Policy

APPROVED

Privacy Management and Accountability

Contents

Policy

APPROVED

Privacy Management and Accountability

Policy

APPROVED

Privacy Management and Accountability

Purpose

To establish requirements for managing Personal Information and protecting privacy in compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), British Columbia. The entire life cycle is addressed, which includes collecting, viewing, using, disclosing, and disposing of Personal Information.

Scope

This policy applies to all employees and Contractors.

This policy applies specifically to information satisfying the definition for Personal Information as stated in BCLC's Policy Glossary.

Policy Statement

BCLC is committed to protecting privacy and being accountable for how it handles Personal Information. The protection of privacy is a shared responsibility at BCLC as outlined below.

Accountability for the day-to-day handling of Personal Information is distributed across the organization to custodians of Personal Information. Personal Information must have a designated custodian. Multiple custodians may be designated for the same set of Personal Information where the Privacy team deems necessary. In this case, all those with custodianship for the set of Personal Information have shared accountability.

Personal Information must be handled pursuant to this Policy, FIPPA, and any other applicable legal and policy requirements. This includes all Personal Information that is in BCLC's Custody or under its Control regardless of the format it is in, where it is physically or digitally stored, or the individual(s) it is about.

EVERYONE'S GENERAL RESPONSIBILITIES

Employees and Contractors must:

- adhere to protections implemented by custodians and must not seek to circumvent them;
- support and cooperate with custodians and the Privacy team when performing their respective duties;

- follow instructions issued by the Privacy team;
- seek advice from the Privacy team in any circumstance involving Personal Information where they are uncertain whether or how to proceed; and
- manage the retention of records containing Personal Information in accordance with the *Information Management Act*, British Columbia and BCLC policies.

Employees and Contractors must not:

- negligently or recklessly handle Personal Information;
- intentionally, purposefully or willfully handle Personal Information unless doing so is:
  - authorized under FIPPA,
  - required for the performance of their job duties; and
  - they are legitimately performing those duties; or
- shift to another individual any of those responsibilities assigned to them in this Policy.

For certainty, the act of intentionally viewing Personal Information without authorization or without a legitimate business purpose (commonly referred to as snooping) may be considered an offence under FIPPA and is strictly prohibited.

A CUSTODIAN'S GENERAL RESPONSIBILITIES

Custodians must make certain:

- BCLC's protections for Personal Information are implemented as prescribed in this Policy and as instructed by the Privacy team;
- the protections are effective; and
- the accuracy of Personal Information is maintained as prescribed in this Policy.

THE PRIVACY TEAM'S GENERAL RESPONSIBILITIES

The Privacy team is responsible for providing advice upon request to employees and may communicate BCLC's expectations to Contractors from time to time regarding FIPPA compliance and adequate protections for Personal Information.

Policy

APPROVED

Privacy Management and Accountability

Context

POLICY OBJECTIVES

The aim of this Policy is to set the minimum, high-level requirements necessary for BCLC to achieve:

- statutory compliance with privacy requirements under FIPPA;
- responsible handling Personal Information; and
- readiness to respond to the Office of the Information and Privacy Commissioner (OIPC) for British Columbia, which oversees the administration and enforcement of FIPPA.

LEGISLATIVE AND POLICY FRAMEWORK

This Policy is governed by FIPPA, which establishes requirements for how public bodies, including BCLC, must protect personal privacy where they collect, use, or disclose Personal Information. FIPPA is accompanied by the *Freedom of Information and Protection of Privacy Regulation* (the FIPPA Regulation), which establishes additional requirements applicable to BCLC for, among other things, obtaining consent from individuals to collect, use, or disclose their Personal Information. FIPPA is also accompanied by the *Personal Information Disclosure for Storage Outside of Canada Regulation* (the Transborder Disclosure Regulation), which establishes additional requirements applicable to BCLC for the transfer of Personal Information outside of Canada.

The responsibilities and authorities assigned within this Policy are governed by a Delegation of Authority instrument (DAI). A DAI formalizes the delegation of duties, powers, and functions from the head of a public body to its officers or employees pursuant to section 66 of FIPPA. This Policy was developed to align with the inaugural BCLC DAI. The currently applicable DAI shall prevail in the event of a discrepancy.

