

Privacy Impact Assessment Form

PIA # and Name-**assigned by Privacy Office**

1 Key concepts

Contents

1	Key concepts	1
2	General Information	3
3	Collection, Use, and Disclosure	6
3.1	Collection Notice	8
3.2	Use	9
3.3	Disclosure	9
4	Storage and Location of the Personal Information	12
5	Data Linking	16
6	Privacy and Security Safeguards	17
6.1	Security Safeguards	17
7	Privacy Risk Identification and Mitigation	19
8	Accuracy, Correction, and Retention	26
9	Personal Information Banks	29
9.1	Description of personal information bank.	29
9.2	Method of De-identification/Anonymization/Aggregation for Personal Information	31
9.3	Audits	31
10	Conclusions and Approvals	34
11	APPENDIX A: DEFINITIONS	37

Privacy Impact Assessment Form

12 APPENDIX B CSA MODEL CODES 43

13 APPENDIX C SAMPLE PRIVACY AND CONSENT NOTICE 44

“**personal information**” means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except where they relate to another individual,
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- (g) the views or opinions of another individual about the individual, and
- (h) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

2 General Information

1. Name of Department, Branch and Program Area

Finance and Administrative Services

2. Name of Program or Service Representative

Christie Ray

3. When will the initiative take place? 1/30/23

4. Is this a one-time event?

Yes

No

5. Do you have an end date planned?

Yes

No

6. Describe the New Program or Service or the Change

Building upon the strength of the UNBC community, dedication, commitment, and resilience of its faculty and staff; and grounded in the collective acknowledgment for a desired transformative change, UNBC is embarking upon an exercise to develop a road map for the proposed transformation journey for UNBC Finance and Administrative Services. This exercise will be informed and driven by ideas, innovations, suggestions, and a persistent message for a desired transformative change that has been conveyed on an ongoing basis by the UNBC community over the past several years.

Privacy Impact Assessment Form

7. Describe the Purposes, Goals and Objectives

Why are you doing the initiative? What need does the initiative meet?

Assess the current state organizational structure of UNBC Finance and Administrative Services identifying gaps and misalignment(s);

Recommend a “desired-state” transformative organization structure and People plan that is aligned with service expectations with a view to value addition; and

Propose an implementation approach and a road map to support the future state and achieve the desired transformation.

8. Describe the Governance Model

Accountability – who is ultimately accountable for the program or system

Christie Ray will be coordinating engagement activity and communication
MNP consultants will be facilitating meetings and assembling recommendations / report
Rahim Somani will be receiving the report

Privacy Impact Assessment Form

9. List of All Stakeholders Impacted / Involved

Stakeholder	Role
Christie Ray	Coordinating
Rahim Somani	Report Recipient
MNP	Consultants

10. Please add any additional comments below.

NA

11. Describe any Relevant Existing Policies

NA

Privacy Impact Assessment Form

12. Describe any Related PIAs

NA

13. Describe any Relevant contracts

contract with MNP signed prior to PIA

14. Research / Health System Use

Do you anticipate that data collected by this program / system will be used for research or health system use?

Yes

No

15. If so, please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

3 Collection, Use, and Disclosure

16. 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. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix

Privacy Impact Assessment Form

FIPPA Section	Authority to Collect Personal Information
26(a)	The collection of the information is expressly authorized under an Act
26(b)	The information is collected for the purposes of law enforcement
26(c)	The information relates directly to and is necessary for a program or activity of UBC
26(e)	The information is necessary for the purposes of planning or evaluating a program or activity of UBC
26(f)	The information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur
26(g)	The information is collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appears, and that is open to the public

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure	FIPPA Section
Individual's name	identifies person to collect info from	Indirect (org chart)	26(e)
Position title	identifies role / duties within organization	Indirect (org chart)	26(e)
Work email and phone	for scheduling	Indirect (from UNBC)	26(e)
Tenure in role	assess history / duration of current state descriptions and understand organizational cultural factors	Direct	26(e)
Employment history summary	to understand experience of individual sharing opinions	Direct	26(e)
Duties / accountabilities and associated roles (direct or indirect)	to assess current assignment of work	Direct	26(e)
Opinions about how well accountabilities are acted upon	to assess current state of organizational design	Direct	26(e)
Opinions for opportunities for change or improvement for work delegation	to assess current state of organizational design	Direct	26(e)

