SFU UNIVERSITY SECRETARIAT | ARCHIVES AND RECORDS MANAGEMENT DEPARTMENT

PRIVACY IMPACT ASSESSMENT (PIA)

for

Ednius Copilot for Educators Pilot Program

Table of Contents

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: 2024-048

Initiative title:	[Ednius Copilot for Educators]
SFU Department / Faculty:	[Beedie School of Business]
Branch or unit:	[Graduate Programs]
Link to SFU initiative website:	[https://beedie.sfu.ca/]
Link to vendor website:	[https://www.ednius.com/]
Link to vendor privacy policy:	[https://app.ednius.com/privacy]
Your name and title:	[Jose Luis Dominguez Damas – Associate Director, Business Solutions]
Your work phone and email:	[No work phone assigned – josed@sfu.ca]
Initiative Lead name and title:	[Maria Szymczak – Director, Graduate Program Delivery]
Initiative Lead phone and email:	[No work phone assigned – mdelguer@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:

- Not applicable

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

- A contract has been signed.

C. Has SFU's "Privacy Protection Schedule" been agreed to by the vendor?

- Yes

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

Ednius Copilot for Educators is an AI-powered tool designed to assist educators with providing feedback and grading. The product will undergo a pilot testing phase during its first year of implementation before any broader adoption across other courses. Initially, it will be used exclusively in the following course: BUS 557 G300.

BUS 557 G300, comprised of around 35 students, consists of the following student evaluation criteria that will be piloted with the Ednius system:

> Four assignments, i.e. four quizzes. Each quiz is composed of a set of short answer questions and will affect up to 10% of students' grade for a total of 40%.

After the pilot program is completed, an addendum to the Privacy Impact Assessment (PIA) will be conducted for potential implementation across all courses within the Beedie School of Business.

The implementation of Ednius Copilot for Educators, an AI tool, is expected to start during the Fall 2024 – 1247 term, as a way to add more value for the learning experience in the Beedie School of Business Graduate Programs. Ednius Copilot for Educators will be part of the tools used during the courses, if applicable.

Ednius Copilot for Educators is an AI-based tool that can analyze and personalize grades and feedback for student responses, based on criteria established by course leaders. The application evaluates and suggests grades and feedback by comparing the

student's assignment and exam responses to a rubric provided to Ednius by the educator. The aim of using Ednius is to assist Professors, Teaching Assistants, and Markers in making more efficient decisions. However, the final decision on grades and feedback rests entirely with the course leader (could be only the faculty in charge), who, along with Professors, Teaching Assistants, and Markers, has the discretion to determine what percentage of the suggested grades and feedback provided by Ednius Copilot for Educators will be utilized.

The tool will be managed by the Faculty and/or Staff at the Beedie School of Business. Students will not need to create any account or provide any further information.

Ednius uses artificial intelligence (AI) technologies (specifically, the GPT-4 family, Llama 3, and Phi 3) to automate and enhance the grading process, integrating directly with Learning Management Systems (LMS) like Canvas through APIs.

The operational process starts when an instructor finalizes a quiz on Canvas. At this stage, Ednius utilizes the Canvas API (using the user authorization and developer keys provided) to retrieve the quiz content and students' responses, while excluding personal identifiers like names or Student IDs. Once the responses are imported into Ednius, advanced AI models perform a thorough analysis of each answer. These models evaluate how well each response aligns with the predefined rubric criteria (which might be provided by the professor) and the correct answers set by the instructor (which must be provided by the professor). The AI is designed to understand various writing styles, ensuring that grading is consistent, accurate, and impartial. The Marker/Professor will retain the final decision and will review the feedback and grades before assigning them

After the AI completes its evaluation, Ednius produces personalized grades and feedback for each student, highlighting the strengths of their responses and pinpointing areas for improvement. Instructors will review, adjust, and finalize this feedback on the Ednius platform before it is sent back and posted on the LMS. This process, initiated at the user's discretion, once again utilizes the Canvas APIs and the anonymized submission ID key provided by Canvas for each student submission.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This PIA is exclusively for the Ednius pilot program related to the BUS 557 G300 course.

The product will undergo a pilot testing phase during its first year of implementation before any broader adoption across other courses. Initially, it will be used exclusively in the following course: BUS 557 G300

After the pilot program is completed, an addendum to the Privacy Impact Assessment (PIA) will be conducted for potential implementation across all courses within the Beedie School of Business

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

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative.

Consider segmenting your response into the different categories of people who you will collect different types of information from (e.g. students, administrators, employees, alumni, etc.).

Please include where the information is coming from (directly from users, pulled from pre-existing SFU databases, etc.).

The personal information collected may include:

- Individual's personal views or opinions
- Identifying number*

*For the Canvas integration, Ednius utilizes the "submission_id" as the unique identifier, which is generated for each student upon submitting an assignment (randomized for every submission). Additionally, the API provides access to an anonymous "user_id" associated with the Canvas user (distinct from the student ID or other personal details), but Ednius does not use or store this data. The rate at which this identifier changes is subject to SFU's IT policies.