BCLC's Standards of Ethical Business Conduct (SOEBC) should be read in conjunction with this Policy as it sets a broad expectation for employees and Contractors concerning the protection of Confidential information. BCLC classifies Personal Information as Confidential information under its Information Classification Policy.

Policy

APPROVED

Privacy Management and Accountability

BCLC's Information Security Policy and associated standards should be read in conjunction with this Policy by individuals responsible for implementing protections for Personal Information. These establish a minimum set of security measures for protecting all information and information technology resources. This Policy will prevail in the event of any ambiguity or discrepancy between a specific expectation in this Policy and another expectation within the Information Security Policy or associated standards.

BCLC's Appropriate Use of Information and Information Technology Resources Policy should be read in conjunction with this Policy as it addresses reporting Information Security Incidents, which may include events defined in this Policy as Privacy Breaches.

Policy Details

INTERPRETATION OF "HANDLING"

Where this Policy refers to "handling" Personal Information or Personal Information being "handled", this should be interpreted as:

- information about an identifiable individual that is or will be collected, recorded, used, viewed, disclosed, or disposed of; or
- the security, storage, accuracy, or correction of recorded information about an identifiable individual that is or will be affected.

CUSTODIANS

Identification

A custodian must be identified and assigned custodianship of Personal Information based upon an individual's role satisfying the following principles:

- There is a close alignment between a role's accountabilities and the accountabilities assigned to custodians within this Policy for protecting Personal Information.
- The role is the same as the one identified under BCLC's corporate policies and standards for information security, which require information to have an owner.
- The role is performed by a BCLC employee who is at the Director-level or above.

For additional guidance, the individual overseeing the operational processes and functions that are mostly supported by the information that includes Personal Information should be given the rights and obligations to protect that information pursuant to the first principle listed above.

As per the second principle listed above, the individual identified as the owner of an information set (that includes Personal Information) pursuant to BCLC's corporate policies and standards for information security should be the same individual (or at least one of the individuals) identified as the custodian for that same information set under this Policy. The intent of this principle is to achieve alignment and avoid inadvertently or unknowingly dividing accountabilities for information security and privacy protection among multiple individuals for the same information set.

Custodians are identified and assigned when a Privacy Impact Assessment (PIA) is completed.

Delegation

Custodians may designate other BCLC employees to carry out functions, tasks, and decisions necessary for complying with this Policy. However, BCLC holds custodians ultimately accountable for the handling of Personal Information assigned to them. This accountability may not be delegated.

This limitation also applies where a custodian grants a request authorizing individuals or Organizational Units to handle personal information under their protection. In this case, the custodian's accountability is not transferred nor extended to the requesting individual or Organizational Unit. However, the general responsibilities of employees and Contractors will apply to any authorized individuals or Organizational Units (see Everyone's general responsibilities).

PRIVACY IMPACT ASSESSMENT (PIA)

General

Custodians must complete an assessment for risks related to the protection of privacy (commonly referred to as a Privacy Impact Assessment or PIA) in accordance with section 69 (5.3) of FIPPA and the Transborder Disclosure Regulation. A PIA is required where a BCLC-led Initiative involves the handling of Personal Information, regardless of whether the Initiative includes handling Personal Information internally or externally. For certainty, this requirement

applies to those Initiatives described in the Minister's Directions on Conducting PIAs: Non-Ministry Public Bodies (2021), which includes:

- a new Initiative for which no PIA has previously been completed; and
- an existing Initiative where substantive modifications are proposed or being implemented.

The Privacy team has authority to decide whether an Initiative warrants a PIA and to determine the scope of the PIA.

Section-by-Section review

A section-by-section review of those FIPPA sections relevant to an Initiative may be warranted as part of a PIA (commonly referred to as a PIA Part 2). The Privacy team completes these reviews from time to time to confirm compliance. The Privacy team has authority to decide whether an Initiative warrants such a review.

Completion

A PIA is considered complete where the following conditions are met:

- the Privacy team acknowledges the PIA as completed; and
- where a section-by-section review is conducted, the custodian and any other required parties acknowledge the PIA as completed.

