SFU UNIVERSITY SECRETARIAT | ARCHIVES AND RECORDS MANAGEMENT DEPARTMENT

PRIVACY IMPACT ASSESSMENT (PIA)

for

Canvas Cloud

Table of Contents

Before you begin 2

PART ONE: PRIVACY REVIEW 2

Section 1: GENERAL INFORMATION 2

Section 2: COLLECTION, USE AND DISCLOSURE 8

Section 3: STORING PERSONAL INFORMATION 11

Section 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 13

Section 5: ACCURACY, CORRECTION AND RETENTION 16

Section 6: ADDITIONAL RISKS 17

Section 7: PRIVACY SIGNATURE 19

PART 2: SECURITY REVIEW 20

Section 1: PHYSICAL AND TECHNICAL SECURITY 20

Section 2: ACCESS CONTROL 21

Section 3: RISK RESPONSE 23

Section 4: IT COMMENTS AND SIGNATURE 25

PART 3: ACCOUNTABILITY REVIEW 27

Before you begin

This form is used by SFU to determine if a new or a proposed substantial change to a system, project, program or activity meets or will meet the protection of privacy requirements under Part 3 of the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA). FIPPA makes it a legal requirement that SFU conduct a PIA in accordance with the directions of the minister responsible for the Act. The PIA is a risk management and compliance tool to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly redesign; privacy complaints or breaches; and harm to personal, professional and institutional reputation.

Before you begin this form, please contact the Privacy and Access Program, through the Archives and Records Management Department. See more information about the process here: https://www.sfu.ca/archives/fippa/privacy-impact-assessments.html.

PART ONE: PRIVACY REVIEW

Section 1: GENERAL INFORMATION

PIA file number: 2024-073

Initiative title:	Canvas Cloud
SFU Department / Faculty:	IT Services
Branch or unit:	N/A
Link to SFU initiative website:	[Answer]
Link to vendor website:	https://www.instructure.com/canvas
Link to vendor privacy policy:	https://www.instructure.com/privacy-center
Your name and title:	Peter Onota, Project Manager
Your work phone and email:	peter_onota@sfu.ca
Initiative Lead name and title:	Keith Fong, Director, Application Services
Initiative Lead phone and email:	keith_fong@sfu.ca
Privacy Rep name and title:	Ernest Soares – Privacy Legal Counsel
Privacy Rep phone and email:	Ernest_soares@sfu.ca

A. Related PIAs, if any:

- PIA2022-001 Instructure Canvas LMS for SFU Beedie School of Business
- PIA2013-003 Learning Management System “Canvas@SFU”

B. If this initiative involves an external service provider or vendor, has a contract between SFU and the vendor been signed?

- Yes

C. Has SFU’s “Privacy Protection Schedule” been agreed to by the vendor?

- Yes

1. What is the initiative?

Canvas Cloud is a cloud-based Learning Management System (LMS) developed by Instructure, designed to enhance online and hybrid education for educational institutions, businesses, and organizations. It provides tools for creating, organizing, and delivering course content, including multimedia materials, quizzes, and assignments.

The purpose of this project is to migrate from the self-hosted, open-source version of SFU’s Canvas Learning Management System (LMS) to the vendor-hosted Canvas Cloud product. SFU’s centrally supported LMS serves as a foundational platform for teaching and learning. An average of 26,000 undergraduate and graduate students enroll in Canvas courses each term. With Canvas Cloud, SFU has an opportunity to take advantage of functionality that is not available in the self-hosted, open-source version.

2. What is the scope of the PIA?

This PIA covers the implementation of the Canvas Cloud product for credit and non-credit courses offered by SFU’s academic units and Lifelong Learning, as well as non-academic courses made available to employees for training and knowledge sharing purposes.

This PIA does not cover use of tools that are possible to integrate with the Canvas environment that may use data centres beyond those run by Instructure in the AWS Canada Zone. Any future integrations will require separate assessments for privacy and security compliance.