Privacy Impact Assessment Form

Opinions on where work accountabilities would be most appropriately assigned	to assess current state of organizational design	Direct	26(e)
Opinion on beneficial and potentially harmful changes	to assess current state of organizational design	Direct	26(e)
Examples of things that work well / don't work well (may include names / position titles of others)	to assess current state of organizational design	Direct	26(e)
Reporting relationships and Performance tracking / measurement (individual / team / unit)	to assess current state of organizational design	Direct	26(e)

3.1 Collection Notice

Personal Information is being collected under the authority of the University Act and Section 26 of BC's Freedom of Information and Protection of Privacy Act. personal information may be collected only if such collection is authorized by or under legislation, essential for operating programs or activities, or collected for law enforcement purposes.

If you are collecting personal information directly from the individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

17. Describe how personal information is to be collected

<ul style="list-style-type: none"> • At the beginning of each interview and meeting, participants will be asked to provide consent to the participation. • The information being shared by participants will be summarized in a manner that maintains anonymity (identifying information will not be reported). • The results of the interviews and meetings will only be included in a report that provides generalized findings and is shared with UNBC. <p>Surveys (if employed):</p> <p>Privacy Notification / Informed Consent – Responses will be aggregated into a summary document for use in the Finance & Administrative Review process. It will be valuable to understand perspectives on accountabilities, opportunities and potential changes, as well as differences in perception that may exist between units. There is no intent to identify any individual based on survey question responses. But due to small sizes of some units it may technically be possible to do so in some cases. Participation in this review is voluntary. Choosing not to participate will not affect the employment of the individual or how they are treated.</p> <p>Please click Agree if you are willing to contribute your valued responses to this effort, while recognizing the potential ability to be identified by such. If you do not agree you will not be able to participate. Rest assured that the participants will not have any negative implications irrespective of their decision to participate or otherwise. However, your valuable input will provide critical contribution to our transformational journey.</p> <p>Please direct any questions about the purpose or intent of this survey and associated data collected, to Christie.ray@unbc.ca.</p>
--

18. Review the sample collection notice and attach the notice as an appendix.

(See Appendix C for an example)

Privacy Impact Assessment Form

3.2 Use

19. Please list all users of PI including third parties

Rahim Somani, VP of the Finance & Administration portfolio
MNP

20. Describe how personal information is to be used

All info held in confidence by MNP, who will anonymize and aggregate collected data and provide recommendation and rationale for new organizational structure, and plan to achieve such. This will be delivered to the project sponsor (Rahim Somani, VP of the Finance & Administration portfolio).

Personal contact detail (email addresses, phone numbers) will only be used for outreach on scheduling of interviews and meetings and kept confidential by MNP in accordance with the firm's privacy policy and provincial legislation (regulation). The MNP Privacy Policy can be viewed at www.mnp.ca/en/privacy-policy.

The information being shared by participants will be summarized in a manner that maintains anonymity (identifying information will not be reported).

The results of the interviews and meetings will only be included in a report that provides generalized findings and is shared with UNBC.

3.3 Disclosure

Section 26 states that A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3. A public body may

Privacy Impact Assessment Form

disclose personal information referred to in section 33 inside or outside Canada as follows:

in accordance with Part 2;

if the information or disclosure is of a type described in section 22 (4) (e), (f), (h), (i) or (j);

if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable.

21. To whom will you be disclosing personal information?

Provide details on the disclosure, including where and how personal information will be stored.

We use an enterprise contract with Microsoft Canada for the provision of cloud-based storage of files and information using the productivity suite of Microsoft Office and related applications such as Sharepoint, OneDrive and MS Teams. All information collected in documents will be stored on these sites.

Privacy Impact Assessment Form

22. Will it be disclosed to anyone outside of Canada?

Provide details on the disclosure, including where and how personal information will be stored.

N/A

23. Will it be disclosed as part of Health System Use?

Provide details on the disclosure, including where and how personal information will be stored.

N/A

24. Will it be disclosed as part of Research / Open Data?

Provide details on the disclosure, including where and how personal information will be stored.

N/A

4 Storage and Location of the Personal Information

25. Is any personal information stored outside of Canada?

Yes

No

26. Describe how PI information will be stored

If you are using a cloud solution, there may be multiple cloud service providers involved in your initiative. Cloud solutions are typically considered to be made up of a 'stack' of infrastructure (IaaS), platform (PaaS) and/or software (SaaS) that might be operated by the same or different cloud service providers.

