Policy

APPROVED

Privacy Breach

Purpose

This policy provides a process for reporting known or suspected Privacy Breaches to the appropriate individuals, and sets out the steps to be followed once BCLC learns of a suspected breach of privacy.

Scope

This policy applies to all BCLC employees and to third parties as required by BCLC, such as BCLC's contractors, vendors and service providers.

This policy applies to BCLC records containing personal information, in any format, that are under BCLC's custody (i.e., physical possession) or under BCLC's control (i.e. power or authority to manage information including restricting, regulating and administering its use or disclosure). It also applies to computer systems, network devices and any additional systems and outputs containing or transmitting personal information.

Policy Statement

Any employee or third party, if applicable, who suspects or becomes aware that a Privacy Breach has or may have occurred must immediately initiate Step 1 of this policy. Reporting a Privacy Breach as soon as one is suspected or known to have occurred provides the greatest opportunity to effectively contain, investigate and, where necessary, advise affected individuals of the scope and circumstances of the breach, and to recommend steps that should be taken to prevent further impacts from the breach.

Privacy Breaches may include, for example:

- personal information used for a purpose not stated in the applicable privacy notice or consistent with the original collection;
- unauthorized access to personal information;
- stolen or lost personal information (e.g., a computer containing personal information is stolen); or
- inadvertent or deliberate disclosure of personal information to an unauthorized person or group (e.g., personal information is emailed to the wrong person).

Context

The *Freedom of Information and Protection of Privacy Act* (FIPPA), British Columbia governs access to, and the collection, use, disclosure, disposal, retention and security of personal information, and establishes rules for public bodies, such as BCLC, to follow in order to protect the privacy of individuals. Section 30.5 outlines a notification obligation where there is an unauthorized disclosure of personal information. Section 74.1 outlines privacy protection offences and penalties. For BCLC, this means reporting a breach, providing information about a breach

and taking steps to contain a breach as directed by the Director responsible for privacy at BCLC and BCLC's Privacy Officer.

Privacy Breaches may be related to an information security incident, which involves a disruption or threat to BCLC's services or protection of data and information. In these cases, the procedure set out in BCLC's Information Privacy and Security Incident Management Procedure may need to be followed.

BCLC refers to materials provided by the Office of the Information & Privacy Commissioner for British Columbia (OIPC) for guidance, including the document Privacy Breaches: Tools and Resources.

Policy Details

BCLC responds to suspected Privacy Breaches by following the steps outlined below that are relevant to the Privacy Breach.

Given the varied nature of Privacy Breaches, no "one-size-fits-all" response is possible or practical. BCLC tailors actions to make certain they are proportional and appropriate to each Privacy Breach. Accordingly, steps may not occur in the order listed and, as additional information is discovered, additional action may be required to contain or address a Privacy Breach.

STEP 1: REPORT THE SUSPECTED PRIVACY BREACH

BCLC's Director responsible for privacy and BCLC's Privacy Officer must be immediately informed of a suspected or known Privacy Breach involving personal information in the custody or control of BCLC. The individual who first becomes aware of a suspected or known Privacy Breach is responsible for reporting.

Preliminary details that an individual should be prepared to provide when reporting a suspected Privacy Breach are:

- What happened?
- Date the breach was discovered.
- Date of the breach.
- Location of the breach.
- How was the breach discovered?
- Has the breach been contained?

Reports of suspected Privacy Breaches must be investigated to determine if a Privacy Breach has in fact occurred.

STEP 2: CONTAIN THE PRIVACY BREACH

Actions must be taken to contain a Privacy Breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, or correcting weaknesses in security. Privacy Breaches should be contained immediately.

STEP 3: DOCUMENT THE PRIVACY BREACH

Privacy Breaches must be documented so that the risks and corrective actions taken may be reviewed. Information about the Privacy Breach that must be documented includes a description of the incident, any containment activities, identified risks, notification details and recommendations.

STEP 4: EVALUATE THE RISKS

Risks associated with the Privacy Breach must be assessed. This step includes assessing: the extent and sensitivity of the personal information involved; the cause and extent of the Privacy Breach; the number and types of individuals affected by the breach; and foreseeable harm from the Privacy Breach.

STEP 5: NOTIFY IF NECESSARY

An assessment must be made as to whether notification about a Privacy Breach is required to: individuals impacted, law enforcement bodies, regulatory bodies, the OIPC and to appropriate individuals within BCLC, including the Board of Directors. If notification is necessary, prompt notification to the appropriate parties should be carried out.

STEP 6: ANALYZE AND CORRECT

The cause of a Privacy Breach must be investigated and steps that can be taken to reduce the likelihood of a recurrence must be considered. If necessary, this will include an evaluation of physical, organizational and technological security measures. If appropriate, the Director responsible for privacy and Privacy Officer may assist the responsible department(s) in implementing additional safeguards against further Privacy Breaches.

Roles and Responsibilities

Employees and **third parties** are responsible for:

- reporting suspected Privacy Breaches, in accordance with Step 1; and
- supporting the Director responsible for privacy, or his/her designate, and the Privacy Officer in carrying out their assigned responsibilities under this policy.

APPROVED

Privacy Breach

Director responsible for privacy is responsible for:

- investigating reports of suspected Privacy Breaches or designating a delegate to conduct an investigation; and
- ensuring steps two through sixth are carried out and completed in co-operation with BCLC departments, employees and third parties as necessary.

Privacy Officer is responsible for:

- supporting BCLC's Director responsible for privacy in leading investigations of suspected Privacy Breaches; and
- ensuring steps two through sixth are carried out and completed in co-operation with BCLC departments, employees and third parties as necessary.

Definitions

Privacy Breach	means unauthorized access to or collection, use, disclosure, retention or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of Part 3 of FIPPA. This may be inadvertent or deliberate.

Policy Ownership

Policy Owner	Director, Security, Privacy and Compliance
Approving Body	Vice President, Legal, Compliance, Security

Policy

APPROVED

Privacy Breach

Revision History

Version	Effective	Approved by	Amendment
3.1	Oct 27, 2020	Vice President, Legal, Compliance, Security	Update to Approving Body title to reflect changes following the organizational restructure for OneBCLC.
3.0	May 18, 2016	Vice President, Corporate Security & Compliance	Major amendments to clarify scope, policy context, and the definition of a Privacy Breach. Added a new step and requirements and clarified existing requirements. Minor amendments made to align content with policy template, policy writing guidelines, and changes in role titles.
2.3	Jan 29, 2015	Vice President, Corporate Security & Compliance	Minor amendment to footer text. This document was re-classified from 'Internal' to 'Public' in order to comply with a directive from the Public Sector Employers' Council. An exemption to policy approval requirements was made due to exceptional circumstances.
2.2	Aug 19, 2013	Vice President, Corporate Security & Compliance	Updated to reflect organizational changes.
2.1	Jan 31, 2013	(Acting) Director, Privacy	Minor amendment to remove contact phone number of previous Director of Privacy.
2.0	Mar 16, 2012	Director, Privacy	Updated to reflect operational experience of managing privacy breaches.
1.2	Jan 21, 2011	Director, Privacy	Telephone contact details for Director of Privacy updated.
1.1	Jul 16, 2010	Director, Privacy	Privacy breach reporting amended to report directly to the Director of Privacy.
1.0	Apr 12, 2010	Vice President, Corporate Security & Compliance	Inaugural.