Acknowledgement must be provided in writing and, in the case of a section-by-section review, in the form of a signature.

The Privacy team has authority to determine those other parties required to acknowledge a PIA as completed where a section-by-section review is conducted.

Timing

A PIA must be completed prior to BCLC launching (or activating) an Initiative. Completion of the PIA may be deferred on a case-by-case basis where Personal Information will not be handled upon launch (or activation) of an Initiative. Only the Privacy team has authority to grant deferrals.

Privacy Management and Accountability

Implementation

Custodians must implement directions, as issued within a PIA, where there is reasonable certainty that disregarding a direction would result in BCLC violating FIPPA. Otherwise, custodians may implement directions, as issued within a PIA, at the custodian's discretion. A direction may compel custodians to modify or suspend an Initiative.

The Privacy team has authority to issue directions and to decide whether implementation of a direction is deemed necessary.

Maintenance

Custodians must make certain completed PIAs are kept up to date.

Custodians must review and update a completed PIA where substantive changes are proposed or where required to by the Privacy team. A substantive change is one that impacts the handling of Personal Information in a manner not previously assessed. Custodians are responsible for engaging the Privacy team where substantive changes are proposed.

The Privacy team may review a completed PIA at any time.

The Privacy team has authority to decide whether an Initiative warrants a new PIA or an update to an existing one.

Commissioner's review

BCLC may on a voluntary basis submit a PIA to the OIPC for proactive review and comment. The manager responsible for the Privacy team or another individual authorized under the DAI has authority to decide whether to submit a PIA to the OIPC.

BCLC must notify the OIPC and submit a PIA for review and comment, where required, pursuant to section 69. In this case, the manager responsible for the Privacy team must make certain BCLC provides notice.

PRIVACY RISK RESPONSES AND SECURITY ARRANGEMENTS

Custodians must develop, implement, and enforce reasonable risk treatments and on-going controls to minimize risks related to the unauthorized handling of Personal Information, including but not limited to those administrative (e.g., policies, procedures, etc.), technical and

physical controls identified in a PIA. Note: Initial risk treatments and on-going controls are typically developed collaboratively between the Privacy team and custodian(s) during the PIA process.

Risk treatments that are acceptable include:

- avoiding a risk;
- reducing the likelihood of a risk by removing one or more sources of the risk;
- reducing the impact or consequences of a risk;
- sharing a risk (also known as risk distribution); or
- accepting or retaining a risk.

Custodians are prohibited from sharing, accepting, retaining, or otherwise employing a risk treatment where doing so would result in BCLC contravening FIPPA. The Privacy team or Legal Services has authority to determine whether a treatment would result in a contravention of FIPPA.

PROCUREMENT AND PRIVACY PROTECTION SCHEDULES (PPS)

General

Custodians must make certain that Contracts contain reasonable security safeguards for protecting Personal Information. To meet that end, a Privacy Protection Schedule (PPS) is required for any Contract between BCLC and a third party that involves handling Personal Information.

Custodians must make certain a PPS is included within Contracts where required, in accordance with section 30 of FIPPA and in alignment with 47.i., Chapter 6 of the Government's Core Policy and Procedure Manual [6 Procurement: 6.3 Policy: 6.3.2 Procurement Phases: Contract Phase]. A PPS is not required where:

- Legal Services and Privacy instruct the custodian that a Contract contains other, comparable security safeguards; or
- BCLC will not have Custody or Control of the Personal Information.

Privacy Management and Accountability

Note: For the purposes of satisfying the requirements in the Minister's Directions on Privacy Management Programs (2023), a PPS is BCLC's common method for ensuring third parties are informed of their privacy obligations.

Timing

Contracts containing a PPS or comparable security safeguards must be completed prior to a third party handling Personal Information. A Contract is considered complete once all required parties have signed.

Standard PPS

BCLC's standard PPS should be used wherever possible.

The Privacy team must make certain a standard PPS is developed, issued, and maintained.

Alternative versions of PPSs

The use of an alternative PPS is permitted on a case-by-case basis where the circumstances warrant one. Alternative PPSs should be used sparingly. Custodians have authority to decide whether an alternative PPS is warranted.