For example, Software as a Service (SaaS) providers often offer services built on infrastructure (IaaS or Infrastructure as a Service) offered by a different cloud service provider.

We use an enterprise contract with Microsoft Canada for the provision of cloud-based storage of files and information using the productivity suite of Microsoft Office and related applications such as Sharepoint, OneDrive and MS Teams. All information collected in documents will be stored on these sites.

Privacy Impact Assessment Form

27. Describe the contractual terms in place.

Here you will describe what type of contract you rely on for your initiative (if applicable). For example, you might be contracting a cloud-based service specifically for your initiative, or you might be using an enterprise offering.

Contract with MNP signed before PIA was completed

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

Access to our documents stored in these applications is strictly controlled to use by those within MNP specified with access to the designated MS Teams Channel, OneDrive or Sharepoint Directory. Links to documents can be shared only with specified employees of MNP and/or UNBC.

29. Please provide details on how you will track access to personal information.

MS Teams, Sharepoint and OneDrive provides ways to track and audit accessing of files stored there, if required. We will primarily be using MS Teams. Documents stored here have a tracker for last accessed and saved, as well as past version and access.

Privacy Impact Assessment Form

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

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

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

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

Privacy Impact Assessment Form

ACTIVELY INITIATIVE

5 Data Linking

In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

31. Does this initiative involve a program or activity that provides a service (or services) through a public body and at least one other public body or agency working collaboratively to provide that service?

Yes No

32. Does this initiative involve a program or activity that provides a service (or services) through a public body that is working on behalf of one or more other public bodies or agencies?

Yes No

33. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the Regulations? (Privacy Officer will answer).

Yes No

6 Privacy and Security Safeguards

People, organizations and 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 your personal information is safely secured in both physical and technical environments.

34. Does your initiative involve digital tools, databases information systems?

Yes

No

If yes, please discuss with ITS whether you also require a security and threat risk assessment

A digital tool, database or information system may leave personal information exposed or otherwise vulnerable to security threats. Security assessments are used on information systems and other digital tools to assess and document security risks, risk ratings and planned risk responses.

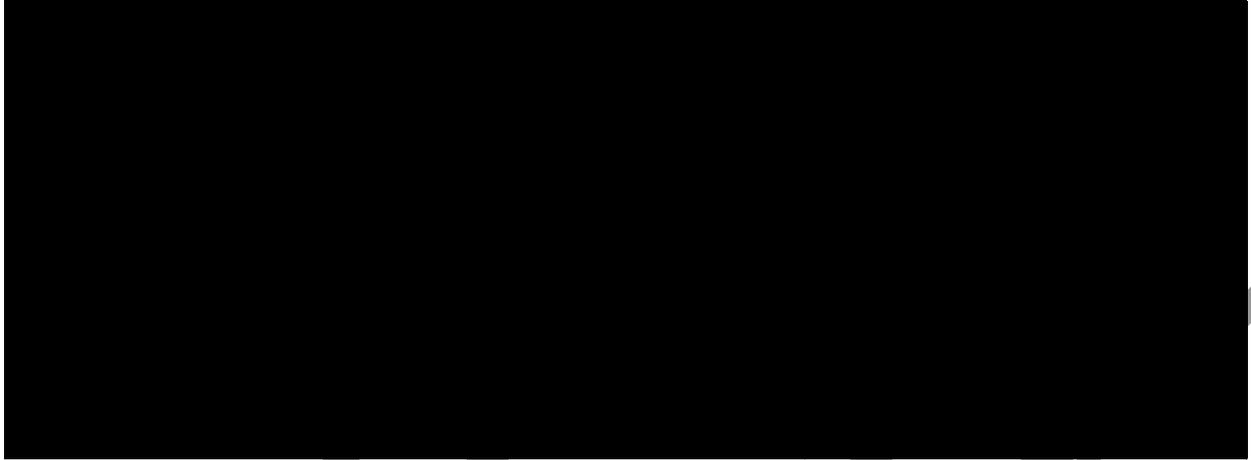
6.1 Security Safeguards

There are three broad types of security measures:

