
Privacy Risk Assessment Procedure

[DRAFT - new]

Procedure No:	6700-PR3
Version:	1
Policy Reference	6700 Access and Privacy Management Program
Category:	Administrative
Approval Body:	Board of Governors
Executive Sponsor:	VP People, Culture, Inclusion (PCI)
Entity Responsible:	Information Access and Privacy Office (IAPO)
Directory of Records:	0650-15
Classification:	Information Management
Approval Date:	2026 Mxx DD [tbd]

Overview

This Procedure forms part of Policy 6700 Access and Privacy Management Program. It establishes the requirements and process for conducting Privacy Risk Assessments at BCIT.

Privacy Risk Assessments help identify and address privacy and information security risks when BCIT introduces new Initiatives, implements new technologies, procures services, or makes significant changes to existing programs, systems, or processes involving Personal Information.

Privacy Risk Assessments support BCIT's compliance with Part 3 of the *Freedom of Information and Protection of Privacy Act* (FIPPA), including section 69(5.3).

Objectives

This Procedure creates a consistent process for assessing Privacy Risks to ensure compliance with BCIT's Access and Privacy Management Program (Policy 6700) and FIPPA.

Application

This Procedure applies to all new or changed Initiatives at BCIT actually or potentially involving:

- collection, use, disclosure, storage of, or access to Personal Information;
- implementation of new technologies, including those incorporating artificial intelligence (AI);
- procurement or implementation of software or cloud-based services; or
- information sharing arrangements involving Personal Information.

All employees participating in the planning, development, approval, procurement, or implementation of such Initiatives must comply with this Procedure.

Program Sponsors must ensure that Initiatives within their area of responsibility are assessed in accordance with this Procedure.

Related Documents and Legislation

Provincial Legislation

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165

Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 155/2012

Personal Information Disclosure for Storage Outside Canada, B.C. Reg. 294/2021

BCIT Policy

6700 Access and Privacy Management Program

Related References

Minister of Citizens' Services Direction 2-21 *Privacy Impact Assessment Directions for Public Bodies that are Not Ministries*, (26 November 2021), issued under the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, s. 69(5.3).

Office of the Information and Privacy Commissioner for British Columbia. *Guidance on Disclosure of Personal Information Outside of Canada (s. 30 FIPPA)*, Guidance Document 2486 (2021).

Office of the Information and Privacy Commissioner for British Columbia. *Principles for responsible, trustworthy and privacy-protective generative AI technologies*. Guidance Document 2811 (2023)

Definitions

Definitions in Policy 6700 Access and Privacy Management Program apply to this Procedure, as well as the additional terms below:

Data Linking means the matching or combining of information from two or more datasets using a common identifier to create a new dataset or derive new information.

Data-linking Program means a program in which a dataset in the Custody or Control of a public body is linked with a dataset held by one or more other public bodies or agencies without the consent of the individuals whose Personal Information is contained in the datasets.

Foreign Supplement is an enhanced assessment of the privacy and data security measures protecting Sensitive Personal Information where the Information is stored outside Canada, in accordance with the *Personal Information Disclosure for Storage Outside of Canada Regulation*.

Privacy Impact Assessment (PIA) means the Privacy Risk Assessment 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 and Security Threshold Assessment (PSTA) means the preliminary Privacy Risk Assessment used to identify privacy and information security risks associated with new or significantly changed initiatives and to determine whether additional review or assessment is required. It is the initial screening tool within BCIT's Privacy Risk Assessment Framework used to ensure early identification of privacy and security considerations in project planning and decision-making.

Privacy Risk means the probability of actual or potential harms to an individual or the Institute arising from unauthorized collection, use, disclosure, or storage of Personal Information in BCIT's Custody or Control.

Privacy and Security Data Protection Schedule means the Schedule that may attach to a contract between BCIT and a Service Provider involving Personal Information. Its purpose is to:

- a) enable BCIT to comply with its obligations under FIPPA; and
- b) ensure that the Service Provider is aware of and complies with its obligations under FIPPA.

Program Lead is the assigned point of contact for the Privacy Risk Assessment responsible for documenting key details, identifying Personal Information flows, communicating with applicable Service Providers where appropriate, and ensuring the accuracy and completeness of the assessment.

Program Sponsor means the Business Owner or delegate responsible for the Initiative undergoing a Privacy Risk Assessment, with authority to allocate resources necessary for privacy and security requirements.

Sensitive Personal Information means Personal Information presenting heightened risk of harm to an individual if improperly collected, used, disclosed, or accessed. Sensitivity is determined in accordance with FIPPA, the Privacy Office and subject matter experts, based on the nature of the information and the context in which it is handled. Certain types of Personal Information that may be considered sensitive include health, financial, biometric, Indigenous, and/or information revealing race, beliefs, or sexual orientation.