Alternative versions of PPSs must include similar or superior requirements to BCLC's standard PPS. Prior to deciding whether an alternative PPS is warranted, Custodians must consult the Legal Services team and the Privacy team concerning use of an alternative PPS for the purpose of assessing its adequacy.

Preparation

PPSs may be drafted or modified on behalf of BCLC solely by Legal Services.

INFORMATION SHARING AGREEMENTS (ISA)

General

Custodians must make certain an ISA is completed where warranted. An ISA might be appropriate where:

- an Initiative involves sharing Personal Information between BCLC and a third party; and
- no other Contract will, or could be altered to, apply to the Initiative.

For guidance, sharing may include one-time transfers or recurring exchanges of Personal Information as well as one-way transfers or reciprocal exchanges of Personal Information. ISAs are normally used where there will be a regular and systematic sharing of Personal Information, as explained in the Government's ISA Guidance document.

Legal Services has authority to decide whether an Initiative warrants an ISA.

Completion

An ISA is considered complete once all required parties have signed. Custodians (or a designate with the requisite signing authority pursuant to the Spending and Signing Authority Policy) are responsible for signing an ISA on BCLC's behalf.

Timing

An ISA must be completed prior to a third party handling Personal Information.

Preparation

ISAs may be drafted solely by authorized individuals. Legal Services has authority to draft an ISA on behalf of BCLC.

Consultation

Custodians must consult Legal Services where their Initiative involves sharing Personal Information with a third party and where requirements for a PPS are not applicable.

Custodians must consult the Privacy team prior to signing an ISA so the Privacy team may determine whether a PIA is warranted.

Custodians must notify their Executive leader of their intent to share Personal Information with a third party prior to signing an ISA.

PERSONAL INFORMATION BANKS AND DIRECTORY

The Privacy team must develop and maintain a directory of BCLC's Personal Information Banks (PIBs). This directory must list all known PIBs and include all related information in accordance with section 69(6) of FIPPA. The Privacy team has authority to decide what constitutes a PIB.

APPROVED

Privacy Management and Accountability

Custodians must inform the Privacy team, upon request, about Personal Information in their Custody or PIBs. Full and accurate information about PIBs must be provided.

An individual who is authorized under the DAI must make available to the public BCLC's directory, in accordance with section 69(6) and 69(7) of FIPPA.

PRIVACY BREACHES

Report incidents

Employees and Contractors must report any incident where Personal Information was, or is suspected to have been, disclosed without authorization, either inadvertently or deliberately. For certainty, this applies to any information about an identifiable individual(s).

Reports should be made directly to the Privacy team. Where a report is made to another authority within BCLC, that authority is expected to redirect the report (or the individual who is reporting) to the Privacy team. For guidance, an employee or Contractor may bring an incident to the attention of their manager or another Organizational Unit such as the Cyber Security team. In these cases, the recipient of the report is expected to make the Privacy team aware of the incident.

Reports must be made (or redirected) immediately upon becoming aware of an incident.

Receipt of incident reports

The Privacy team must develop, implement, and maintain a means for receiving reports of incidents from employees, Contractors, and Service Providers to support compliance with sections 30, 30.5(2), and upon coming into effect, 36.3 of FIPPA.

Confirmation of breach

Each reported incident will be assessed to determine whether an actual Privacy Breach has occurred or is occurring. The Privacy team has authority to determine whether an incident involves a Privacy Breach.

Response to breach reports

Each reported Privacy Breach must be responded to in a tailored manner that is proportional and appropriate. Responses should involve containing, investigating, or resolving the matter.

APPROVED

Privacy Management and Accountability

The Privacy team has authority to decide whether a report of a Privacy Breach is shared internally and with whom and it is responsible for coordinating BCLC's response.

Responses should be carried out in collaboration with those employees and Contractors having relevant responsibilities, including those necessary for containing, investigating, or resolving a Privacy Breach. The Privacy team has authority to decide on a case-by-case basis who should be involved in responding to a reported Privacy Breach.

Employees and Contractors must adhere to instructions and implement recommendations issued by the Privacy team. The Privacy team has authority to issue instructions or recommendations to employees and Contractors for the purposes of containing, investigating, and resolving a Privacy Breach or reducing the risk of reoccurrence.