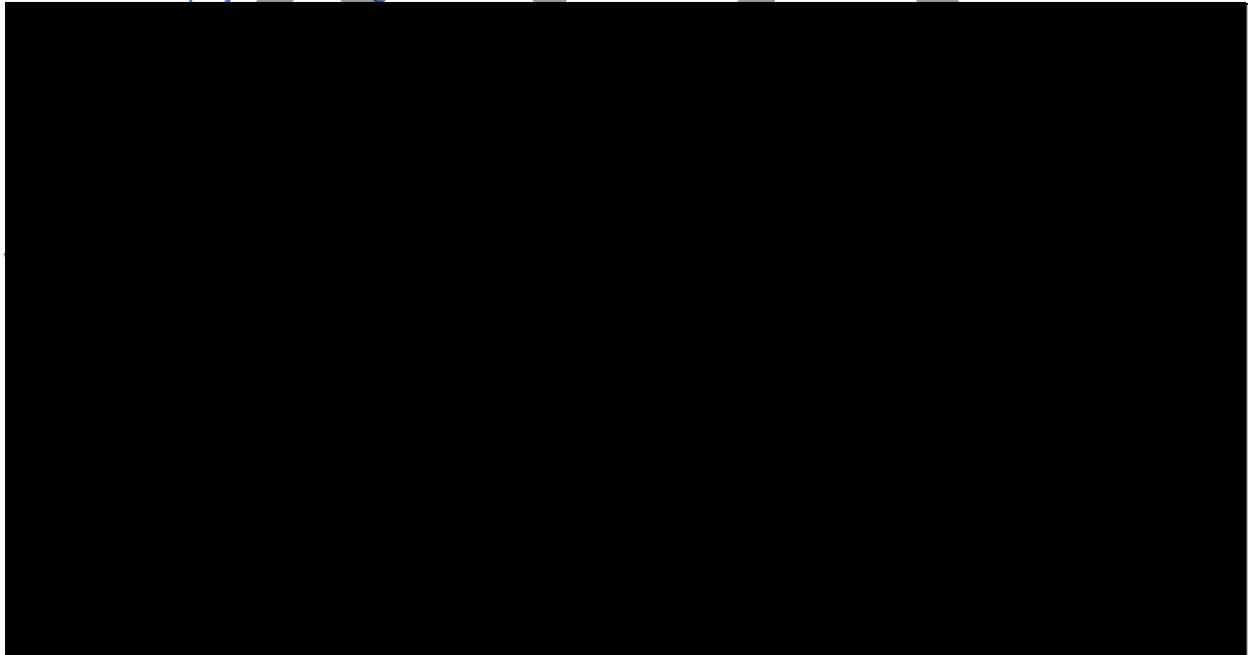
PHYSICAL	These security measures relate to the physical environment that the information is stored in; for example, whether your organization limits access to the filing cabinet or file room through select staff having a key.
TECHNICAL	Technical measures relate to your organization's hardware and software; for example, firewalls, encryption, and intrusion prevention systems.
ADMINISTRATIVE	Administrative controls are rules and processes for your employees or third parties that prevent them from inappropriately accessing, using, or disclosing your client's personal information; for example, role-based access controls, annual privacy training, employee codes of conduct, and privacy-related clauses in contracts.

Privacy Impact Assessment Form

35. Describe administrative safeguards



36. Describe physical safeguards



Privacy Impact Assessment Form

37. Please reach out to our CISO Office and ITS for the vendor assessments and technical requirements for IT/security threat risk assessment to fill out these sections or attach that assessment to this PIA.

Any online meetings will be scheduled use a UNBC zoom enterprise accounts or Microsoft Teams account.

7 Privacy Risk Identification and Mitigation

PRELIMINARY RISK ASSESSMENT

PROGRAM/ACTIVITY

LOWER RISK **HIGHER RISK**

Your program's risk level is based on the total of all risk factors. Each risk factor either increases or decreases the overall program risk.