3. What are the data or information elements involved in your initiative?

3.1.1 Student Information – Credit Students

- Name
- SFU ID (student number)
- SFU email address
- Course enrollments
- Additional personal information as entered by the student (profile details, assignments, quizzes, opinions in published posts and comments

Collection: Secure data exchange processes automatically send student information (i.e., name, SFU ID (student number), SFU email address, course enrollments) from SFU's main Systems of Record (goSFU, Amaint) to Canvas Cloud. These exchanges are managed and controlled by IT Services. Some data elements may flow to external, third-party (LTI) tools, each of which has its own PIA. Students may also voluntarily submit additional personal information such as profile details, assignments, quizzes, and opinions in published posts and comments.

Access: Instructors and Teaching Assistants (TAs) are only authorized to access information about students enrolled in their course. Staff in IT Services, the Centre for Educational Excellence, and administrative staff in academic units may access information about a broader pool of students (e.g. students within a given program or Faculty) for support purposes. Instructors and administrators may access information about student engagement activity (e.g., page views). Students may access the names, published discussion posts and comments for classmates who are also enrolled in the same course as the student.

Logs of activities, IP addresses and other information necessary for security, audit logging, and similar operational activities of the service by Instructure are visible to their staff under Instructure's Data Classification, Handling and Encryption Policy. Customer data and identity information is classified as Confidential under this policy, encrypted at rest, and shared only with appropriate and authorized personal when necessary.

Use: Student information is used within authorized Canvas courses for learning and assessment purposes. Participation in course activities including accessing and responding to discussion items, submitting assignments and quizzes, and retrieving course content. Identity information is used to control access to resources appropriate to the role that a student has in a course.

Disclosure:

1. IT Services staff who are responsible for troubleshooting technical issues and administrating the application at an enterprise level.
2. CEE staff who are responsible for supporting instructors in the delivery of their courses, troubleshooting functional issues, and administrating the application at an enterprise level.
3. Academic unit administrative staff who are responsible for administrating Canvas courses and providing support for their individual programs.
4. Instructors who view submitted content from students as well personal information related to enrollment and participation in the courses they are teaching.
5. Students authorized to view the names of, and content published by, their fellow classmates.

Retention: Course data is retained on the server after the course is completed unless deleted by a course administrator. SFU course content that is used to evaluate a student is required to be kept for one year following the final exam of a course in order to support grade appeal processes. See RRSDA 1995-018, Examination Papers and Course Assignments. Student information is required while the student is in a program that requires access to Canvas and will be maintained in the Canvas user database until deleted/removed by administrative staff or via deprovisioning processes.

3.1.2 Student Information – Non-Credit Students

- Name
- Student ID number
- External email address
- Course enrollments
- Additional personal information as entered by the student (profile details, assignments, quizzes, opinions in published posts and comments

Collection: Secure data exchange processes automatically send student information (i.e., name, external email address) from Lifelong Learning's main Systems of Record (SERA or Modern Campus) to Canvas Cloud. These exchanges are managed and controlled by IT Services through an integration. Some data elements may flow to external, third-party (LTI) tools, each of which has its own PIA. Lifelong Learning students may also voluntarily submit additional personal information such as profile details, assignments, quizzes, and opinions in published posts and comments.

Access: Instructors are only authorized to access information about students enrolled in their course. Staff in IT Services and Lifelong Learning may access information about a broader pool of students based on their level of access. Instructors and administrators may access information about student engagement activities (e.g., page views).

Logs of activities, IP addresses and other information necessary for security, audit logging, and similar operational activities of the service by Instructure are visible to their staff under Instructure's Data Classification, Handling and Encryption Policy. Customer data and identity information is classified as Confidential under this policy, encrypted at rest, and shared only with appropriate and authorized personnel when necessary.

Use: Student information is used within authorized Canvas courses for learning and assessment purposes. Participation in course activities including accessing and responding to discussion items, submitting assignments and quizzes, and retrieving course content. Identity information is used to control access to resources appropriate to the role that a student has in a course.

Disclosure:

1. IT Services staff who are responsible for troubleshooting technical issues and administrating the application at an enterprise level.
2. Lifelong Learning staff who are responsible for supporting instructors in the delivery of their courses, troubleshooting functional issues, and administrating the application at a departmental level.
3. Instructors who view submitted content from students as well personal information related to enrollment and participation in the courses they are teaching.
4. Students who may view the names of, and content published by, their fellow classmates.