Containment

Employees and Contractors involved in responding to a reported Privacy Breach must make reasonable efforts to immediately contain the matter.

Investigation

Reported Privacy Breaches should be investigated unless it is deemed unnecessary for resolving the matter. The Privacy team has authority to decide whether an investigation is unnecessary.

Resolution

The Privacy team must make certain all reported Privacy Breaches are resolved. A reported Privacy Breach may be considered resolved where the underlying cause(s) of the Privacy Breach are addressed.

The Privacy team has authority to decide whether a Privacy Breach is resolved.

Breach documentation

The Privacy team must make certain confirmed Privacy Breaches are documented.

Notification to the head of BCLC

An individual who is authorized under the DAI must notify the head of BCLC of a known Privacy Breach in accordance with section 30.5 (2) of FIPPA. Notification must be provided immediately.

This same individual must make certain the Privacy team is informed of when notification was delivered and the medium that was used.

Notification to affected individuals and the Commissioner

Employees and Contractors are prohibited from notifying or otherwise discussing a Privacy Breach with affected individuals unless directed to do so by the Chief Compliance Officer or the head of BCLC.

An individual who is authorized under the DAI to notify the head of BCLC of a known Privacy Breach should make recommendations to the head of BCLC, in consultation with the Privacy team and/or Legal Services, concerning the following:

- whether notification to an affected individual(s) is required or not under section 36.3(2)(a) and 36.3(3);
- whether notification to the Commissioner is required or not under section 36.3(2)(b);
- the content of a notification;
- the method of delivery; and
- the sender of a notification.

The OIPC's guidance and any other relevant factors should be considered when making recommendations.

Notification to others

Notification to one or more of the following parties should be considered where a Privacy Breach is confirmed:

- BCLC's Board of Directors;
- appropriate individuals within BCLC;
- regulatory bodies; and
- law enforcement bodies.

The Chief Compliance Officer (or their designate) has authority to decide, upon consultation with the Privacy team and/or Legal Services, whether notification is appropriate or not as well as who should provide notification.

Privacy Management and Accountability

An individual from the following list should provide notification where deemed appropriate:

- CEO and President;
- Chief Compliance Officer;
- A member of the Executive;
- Director responsible for Privacy;
- Manager responsible for Privacy; or
- A member of the Privacy team.

This individual should be determined on a case-by-case basis. Notification should be provided without unreasonable delay.

PRIVACY NOTICES AND OBTAINING CONSENT

Custodians must develop, issue, and maintain Privacy Notices, in accordance with section 27(2) of FIPPA. A Privacy Notice must be issued whenever BCLC collects Personal Information from an individual unless an exemption under section 27(3) applies.

Custodians must seek confirmation from the Privacy team that a Privacy Notice, including modifications thereto, is compliant prior to issuance.

Custodians must make certain Privacy Notices are issued prior to collecting Personal Information.

Custodians must develop, implement, and maintain an auditable means for obtaining an individual's consent to collect, use, and disclose their Personal Information, in accordance with section 26(d), 32(b), 33(2)(c) and 33.1 of FIPPA. Custodians must make certain consent is valid, which means it is compliant with section 11 of the FIPPA Regulation.

APPROVED

Privacy Management and Accountability

INDIVIDUAL ACCESS, CORRECTION, AND ANNOTATION

Custodians must develop, implement, and maintain a means for individuals to access, correct, and annotate their own Personal Information, either on their own or with BCLC's assistance, in accordance with the DAI and sections 28, 29(2), 29(3), and 29(4) of FIPPA. Custodians must make certain BCLC provides a timely response to such requests.

Employees and Contractors are expected to respond to individuals' requests in accordance with directions provided by the relevant custodian for the Personal Information or the team responsible for addressing Freedom of Information requests (the FOI team). The FOI team's directions are issued through BCLC's Access to and Correction of Personal Information Standard.

QUESTIONS ABOUT COLLECTION AND COMPLIANCE COMPLAINTS

The Privacy team must make certain a means for receiving and responding to questions and complaints from individuals concerning the collection of their personal information or BCLC's compliance with Part 3 of FIPPA is developed, implemented, and maintained to support compliance with section 27 (2)(c) of FIPPA.