Involves limited personal information	Involves large amount of personal information
Does not involve sensitive personal information	Involves sensitive personal information such as financial or medical information, SIN, children's information
Context is not sensitive	Context is sensitive
Involves the personal information of a few individuals	Involves the personal information of many individuals
Does not involve personal information of vulnerable populations	Involves personal information of one or more vulnerable populations
Has a minimal impact on individuals (e.g. lower stakes)	Has a major impact on individuals (e.g. high stakes)
Is one-time or short term	Is long-term
Does not involve the additional risk factors (see additional risk factors above)	Involves one or more of the additional risk factors (see additional risk factors above)

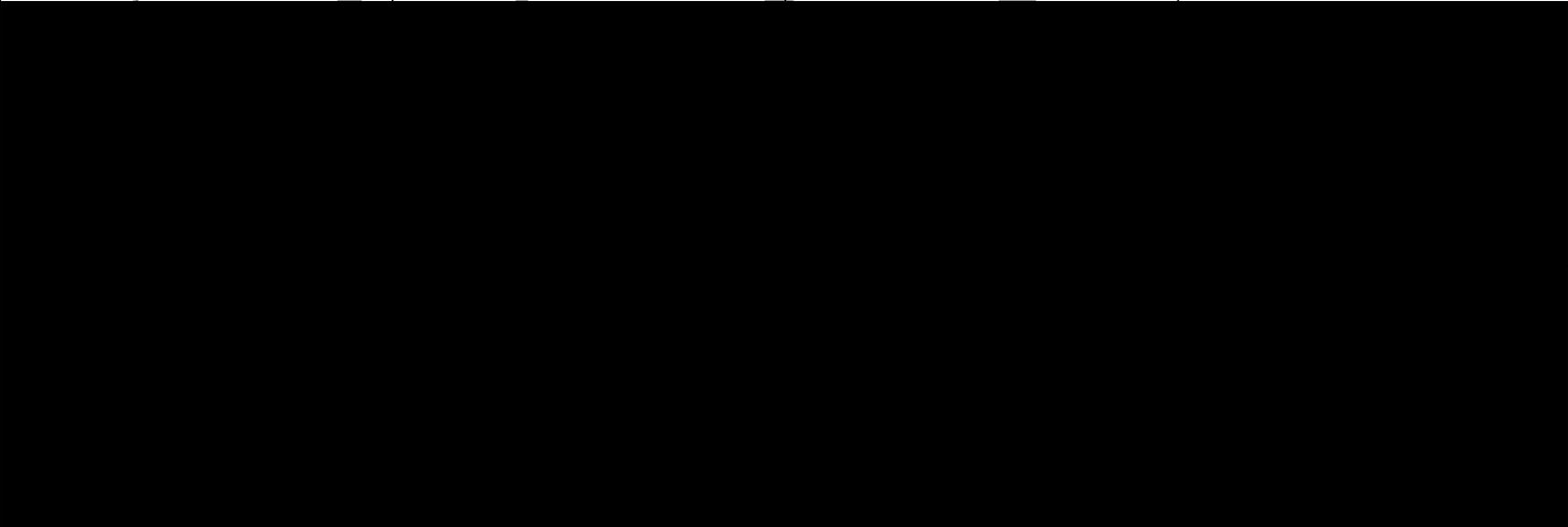
Privacy Impact Assessment Form

38. Identify any privacy risks, even very unlikely ones, associated with the initiative and the mitigation strategies that will be implemented.

Please provide details of all such strategies. The Privacy Officer will help identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

*Risk Levels	Likelihood	Harm
Low	Little possibility that the risk will occur due to mitigating factors	Compromise would likely not result in any significant harm to the privacy, safety, or economic standing of individuals or the corporation.
Moderate	A possibility that the risk will occur if no additional measures are taken.	Compromise would likely cause some harm to the privacy, safety, or economic standing of individuals or the corporation.
High	Near certainty that the risk will occur in the future if no corrective measures are taken.	Compromise would likely cause significant and immediate harm to the privacy, safety, or economic standing of individuals or the corporation.

Privacy Impact Assessment Form

RISK	MITIGATION STRATEGY	LIKELIHOOD	IMPACT
<p>EXAMPLES</p> <p>Data that is no longer needed is at risk of being breached because it is being retained in the platform longer than is necessary</p>	<p>Implement a process on the IT platform to automatically delete data once is it no longer needed</p>	<p>Moderate</p>	<p>High</p>
			

Privacy Impact Assessment Form

Privacy Impact Assessment Form

ACTIVELY INITIATIVE

Privacy Impact Assessment Form

ACTIVELY INITIATIVE

Privacy Impact Assessment Form

--	--	--	--

If this PIA addresses a common or integrated program, UNBC must submit this PIA to the Office of the Information and Privacy Commissioner and be subject to their examination, advice, and timelines.

8 Accuracy, Correction, and Retention

39. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Empty response box for question 39.

40. Do you have a process in place to correct personal information?

Yes No

41. If yes, please describe your process below?

Empty response box for question 41.