Retention: Course data is retained on the server after the course is completed unless deleted by a course administrator. SFU course content that is used to evaluate a student is required to be kept for one year following the final exam of a course in order to support grade appeal processes. Student information is required while the student is in a program

that requires access to Canvas and will be maintained in the Canvas user database until deleted/removed by administrative staff or via deprovisioning processes.

3.2 Instructor/Employee Information

- Name
- SFU employee number
- SFU email address
- Course teaching assignments

Collection: Secure data exchange processes automatically send instructor information (i.e., name, SFU employee number, SFU email address, course assignments) from SFU's main Systems of Record (goSFU, myINFO, Amaint, SERA/Modern Campus) to Canvas Cloud. These exchanges are managed and controlled by IT Services.

Access: Secure, centralized identity management mechanisms automatically send instructor data from the above Systems of Record to Canvas courses. Instructor data may be accessed by authorized administrative staff. Instructors may be able to view the names, email addresses, and published content of instructors and TAs who are also assigned a teaching role in the same course. Administrative staff who are managing courses for employee groups will be able to view the names, email addresses, and published content of employees.

Logs of activities, IP addresses and other information necessary for security, audit logging, and similar operational activities of the service by Instructure are visible to their staff under Instructure's Data Classification, Handling and Encryption Policy. Customer data and identity information is classified as Confidential under this policy, encrypted at rest, and shared only with appropriate and authorized personnel when necessary.

Use: Instructor/employee information is used within authorized Canvas courses for teaching purposes. Identity information is used to control access to resources appropriate to the role that an instructor has in a course and to make it possible for students to identify and communicate with the instructor as needed.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference. For example:

- *names, home addresses, emails, and telephone numbers of the individual or of their guardians or family members;*
- *images of the individual;*
- *anyone else's opinions about an individual;*
- *an individual's personal views or opinions;*
- *identifying number (e.g., student number, employee number, health care number;*
- *age, sex, gender, marital status, race, national or ethnic origin;*
- *religious or political beliefs or associations;*
- *educational, medical, criminal, financial, employment history.*

Type "yes" or "no" to indicate your response.

Yes

- ***If yes**, are all of the personal information elements you are collecting necessary for your initiative?*
  - Yes
- ***If no,** how will SFU reduce the risk of unintentionally collecting personal information? After you Answer this question, submit this PIA to the Access and Privacy Program. **You do not need to complete the rest of the PIA template**.*
  - N/A

Section 2: COLLECTION, USE AND DISCLOSURE

4. Collection, use and disclosure flow

Describe the information flow of your initiative in the below chart.

- **Collection**: *Describe the steps in collecting personal information from individuals by SFU and/or the vendor (be sure to clarify which party is collecting the information).*
- **Use**: *How does SFU and/or the vendor use personal information (be sure to clarify which party is using the information)?*
- **Disclosure**: *When, if ever, would SFU and/or the vendor provide the personal information to an internal or external third party that does not normally have access to the personal information?*

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FIPPA authority** *See the most common FIPPA authorities listed below this chart.*	**Other legal authority**
Step 1: Secure data exchange processes automatically send instructor information (i.e., name, SFU employee number, SFU email address, course assignments) from SFU's main Systems of Record	Collection	26(c)	
Step 2: Student information is used within authorized Canvas courses for learning and assessment purposes. Instructor information is used within authorized Canvas courses for teaching purposes. Identity information is used to control access to resources appropriate to the role that an instructor has in a course and to make it possible for students to identify and communicate with the instructor as needed.	Use	32(a)	
Step 3: The vendor may use personal information to provide support and improve their products as detailed in the agreement and attached SFU PPS.	Use	32(a)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority *See the most common FIPPA authorities listed below this chart.*	Other legal authority
The vendor's administrators may monitor sessions, at SFU's request, to install, implement, maintain, repair, troubleshoot or upgrade the system.	Disclosure	33(2)(d)	

Most Common FIPPA Authority References

For more options, see the full text of FIPPA (link).