Questions and complaints must be reviewed and, where feasible, a response must be provided to the complainant. Responses must be provided in a timely manner. A response is not required where there is insufficient contact information available.

Only authorized individuals may review and respond to such questions or complaints. Individuals from the following teams are authorized:

- Customer Support Centre (CSC) team,
- Privacy team, and
- Legal Services.

The CSC team and Privacy team may authorize other individuals as necessary to review and respond to questions and complaints.

Privacy Management and Accountability

Employees and Contractors must not respond unless authorized to do so. Where questions or complaints are received directly, employees and Contractors must redirect the complainant (or their question/complaint) to an authorized individual.

FOREIGN DEMANDS FOR DISCLOSURE

Employees and Contractors are prohibited from responding in any way to requests seeking Personal Information where the demand is received, or suspected to have been received, from an authority they believe to be outside of Canada. Employees and Contractors must forward such demands to the FOI team.

EDUCATION AND AWARENESS

Employees and Contractors must complete training as required by BCLC's Board of Directors, the Privacy team, or custodians.

Managers must make certain their employees and Contractors have completed training as required.

All-staff training

The Privacy team must develop, deliver, and maintain mandatory privacy training that addresses, at minimum, an individuals' privacy obligations. The Privacy team must deliver, at minimum:

- general privacy training that is targeted to any and all BCLC employees and Contractors; and
- general privacy training for gaming facilities that is targeted to any and all Service Provider staff.

General privacy training must be completed upon initial employment, prior to handling Personal Information, and as required thereafter by BCLC's Board of Directors or the Privacy team. Training is prescribed in Appendix C of SOEBC. The Privacy team may make recommendations to the Board as to when privacy training must be completed, including the frequency of completion, and by whom.

Note: This training supports BCLC's compliance with the requirement to undertake privacy awareness and education activities, in accordance with section 36.2 of FIPPA and as directed in the Minister's Directions on Privacy Management Programs (2023).

Role-specific training

Custodians should develop, deliver, and maintain additional role-specific privacy training for BCLC employees and Contractors where operational policies and procedures apply to the handling of Personal Information under their protection. Custodians have authority to decide whether additional training should be provided.

DELEGATION OF AUTHORITY INSTRUMENT (DAI)

The Privacy team and FOI team must jointly develop, implement, and maintain a FIPPA DAI(s) for BCLC.

PRIVACY POLICIES AND PRACTICES

The Privacy team must develop, implement, and maintain privacy-related policies, standards, procedures, guidelines, and templates targeted at any or all employees and Contractors, as deemed necessary, that support compliance with this Policy.

Note: Operational policies and documented processes or practices targeted at a select group of individuals are the responsibility of the applicable custodian as required under Privacy Risk Responses and Security Arrangements and Privacy Notices and Obtaining Consent.

PRIVACY MANAGEMENT PROGRAM (PMP)

The Chief Compliance Officer (CCO) oversees BCLC's Privacy Management Program (PMP), which governs how the organization safeguards Personal Information throughout its life cycle.

The Privacy team must develop, implement, and maintain a privacy management program that supports BCLC's compliance with section 36.2 of FIPPA.

The Privacy team must regularly monitor the PMP and update it as required to ensure it remains appropriate to BCLC's activities and is compliant with FIPPA, in accordance with section 36.2 of FIPPA and as directed in the Minister's Directions on Privacy Management Programs (2023).

For the purposes of satisfying the requirements in the same Minister's Directions, BCLC's point of contact for PMP-related matters is the role listed below under Contract Position (see Policy Ownership). Note: The appropriate custodian(s) or an authorized individual should be the point

of contact for other privacy-related matters (see authorized individuals in Questions about Collection and Compliance Complaints). If uncertain, the appropriate custodian(s) (or their contact information) will be indicated in the applicable Privacy Notice.

Compliance

Failure to comply with this Policy could result in BCLC not meeting its obligations under FIPPA and, consequently, the OIPC may conduct a full investigation or inquiry and/or impose remedial orders.