Guiding Principles

This Procedure is guided by the following principles:

- 1) From the outset, privacy and information security considerations are integrated into the planning, design, and operation of Initiatives.
- 2) Assessments support better decision-making by evaluating the nature, likelihood, and impact of identified Risks and considering their mitigation.
- 3) Appropriate administrative, physical, and technical safeguards are implemented relative to the Sensitivity of the Information and the level of Risk.
- 4) Privacy Risk Assessment supports legislative, regulatory, contractual, and policy compliance.
- 5) Privacy Risks, mitigation, and residual Risks are documented to support governance and ongoing Risk management.
- 6) Privacy Risks are monitored throughout the lifecycle of Initiatives. Assessments are reviewed and updated when changes significantly affect privacy or information security risks.
- 7) Privacy Risk Assessments support privacy safeguards that are inclusive, equitable, accessible, and aligned with BCIT's commitment to the *IDEAS Lens (Indigenous, Inclusion, Diversity, Equity, Access, Sustainability, and Student Wellbeing)*.

- 8) BCIT will ensure that initiatives involving artificial intelligence are assessed proportionately to their level of risk. Where AI technologies introduce additional privacy, security, ethical, or governance considerations, enhanced assessment requirements may apply to support transparency, accountability, and compliance with legal and institutional obligations.

Procedure

The following are Privacy Risk Assessments that may be required for new or significantly revised Initiatives involving Personal Information, Institute data, technologies, systems, services, or business processes.

1. Privacy Risk Assessment Framework

The Privacy Risk Assessment Framework comprises the Assessments and related tools used to evaluate privacy and information security risks. The type of Assessment required depends on the nature of the Initiative and the level of risk identified during its review.

Privacy Risk Assessments need to consider whether an Initiative may create, reinforce, or reduce barriers for Indigenous Peoples and equity-deserving groups.

Assessment	Purpose	Trigger
PSTA	Initially identify privacy and information security risks and determine whether additional review is required.	All new and changed Initiatives. Example: Implementing a new software platform, student service, mobile application, or business process involving Personal Information.
PIA	Evaluating comprehensively FIPPA Part 3 compliance.	Elevated Privacy Risks identified through the PSTA or at the direction of the Privacy Officer. Example: Introduction of a new student information system, collection of new categories of Personal Information, or a major change to how Personal Information is used, accessed or disclosed.

Assessment	Purpose	Trigger
Foreign Supplement	Assessment of foreign storage, access, processing, or disclosure risks.	Sensitive Personal Information may be stored, accessed, processed, or disclosed outside Canada. Example: Use of a cloud-based service with servers outside Canada or foreign support services where Personal Information may be accessed.
Preliminary AI Privacy Risk Assessment	Determines if an AI-enabled Initiative involves Personal Information and requires further review (below).	Initiatives involving artificial intelligence and no Personal Information. Example: Using AI to analyze policy review dates and review priority based solely on metadata and document content.
AI Privacy Risk Supplement	Detailed assessment of AI-specific Privacy Risks.	AI Initiatives where additional privacy review is required. Example: Deployment of an AI tool that processes Personal Information, makes recommendations affecting people, or is integrated into a BCIT system involving Personal Information.

2. Privacy Risk Assessment Outcomes

The outcome of Privacy Risk Assessments may include additional due diligence, contractual safeguards, information-sharing arrangements, data governance controls, or other risk mitigation. Appropriate requirements are determined by the Privacy Officer based on the nature of the Initiative, the information involved, and the identified privacy and security risks.

Privacy and Data Protection Schedule

A Privacy and Data Protection Schedule may be required before entering, renewing, or materially amending a contract where a Service Provider collects, accesses, uses, stores, processes, transmits,

discloses, retains, or otherwise handles Personal Information on behalf of BCIT. The Schedule establishes privacy, security, access, retention, breach notification, and compliance requirements to support BCIT's compliance with FIPPA and other legislation.

Examples:

A Privacy and Data Protection Schedule is typically required when BCIT engages:

- Cloud-based software or SaaS providers storing employee or student information.
- Service Providers hosting, processing, or managing BCIT databases or providing support for BCIT systems containing Personal Information.
- External vendors providing student, employee, payroll, or HR services.
- Third parties conducting surveys, assessments, or research involving the collection of Personal Information.
- AI vendors processing Personal Information on BCIT's behalf.
- Contractors receiving access to BCIT systems or Records containing Personal Information.

Information Sharing Agreement (ISA)

An Information Sharing Agreement may be required when BCIT discloses, receives, or exchanges Personal Information with another organization on an ongoing, systematic, or recurring basis, and the arrangement is not otherwise fully addressed through legislation, a contract, or another formal authority.

The ISA documents the legal authority for the Information sharing, the purpose of the disclosure, the roles and responsibilities of each party, security and retention requirements, and Privacy Incident procedures.