Type	Description	Section
Collection	The collection of the information is expressly authorized under an Act	26(a) **and list the enactment and section above*
	The collected information relates directly to and is necessary for a program or activity of the University.	26(c)
	The collected information is necessary for the purposes of planning or evaluating a program or activity of the University.	26(e)
Use	Use of the information is for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.	32(a)
	The individual the information is about has consented to the use (*If using this authority, provide a copy of the consent language after your collection notice, below)*	32(b)
	Use of the information is for a purpose for which the information may be disclosed to the public body under FIPPA s. 33	32(c) **also list which authority under s.33*
Disclosure	The individual the information is about has consented to the disclosure (*If using this authority, provide a copy of the consent language after your collection notice, below).*	33(2)(c)
	Disclosure of the information is for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose. (*If you select this authority, ensure the disclosure is described in the collection notice, below).*	33(2)(d)
	Disclosure of the information is in accordance with an enactment of British Columbia or of Canada that authorizes or requires the disclosure: *[insert detail]*	33(2)(e) **and list the enactment and section*

***Optional**: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.*

5. Collection Notice and Consent

5.1 Collection Notice: *If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice (except in limited circumstances). If your vendor is collecting personal information on behalf of SFU, the vendor must also provide a collection notice.*

Review the template collection notice and update as applicable. Consider whether you will need more than one collection notice.

Collection Notice

The personal information on this site is collected under the authority of the University Act (R.S.B.C. 1996, c.468) and Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165). It relates directly to and is necessary for the University to admit, enroll and keep a record of students' academic performance, progress and graduation. If you have any questions about the collection, use and disclosure of this information please contact the Associate Registrar, Information, Records and Registration Services, telephone 778.782.6930.

Disclosure Notice

Pursuant to the British Columbia Freedom of Information and Protection of Privacy Act (RSBC 1996, c.165), by enrolling in a course or program at the university, you consent to the university disclosing and storing your personal information, as needed for purposes consistent with those outlined above. You acknowledge and understand that your personal information may be shared internally within the university as needed, as well as with the following organizations when necessary:

- Canada Revenue Agency for tax reporting purposes: student contact information, social insurance number (if provided by student), mailing address, tuition and registration Information
- SFU Alumni Engagement Office for ongoing alumni engagement purposes: student contact information, program title, program completion date
- Government of British Columbia for grant application approval purposes when applicable: this information includes personal information (such as student contact information, Aboriginal status, status in Canada [Canadian Citizen, PR, protected person, etc.]), education history, and financial information (such as previous funding from other organizations, e.g., grants, scholarships).

5.2 Consent: *If you are obtaining consent for the use or disclosure of personal information, add any consent language here.*

Consent must have the following elements:

a) be in writing; and
b) be done in a manner that specifies:
    a. the personal information for which the individual is providing consent;

b. *the date on which the consent is effective and, if applicable, the date on which the consent expires;*
c. *for "use" consent, the use of the personal information; and*
d. *for "disclosure" consent:*
    i. *to whom the personal information may be disclosed;*
    ii. *if practicable, the jurisdiction to which the personal information may be disclosed; and*
    iii. *the purpose of the disclosure of the personal information.*

The below consent notice is posted at https://canvas.sfu.ca

> Read the complete Canvas Privacy Protection Notice. By using Canvas you confirm that you have read, understand and agree to this notice.

The Canvas Privacy Protection Notice reads:

> Protection of privacy rights and responsibilities at SFU is administered according to the provisions of BC's *Freedom of Information and Protection of Privacy Act* (the Act) and the University's Information Policies, published in its Policy Gazette.
>
> SFU must comply with protection of privacy requirements under the Act, which specifies when and how the university, its employees, service providers and volunteers are permitted to collect, access, use, disclose, store and retain personal information.
>
> By using the learning management system, you acknowledge that you have read, understood and agreed to the notifications and policies that are displayed, or linked to, on this page.

Section 3: STORING PERSONAL INFORMATION

6. Is any personal information stored outside of Canada?

Yes

All Canvas data is hosted in Canada. Support ticket data is hosted in the USA which may contain some personal information.