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**.*
  - Answer

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: The professor / Beedie Graduate Programs Course Production Staff creates a quiz/assignment in Canvas. In Ednius, the professor or Beedie Graduate Programs Course Production Staff will import course information from Canvas, which at this stage will include only the selected quizzes and assignments. The professor will then add the correct answers and optional grading notes in Ednius, linked to the imported Canvas content.	n/a	n/a	
Step 2: Students log into Canvas and the course modules accordingly, complete the quiz/assignment, and submit their final answers.	Collection	26(c)	

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 3: The quiz/assignment, along with the students' responses, will be imported/ synced to the Ednius platform from the Canvas Course Modules to be analyzed and evaluated comparing the submission with the required correct answers, and optional grading notes from the professor.	Use Disclosure	32(a) 33(2)(d)	
Step 4: Ednius analyzes the students' quiz/assignment imported responses, generating suggested feedback by comparing them to the required correct answers and optional grading notes provided by the professor.	Use	32(a)	
Step 5: Ednius suggested feedback will be reviewed by the course professor who might adjust, re-process or approve the feedback suggested by Ednius, thereafter the course professor will finalize the feedback for the students, and assign a final grade.	Use	32(a)	
Step 6: The finalized feedback and assigned final grades are sent back to Canvas, where they are made available for the students to view in the Course Module accordingly.	Use	32(a)	

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*

Type	Description	Section
	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.

The below collection notice will be posted Canvas Course Page when applicable.

Canvas Course Page Collection Notice

> Ednius Copilot for Educators Pilot Program collects personal information on behalf of SFU under the authority of the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c.165). The personal information collected includes your personal opinions, and assignment and/or exam responses.

It is related directly to and needed by the University to enhance the grading and feedback process for students by leveraging AI technology. The information will be used to personalize and propose grades and feedback for students' responses, based on the grading rubric provided by the course leaders to Ednius. Course leaders/professor will at all times make the final determination of feedback and grades assigned. The information provided may be disclosed to other third party AI systems, namely:

- the GPT-4 family;
- Llama 3;
- and Phi 3.

If you have any questions about the collection and use of this information, please contact the Associate Director, Graduate Programs, busarcrd@sfu.ca, 778-782-5718.

Advisory notice to be posted for Educator's attention:

In using the Ednius Copilot for Educators Pilot Program, you agree not to upload, submit, or provide access to documents or information that contains or includes personal (non-business contact information) or confidential information to this AI companion, for example:

Personal Information: may include student names, private non-business addresses, non-work related phone numbers, non-work related email addresses, social security numbers, employment or education history, etc. For a more expansive list of personal information data elements please see: https://www.sfu.ca/content/dam/sfu/policies/files/information_policies/I10-11/I10.11 Schedule 1 - May 29 2021.pdf

Confidential or Sensitive Content: Including regulated data, proprietary business information, financial details, legal documents, or any other information that is confidential in nature regarding the university.

Please avoid relying on any responses from this AI companion to make decisions concerning individuals unless you have verified the accuracy of the information provided to, and statements provided by, this AI companion.

Please ensure you provide the correct answers for each quiz so that Ednuis can accurately evaluate students' responses. You will need to provide your intended grading criteria for Ednius to be more refined in the proposed feedback and grading.

Should you have any inquiries or concerns regarding the appropriate use of this platform, please contact the Associate Director, Graduate Programs, busarcrd@sfu.ca, 778-782-5718.

We would like to caution users about the responsible use of Artificial Intelligence (AI). While AI enhances productivity capabilities, and user experience, it is essential to be mindful of its potential consequences. Please consider the following when providing prompts to the AI :

1. Ensure that no personal information is entered into the prompts given to the AI. If any personal information is entered, please ensure that it is handled responsibly, in accordance with any Freedom of Information and Protection of Privacy Act (RSBC 1996, c.165) and university policy related obligations you may have.
2. As AI can inadvertently amplify misinformation. Users should critically evaluate information and cross-reference information generated with reliable sources to verify the accuracy of the provided results.
3. AI algorithms may unintentionally reflect biases present in the training data. Be aware that provided results can carry inherent biases, and it's crucial to critically evaluate information generated by AI.

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.

Consent Notice for Students

Consent Notice for Use of Personal Information

Thank you for participating in our Ednius Copilot for Educators Pilot Program. To enhance your learning experience and ensure the best possible outcomes, we require your consent to use your personal information in Ednius Copilot for Educators Program. Please carefully read the following consent notice before agreeing.