Examples:

An Information Sharing Agreement is typically required when:

- BCIT and another public body regularly exchange Personal Information to administer a shared program.
- BCIT shares student information with a partner institution to support joint educational programs.
- BCIT provides Personal Information to a professional regulator, licensing body, or government organization under an ongoing arrangement.
- BCIT participates in a collaborative research, safety, wellness, or student-support Initiative involving recurring Information sharing.
- Multiple organizations require access to the same Personal Information to deliver coordinated services.

Research Agreement

A Research Agreement is required when BCIT participates in, sponsors, conducts, or collaborates on research activities involving Personal Information, confidential information, or data sharing with

external researchers, institutions, organizations, or funding partners. The Agreement establishes the legal authority for the collection, use, disclosure, retention, security, publication, and disposal of research data, and clarifies the roles and responsibilities of the parties.

Examples:

A Research Agreement is typically required when:

- BCIT researchers collaborate with another post-secondary institution on a research project involving Personal Information.
- Personal Information is shared with external researchers for an approved research purpose.
- A research sponsor or funding agency requires access to Personal Information data.
- A research project involves human participants and the collection, use, or disclosure of Personal Information.
- Multiple institutions contribute data to a joint research Initiative involving Personal Information.
- Research data involving Personal Information will be transferred to, stored by, or analyzed by an external organization.

3. Review and Approval

All required Assessments are reviewed and approved by the Privacy Officer, Chief Information Security Officer, or their designates, and the Program Sponsor.

Duties and Responsibilities

Program Lead

The Program Lead is an employee with direct knowledge of the Initiative under review and is responsible for:

- Initiating a PSTA for any new or changed Initiative that involves, or may involve, the collection, use, disclosure, processing or storage of Personal Information.
- Completing the Assessment and seeking input or assistance from BCIT business areas as needed (e.g., Information Technology Services, Teaching and Learning Unit, RDI, and the Records Management Office).
- Seeking information, clarification, or technical input from Service Providers where needed; however, the PSTA form itself is not disclosed to them.
- Upon request, providing any additional information required to complete the Assessment.

Program Sponsor

The Program Sponsor (Dean, Associate Dean, Director, Program Head, or their designate) is responsible for:

- Ensuring that all new or changed Initiatives within their area of responsibility are planned and Assessed in accordance with the requirements of this Procedure.

- Supporting the successful completion of PSTAs and PIAs as needed.
- Reviewing the documented outcomes, including any residual Risks.
- Ensuring the Initiative is implemented and operated in accordance with mitigation measures, risk response strategies, and conditions identified in completed PSTAs or PIAs.
- Notifying the Privacy Office of any material changes to an Initiative that may require additional Assessment.

IAPO

- Guides and supports the drafting and completion of PSTAs and PIAs.
- Develops, maintains, and updates PSTA and PIA templates, tools, and guidance materials for consistent application at BCIT.
- Maintains a repository of completed PSTAs and PIAs to support Institute recordkeeping, knowledge sharing, and oversight in accordance with BCIT policy and applicable legislation.
- Prior to final approval, reviews PSTAs and PIAs to ensure completeness, accuracy, and alignment with FIPPA and Policy 6700 Access and Privacy Management Program.

Privacy Officer

The Privacy Officer or designate is responsible for Privacy Risk Assessments per FIPPA and Policy 6700 Access and Privacy Management Program.

The Privacy Officer will:

- Recommend Risk mitigation proportionate to the assessed level of risk.
- Determine if a Supplemental Review is required for Personal Information stored outside Canada.
- Determine if an AI Supplemental Privacy Risk Assessment is required.
- Determine whether PIA obligations have been met by completion of the PSTA.
- Require PIAs where Initiatives pose a substantial Risk to individual privacy.
- Review and approve PSTAs and PIAs.
- Review privacy related provisions under relevant contracts.

Chief Information Security Officer (CISO)

The CISO or designate is responsible for:

- Assessing and documenting information security risks per Policy 3502 Cyber Security and related Standards.
- Recommending risk mitigation proportionate to the assessed level of risk.
- Reviewing and negotiating data security related provisions under relevant contracts.

Associated Forms

Forms are managed by and must be requested from the IAPO.

AI Privacy Risk Supplement
Foreign Supplement
Preliminary AI Privacy Risk Assessment
Privacy and Data Protection Schedule
Privacy Impact Assessment
Privacy Security Threat Risk Assessment
Research Agreement

Appendix

None

Approval History

	<u>Approval Date</u>	<u>Status</u>
Created: Procedure 6700-PR3 version 1 [Draft]	2026 Mmm dd [tbd]	pending

Scheduled Review Date

yyyy Month dd [tbd upon Executive or Board approval]; however, the Policy's Executive Sponsor may initiate review at any time.