- *If yes, where (e.g. which states or countries)?*
    - [Answer]

7. Has the vendor agreed to notify SFU if it changes the country in which personal information is stored?

If the vendor has agreed to SFU's Privacy Protection Schedule, then the answer is 'yes'. If 'no', add this as a risk in section 6 "Additional Risks".

Yes

8. Does your initiative involve sensitive personal information that will be stored outside of Canada?

"Sensitive" is not defined. What information is sensitive may depend on the context. Examples can include medical information, unique government issued identifiers (passport number, driver's license, PHN, SIN), financial information, disciplinary or complaint history, ethnic and racial origins, an individual's sexual orientation, religious or philosophical beliefs, etc. You may need help from the Access and Privacy Program to determine whether the personal information is "sensitive".

No

- *If yes, go to question 9.*
- *If no, then skip ahead to Section 5.*

~~9. Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public?~~

~~*Type "yes" or "no" to indicate your response. "No" is the most likely response.*~~

~~[Answer]~~

- ~~*If yes, what enactment? Then skip Section 4 and go to Section 5.*~~
  - ~~[Answer]~~
- ~~*If no, go to Section 4.*~~

Section 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

WAIT! *Complete Section 4* ***only if sensitive*** *personal information will be stored outside of Canada. See question 8, above, for an explanation of what may be "sensitive".*

10. Storage details

Fill in the table below (add more rows if necessary)

Name of service provider (including subcontractors)	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

11. Does the contract you rely on include privacy-related terms?

[Answer]

- *If yes, describe the contractual measures related to your initiative, or copy the terms in here.*
  - [Answer]
- *Has SFU's Cloud Privacy Protection Schedule been appended to the contract?*
  - [Answer]

12. What controls are in place to prevent unauthorized access to sensitive personal information?

[Answer]

13. Provide details about how the vendor will track access to sensitive personal information (e.g. logging access to data).

[Answer]

14. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	**Impact to individuals** (low, medium, high)	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information** (low, medium, high)	**Level of privacy risk** (low, medium, high, considering the impact and likelihood)	**Risk response** (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	**Is there any outstanding risk?** **If yes, please describe.**

Examples of privacy risks	**Examples of risk responses**
Vendor has access to the sensitive personal information on an ongoing basis. This is known as standing access. Standing access increases the risk of an unauthorized disclosure of personal information.	Time limited access where access ends automatically after a set period of time.
Vendor is subject to laws that may compel them to disclose the public body's personal information to another entity without notifying the public body. In this case, the public body may not have an opportunity to contest the disclosure, which may be unauthorized under FIPPA. Assessing this risk should take into consideration the sensitivity of the information and likelihood of occurrence.	Contractual language
The vendor uses third-party subcontractors that they do not agree to be accountable for related to privacy practices.	Contractual language
The jurisdiction in which sensitive personal information is stored does not respect the rule of law or has no privacy laws.	Contractual language (note there will likely be outstanding risks)

Examples of privacy risks	Examples of risk responses
Retention of personal information longer than is necessary, which increases the risk of unauthorized use, access, and disclosure.	Retention schedules, contractual language
Vendor refuses to agree to SFU's Privacy Protection Schedule.	Other contractual privacy language (does the vendor agree it is a service provider subject to FIPPA?)

15. Outcome of Section 4

The outcome of Section 4 will be a risk-based decision made by the role designated accountable (see Part 3) on whether to proceed with the initiative, with consideration of the risks and risk responses, including consideration of the outstanding risks in question.

Is the outcome to proceed with the initiative?

[Answer]

Section 5: ACCURACY, CORRECTION AND RETENTION

16. How will SFU make sure that the personal information is accurate and complete?

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. For example, information collected is provided directly by the individual for a known purpose, information used is not outdated, etc.

- Students use a self-serve update procedure in the student information system (goSFU)
- Instructors send requests for updates to Human Resources

17. Requests for correction

FIPPA gives an individual the right to request correction of errors or omissions to their personal information. SFU's formal process to respond to these requests is here: Requesting a Correction to Personal Information in University Records.

17.1 What process is in place to correct personal information?

- For credit courses, students and instructors are able to correct personal information directly in the source System of Record (goSFU or MyINFO).
- For non-credit courses, students can correct personal information directly in the source System of Record (SERA/Modern Campus). Instructors may ask Lifelong Learning staff to update personal information in the System of Record.

