy Guidelines
Confidentiality and Information Sharing Policy
Contract Terms and Conditions: Schedule E: Privacy Protection
Information Security Policy
Organizational Privacy Policy
Protection of Information Policy

APPENDIX 1: NOTIFICATION

Decisions to notify or not notify affected persons when a privacy breach has occurred require the approval of the Privacy Officer or Director, Quality Assurance. In unusual circumstances where neither is available the Director, Regional Operations may make this decision.

Considerations
The key consideration in deciding whether to notify or not is whether it is necessary to avoid or mitigate harm, such as:

- Risk of identity theft or fraud
- Risk of physical harm
- Risk of hurt, humiliation or damage to reputation
- Risk to business or employment opportunities

Other considerations may include:

- Legislative requirements for notification
- Contractual obligations requiring notification
- Risk of loss of confidence in CLBC and/or good relationships

Process
If it is determined that notification is appropriate, do it as soon as possible following the privacy breach. If law enforcement authorities have been contacted, it may be appropriate to work with those authorities in order not to impede their investigation.

Notify affected persons directly, by phone, email, letter, or in person, whenever possible. Use indirect notification (using general, non-personal information) only if direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification – website publication, posted notices, media – in certain cases may be the most effective approach.

What to Include

- Date of the breach
- Description of the breach (extent)
- Description of the information compromised
- Risk(s) to individual caused by the breach
- Steps taken to mitigate the breach and any related harms
- Next steps planned and any long-term plans to prevent future breaches
- Steps the person can take to further mitigate the harm, or steps CLBC has taken to assist the person in mitigating harm. For example, how to contact credit-reporting agencies to set up a credit watch, or how to change a personal health number or driver's licence
- Contact information of staff who can answer questions or provide further information
- Information about the right to complain to the Office of the Information and Privacy Commissioner and the necessary contact information

- If CLBC has already contacted the Commissioner's office, explain this in the notification letter

What Not to Include

- Personal information about others or any information that could result in a further privacy breach
- Information that could be used to circumvent security measures
- Information that could prompt a misuse of the stolen information (for example, if hardware was stolen for simple 'wiping and resale', but the notification prompts someone to realize that personal information is on the hardware and could be of some value if accessed)