1. Purpose of Information Collection We collect and use your personal information to provide, enhance, and personalize your educational experience. This includes, but is not limited to:

- Providing tailored feedback on assignments and exams

2. Information Collected The types of personal information we may collect include:

- Your name, student ID, and contact details
- Course enrollment and participation data
- Assignment submissions, quizzes, and exam results
- Interaction data within the learning management system (LMS)

3. Products and Tools Using Your Information Your personal information may be utilized in the following educational products and tools:

- **Learning Management Systems (LMS):** For course delivery, assignment submission, and communication.
- **AI-Powered Grading Tools:** To provide personalized grading and feedback based on predefined rubrics.
- **Adaptive Learning Systems:** To offer personalized learning paths and resources based on your performance.

4. Third-Party Disclosure Your information may be shared with third-party service providers who assist in delivering these educational services. These third parties are required to maintain the confidentiality and security of your information and are only authorized to use your data for the specific purposes outlined above.

5. Your Rights You have the right to:

- Withdraw your consent at any time, though this may affect your ability to participate in certain educational activities.
- Access or request correction of your personal information.
- Inquire about the specific third parties with whom your information may be shared.

6. Consent By agreeing to this consent notice, you authorize us to collect, use, and disclose your personal information as described above.

[ ] **I agree** to the collection, use, and disclosure of my personal information as outlined in this notice.

[ ] **I do not agree** and understand that this may limit my ability to participate in certain educational activities.

Section 3: STORING PERSONAL INFORMATION

6. Is any personal information stored outside of Canada?

No, Ednius Copilot for Educators currently offer customers two choices of location for data storage - Canada or the US.

Ednius uses Microsoft Azure's cloud services for AI technologies such as GPT, Llama, and Phi (and not ChatGPT), which support regional data handling by allowing us to select servers located in either Canada or the United States based on the educational partners' preferences.

This ensures that all data remains within the specified legal jurisdictions. Data sent to these services is strictly for grading, feedback, and filtering abusive material, and is not stored by Microsoft Azure or any sub-processors post-processing, nor used to train AI models. Additionally, all data is encrypted during transit and while being processed to prevent unauthorized access, upholding the highest standards of data privacy and security.

- *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.

The information will be sourced from the Ednius Copilot for Educators-Canvas integration, including data based on the level of access authorized by the course leader (Faculty).

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?

If any personal information needs to be updated, users should contact the Associate Director, Graduate Programs, busarcrd@sfu.ca, 778-782-5718, or the faculty in charge of the course.

The Associate Director, Graduate Programs, busarcrd@sfu.ca, 778-782-5718 Staff or the Faculty in charge of the course will need to connect to the Vendor at support@ednius.com from their registered email address and request the correction as specified by the student.

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, The Associate Director, Graduate Programs, busarcrd@sfu.ca, 778-782-5718 Staff or the Faculty in charge of the course will keep a record on the correction as specified by the student in case the personal information cannot be corrected.

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, Personal Opinions

- 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.

The record retention schedule will follow Ednius Copilot for Educators and Canvas policies as they are attached to the information related to the course to be provided with the individualized proposed grade and feedback.

- Student grades are to be kept for 1 year as per RRSDA 1995-018 (1y)
- Additionally, the vendor has agreed to store the history of grades and feedback generated by the AI (both original and final). The vendor will also introduce a process to capture interim grades.

- *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, as per the vendor's agreement to adhere to SFU's Privacy Protection Schedule (PPS)

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
[redacted]			

[redacted]

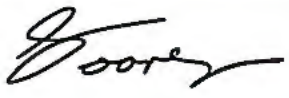
Examples of (non-security) privacy risks	Examples of risk responses / strategies
Vendor is subject to laws that may compel them to disclose the public body's personal information to another entity without notifying the public body (e.g. The USA's *Patriot Act*). In this case, the public body may not 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

Examples of (non-security) privacy risks	Examples of risk responses / strategies
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)
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)	Ernest Soares		November 19, 2024

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.

[Answer]

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: PHYISCAL 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.

[Answer]

- *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?

[Answer]

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
We only allow employees in certain roles access to information	[Y/N]

Strategy	Yes/No
Employees that need standing or recurring access to personal information must be approved by executive lead	[Y/N]
We use audit logs to see who accesses a file and when	[Y/N]
Describe any additional controls:	[Answer]

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
Risk 1: [Answer]	[Answer]
Risk 2:	
Risk 3:	
Risk 4:	

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 / No]

6. Comments / Recommendations:

-

Role	Name & title	Signature	Date signed
Information Security representative	Steve MacGregor, CIPT, PCI ISA Information Compliance Architect		2024-11-21

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.

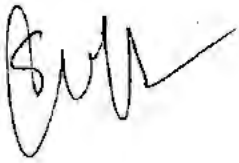
Under SFU's Protection of Privacy Policy I 10.11, administrators are responsible for:

- *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	Maria Szymczak, Director, Graduate Business Programs		November 14th 2024
Role designated accountable for the initiative	Sudheer Gupta, Associate Dean Graduate Business Programs		November 19, 2024

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