17.2 Sometimes it's not possible to correct the personal information. FIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

Yes

17. 3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year to one or more third parties, FIPPA requires you to notify the parties you disclosed to of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

Yes

18. Does your initiative use personal information to make decisions that directly affect an individual?

Yes

- If yes, go to question 19
- If no, skip ahead to Section 6

19. Do you have a records retention schedule in place related to personal information used to make a decision?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

RRSDA-1995-018 Examination Papers, Course Assignments, and Grades
RRSDA-1999-002 Course Files

- *If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.*
    - [Answer]

Section 6: ADDITIONAL RISKS

20. Has the vendor expressed, either through contract, communications with you, or their privacy policy, their agreement to notify SFU of a privacy breach?

Under s.30.5 of FIPPA, an SFU employee or service provider to SFU "who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the [University Archivist and Coordinator of Information and Privacy]".

Privacy breaches can be reported to SFU here:
https://www.sfu.ca/archives/fippa/breaches-complaints/report-respond-to-a-breach.html

Yes

21. Risk Response (non-security risks)

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

If you filled in the risk table at Q.14 for sensitive information stored outside of Canada, only include additional risks here.

Add new rows if necessary.

Possible (non-security) risk	Proportionate response / mitigation strategies	Mitigation strategy to be implemented (Y / N / Already done)	Deadline date for implementation
Risk 1: Non-compliance with FIPPA privacy notification	Collection and privacy notices will be presented to users	Y	September 2, 2025
Risk 2: Vendor does not comply with BC's FIPPA	Vendor will sign SFU's PPS	Already Done	January 31, 2025
Risk 3: Retention of personal information longer than is necessary, which increases the risk of unauthorized use, access, and disclosure.	Retention schedules will be enforced Vendor will sign SFU's PPS	Y	

Examples of (non-security) privacy risks	Examples of risk responses / strategies
Vendor is subject to laws that may compel them to disclose the public body's personal information to another entity without notifying the public body (e.g. The USA's *Patriot Act*). In this case, the public body may not have an opportunity to contest the disclosure, which may be unauthorized under FIPPA.	Contractual language
The vendor uses third party subcontractors that they do not agree to be accountable for related to privacy practices.	Contractual language
The jurisdiction in which sensitive personal information is stored does not respect the rule of law or has no privacy laws.	Contractual language (note there will likely be outstanding risks)

Examples of (non-security) privacy risks	Examples of risk responses / strategies
Retention of personal information longer than is necessary, which increases the risk of unauthorized use, access, and disclosure.	Retention schedules, contractual language
Vendor refuses to agree to SFU's Privacy Protection Schedule.	Other contractual privacy language (does the vendor agree it is a service provider subject to FIPPA?)
Unauthorized use or disclosure by internal SFU staff members with authorized access.	SFU staff sign privacy and confidentiality agreements and are bound by FIPPA and SFU policy I10.11 SFU staff will be trained on privacy protection risks and solutions
Collection notices do not accurately reflect how personal information will be used. Care must be taken that personal information is used for the purpose for which it was obtained or compiled, or for a use consistent with that purpose.	Ensure any future new uses of personal information are first vetted against existing collection notices and amend as necessary.
Inaccurate (i.e., outdated) information is used to make a decision that directly and adversely affects an individual	RRSDAs; Develop mechanisms for ensuring personal information remains up to date and in-sync with related systems.

Section 7: PRIVACY SIGNATURE

This PIA was conducted by the Delegated Authority below, in accordance with the Minister of Citizens' Services Direction 2-21 and SFU Policy I 10.02 'Head of the Institution and Delegation of Authority under FIPPA'.

Under SFU's Protection of Privacy Policy I 10.11, the Access and Privacy Program is responsible for advising on, reviewing, and recommending for approval Privacy Impact Assessments (s.6.1.2).

Role	Name & title	Signature	Date signed
Privacy program representative (Delegated Authority)			

22. Is the Delegated Authority's signature contingent upon review and signature by Information Security per Part 2?

If yes, provide PIA to Information Security to complete Part 2, below.