Employees and Contractors may be personally subject to administrative (e.g., fines up to $50,000), civil, or criminal sanctions pursuant to section 65.4 of FIPPA where:

- there is willful or negligent viewing, collection, use, or disclosure of another individual's Personal Information in BCLC's Custody or under its Control without authorization; or
- there is a failure to notify the appropriate BCLC employee, affected individual(s), and/or Commissioner of a Privacy Breach.

Each case is handled on an individual basis with a full review of all the pertinent facts. The severity of a violation will determine the action taken.

Definitions

Defined (capitalized) terms or acronyms used but not defined in this Policy have the meaning attributed to them in the Policy Glossary.

Control (of information)	means the power or authority to manage the information during its life cycle, including restricting, regulating, and administering its use or disclosure.
Custody (of information)	means having physical possession of information. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security.

Privacy Management and Accountability

Information Sharing Agreement (ISA)	has the meaning ascribed to it in FIPPA (section 69) and, as at the date of this Policy, refers to an agreement between a public body and one or more of the following: • another public body; • a government institution subject to the *Privacy Act* (Canada); • an organization subject to the Personal Information Protection Act or the Personal Information Protection and Electronic Documents Act (Canada); • a public body, government institution or institution as defined in applicable provincial legislation having the same effect as FIPPA; • a person or a group of persons; • a prescribed entity, that sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement.
Initiative	means any current or proposed enactment, system, project, program, or activity.
Personal Information Bank (PIB)	has the meaning ascribed to it in FIPPA (section 69) and, as at the date of this Policy, an aggregation of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.
Privacy Impact Assessment (PIA)	has the meaning ascribed to it in FIPPA (section 69) and, as at the date of this Policy, refers to an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of FIPPA.
Privacy Breach	has the meaning ascribed to it in FIPPA upon Section 36.3 coming into effect. As at the date of this Policy and prior to 36.3 coming into effect, means the theft or loss, or the collection, use or disclosure that is not authorized by Part 3, of personal information in the custody or under the control of a public body.

Privacy Notice	means a written or verbal message satisfying the requirements under Section 27(2) of FIPPA. As at the date of this Policy, this section states a public body must ensure that an individual from whom it collects Personal Information is told: • the purpose for collecting it, • the legal authority for collecting it, and • the contact information of an officer or employee of the public body who can answer the individual's questions about the collection.
Privacy Protection Schedule (PPS)	refers to a standard form of contractual requirements that is included as part of an agreement between BCLC and a third party it hires. A PPS ensures the high privacy standards set by FIPPA are maintained for Personal Information held by third parties.

Policy Ownership

Contact Position	Manager, Information Governance
Policy Owner	Director, Data and Information Governance
Approving Body	Vice President, Legal, Compliance, Security

Policy

APPROVED

Privacy Management and Accountability

Revision History

Version	Effective	Approved by	Amendment
4.0	Apr 14, 2023	Vice President, Legal, Compliance, Security	Renamed, rewritten, and updated following a comprehensive policy review, legal changes, and changes in BCLC's practices, expectations, and organizational structure. Integrated existing direction for PIAs and privacy breaches into this policy so their separate corporate policies could be obsolesced. Introduced the "custodian" label to refer to individuals responsible for Personal Information. Added direction concerning requests for personal information from authorities outside of Canada. Assigned responsibilities to employees, contractors, custodians, and the Privacy team.
3.2	Oct 27, 2020	Vice President, Legal, Compliance, Security	Updates to authority titles to reflect changes following the organizational restructure for OneBCLC.
3.1	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.
3.0	Aug 19, 2013	Vice President, Corporate Security & Compliance	References to Director of Privacy changed to Director of Information Privacy and Security to reflect organizational change. Changes made to reflect integration of privacy and security assessment processes.
2.0	Mar 26, 2012	Director, Privacy	Revised to reflect amendments to FIPPA with respect to Privacy Impact Assessments.
1.1	Jan 24, 2011	Director, Privacy	References to Privacy Compliance Manager changed to Director of Privacy to reflect organizational change.
1.0	Apr 12, 2010	Vice President, Corporate Security & Compliance	Inaugural.