Yes

PART 2: SECURITY REVIEW

In this Part, you will share information about the privacy aspect of securing personal information with an SFU Information Security reviewer. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

Section 1: PHYSICAL AND TECHNICAL SECURITY

1. SFU's Security Arrangements

Will the initiative involve a new system at SFU for storage or access to records, with unique physical or technical security measures to what already exists for SFU records?

Type "yes" or "no" to indicate your response.

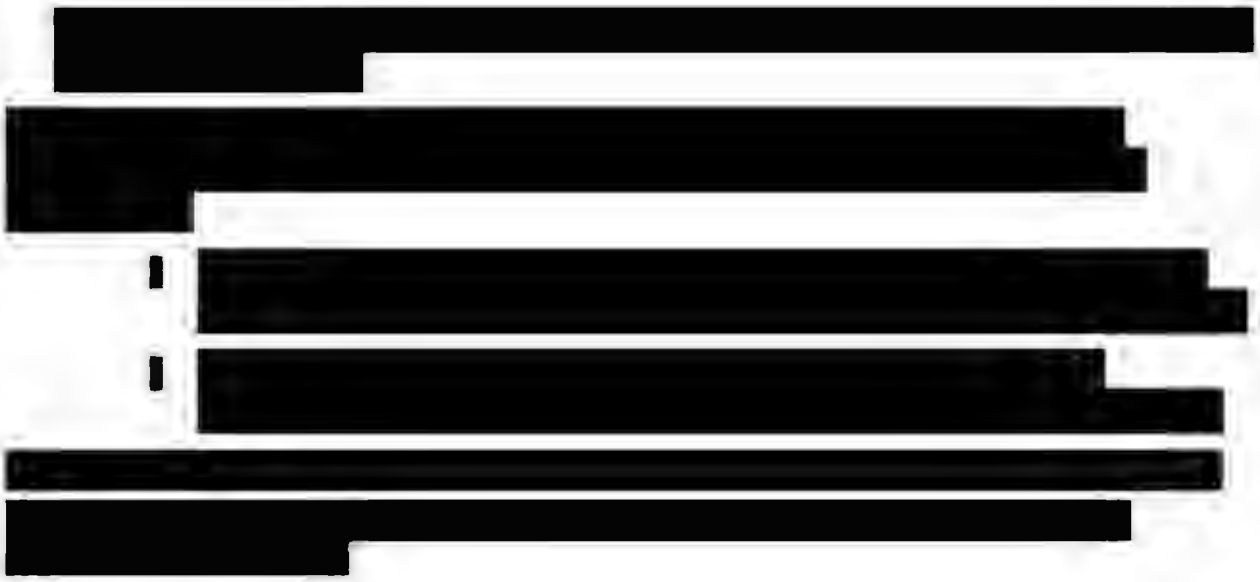
No

- *If yes, describe where the records for your initiative are stored (e.g., on the University's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc. See Schedule A, below, for a list of security measures.*
    - [Answer]

2. Vendor's Security Arrangements

If this initiative involves a vendor, what are their physical and technical security arrangements for protecting the personal information in their custody against such risks as unauthorized collection, use, disclosure, or storage?

[redacted]



Section 2: ACCESS CONTROL

3. Controlling and tracking access

Please check each strategy that describes how you or your vendor limits or restricts who can access personal information and how you keep track of who has accessed personal information in the past. Insert additional strategies if needed.

Strategy	Yes/No

Strategy	Yes/No
Describe any additional controls:	[redacted]

Section 3: RISK RESPONSE

4. Risk Response (Security Risks)

Describe any security risks that arise in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible security risks	Proportionate response / mitigation strategies
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	

Examples of security risks	Examples of risk responses / strategies
Standing access: Vendor has access to the personal information on an ongoing basis, which increases the risk of an unauthorized disclosure of personal information.	Time limited access where access ends automatically after a set period of time.
System and data security breached by a hacker.	Security measures and policies
Individual's personal data is compromised while in transmission.	Security measures
Unauthorized access by SFU employees to the data.	Ensure access and permissions are set up to best practice recommendations. Implement standard off-boarding when employees' roles change or leave SFU.

Section 4: IT COMMENTS AND SIGNATURE

This section is to be filled in by the ITS reviewer.

5. Does this initiative have reasonable security arrangements?

- Yes

6. Comments / Recommendations:

-

Role	Name & title	Signature	Date signed
Information Security representative	Steve MacGregor, CIPT, PCI ISA Information Compliance Architect		June 11, 2025

PART 3: ACCOUNTABILITY REVIEW

The Minister of Citizens' Services Direction 2-21, "Privacy Impact Assessment Directions" requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s.D8).

Accountability is maintained by the role or position, regardless of who fills the role.

The role ultimately responsible for deciding whether or not to implement the initiative referred to in this PIA is the role most likely to be appropriate for holding accountability.

Under SFU's Protection of Privacy Policy I 10.11, administrators are responsible for:

- *ensuring that the activities of their departments are in compliance with the privacy principles articulated in the Policy;*
- *preparing Privacy Impact Assessments; and*
- *abiding by the requirements of a completed Privacy Impact Assessment, including taking steps to correct or mitigate any privacy issues or foregoing the implementation of an initiative if the implementation is in violation of FIPPA or SFU policies.*

Holding accountability for the privacy risks of this initiative includes:

- *reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;*
- *making a risk-based decision on whether to proceed with the initiative, with consideration of the risks and risk responses, including consideration of the outstanding risks in question;*
- *ensuring accountability is transferred to any individual who assumes this role;*
- *if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the Access and Privacy Program is engaged, and if necessary, completing a PIA update; and*
- *understanding what your privacy obligations are, and if not, following up with the Privacy and Access Program.*

Accountability includes affirming that this PIA accurately documents the data elements and information flow at the time of signing.

Role	Name & title	Signature	Date signed
Initiative lead			
Role designated accountable for the operational oversight			
Role designated accountable for the business risk	Paul Kingsbury Associate Vice-President Learning and Teaching		June 23, 2025

Schedule A

Types of security measures	
Physical	1. SFU data centre and backup data centre are both located on SFU campuses in Canada 2. Locked doors 3. Key card and electronic access control devices 4. Securely stored computing equipment 5. Receptionist supervision 6. Physical barrier to the public 7. Staff only access 8. Alarm systems 9. After hours security patrol checks
Technical	1. Firewalls 2. Encrypted network transmission 3. Tiered network infrastructure 4. Identity assurance provided by SFU's main Systems of Record 5. Role-based user access assigned on a need-to-know basis 6. Log-on user ID and password (single sign-on) provided by SFU's Central Authentication Service (CAS) 7. Timed out computer sessions
Security Policy, Procedure and Standards	1. University Policies e.g., GP-24 Fair Use of Information Systems, I 10.04 Access to Information and Protection of Privacy, I 10.05 Collection of Personal Information, I 10.09 Retention and Disposal of Student Exams or Assignments, and I 10.10 Confidentiality Policy 2. Designation and authentication of authorized users is managed through SFU's Identity and Access Management (IDAM) infrastructure, which is registered with the Canadian Access Federation (CAF) 3. SFU's IDAM infrastructure is benchmarked against the InCommon assurance program (http://incommn.org), which certifies campuses, non-profits and research organizations to determine the accuracy of a user's electronic identity and help mitigate risk for the service provider. While InCommon certification is not available outside the US, the assurance program serves as a benchmark for international standards and best practices 4. SFU's Privacy Protection Schedule is included as part of a signed agreement with a service provider of digital storage when purchased through Procurement, which includes provisions relating to data

	ownership, use, disclosure, security, retention and confidential/permanent deletion 5. SFU has signed an Information Sharing Agreement with the public body describing the terms and conditions of their data-linking initiative or common or integrated program or activity 6. Authorized users of the IT system are made aware of protection of privacy rights and responsibilities by means of notices when logging onto the system; education by through the SFU website, workshops and advisory service; and/or signing SFU's Privacy and Confidentiality Agreement 7. Personal information is retained and disposed of according to an existing Records Retention Schedule and Disposal Authority approved by the University Archivist
Tracking Access / Access Controls	1. IDAM infrastructure assures identity 2. Role-based access management infrastructure authorizes access 3. Auditable log files