Privacy Impact Assessment Form

42. Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Describe the process of how you will make a note on the record.

Direct and specific interview and meeting notes generated by MNP will be marked confidential and draft and not allowed access to UNBC team members. Documents will be stored on an MS Teams Channel with access only for MNP project team members. If a request for interview notes is required, UNBC will be consulted on what specific personal information can be shared within the definition of personal information and limits of privacy, confidentiality, and work product to develop a project deliverable.

43. If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third-party recipient of the request for correction. How will you ensure that you conduct these notifications when necessary?

44. Do you use personal information in your initiative to make a decision about an individual?

Examples of using personal information to make decisions include but are not limited to:

- Using a person's date of birth or income to decide whether a person qualifies for a benefit
- Using a person's employment history to decide whether they can move forward in a job competition

Privacy Impact Assessment Form

- Using a person's health information to decide the level and type of care they receive

Yes No

45. If yes, do you have an approved information schedule in place related to personal information used to make decisions?

Yes No

46. If yes, please include your approved information schedule here.

47. If you answered 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.

Personal information is not intended to be used within the scope of this project to determine a better fit of an individual within the F&A Organizational Structure. The project will not be making recommendations of individual fit for recommended positions based on any and personal information.

9 Personal Information Banks

A personal information bank is a collection of personal information that is organized or searchable by the name of the individual or an identifying number, symbol or other identifier. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- Linked to an identifiable individual
- Organized and capable of being retrieved by a personal identifier
- Normally compiled for a single purpose

48. Will your initiative result in a personal information bank?

Yes

No

If yes, answer the following questions, if "No" please proceed to the next section?

9.1 Description of personal information bank.

49. Name:

50. Location:

Privacy Impact Assessment Form

51. Description:

[Empty text box for description]

52. Authority:

This personal information is begin collected under the authority of the University Act and section 26 (a), (c), and (e) of the Freedom of Information and Protection of Privacy Act (FOIPPA).

[Empty text box for authority]

53. Purpose:

[Empty text box for purpose]

54. Category of Users:

[Empty text box for category of users]

Privacy Impact Assessment Form

9.2 Method of De-identification/Anonymization/Aggregation for Personal Information

55. Please explain how Personal Information will be de-identified or anonymized and by whom?

[Empty response box for question 55]

9.3 Audits

56. What does the audit log track? How detailed is the data (e.g., date stamps, time stamps, access control number, IP address, etc.)? Does the audit log include the purpose of an access?

[Empty response box for question 56]

Privacy Impact Assessment Form

57. Are the audit logs immutable?

[Empty response box for question 57]

58. Who reads the audit logs, and how long are they kept?

[Empty response box for question 58]

59. Who is responsible for oversight of user access?

[Empty response box for question 59]

60. Is there a separation of responsibility between those who supervise administration of the system, or security of the system, and those who verify the audit logs (e.g., does the auditor in the organization have a role, or is it the security department?)

[Empty response box for question 60]

Privacy Impact Assessment Form

61. Is the system responsive or passive? For instance, is it possible to put a monitor on particular individuals (e.g., in a hospital setting, if a celebrity is admitted as a patient, etc.)? Will access produce an immediate response and not just a log entry for review months later?

Empty response box for question 61.

62. Will those found to abuse access privileges be sanctioned in a meaningful (and visible) way?

Empty response box for question 62.

10 Conclusions and Approvals

Once the PIA has been approved with or without conditions, the Privacy Officer will collect signatures from the individuals provided below. A copy of the PIA will be distributed to all signatories for convenience or to attach to a requisition or file with a contract.

Name of Individual leading the Program/Project: Christie Ray

Position:
Senior Advisor Business Development, Business Services

I confirm the information management practices in this initiative have been documented as accurately as I am aware and I commit to communicating appropriate information management practices to all individuals participating in this initiative as appropriate. I commit to following the documented practices on this PIA, or arranging a PIA amendment if I am aware information management practices in this initiative change.

Signature:  Date: 02 February 2023

Privacy Impact Assessment Form

Name of Director or Dean Overseeing the Program/Project:

I am accountable for overseeing my staff involved in this initiative to ensure they adhere to information management practices presented in this PIA. I will arrange for the project lead named above to contact the Privacy Officer to arrange a PIA amendment if required.

Signature: _____ Date: _____

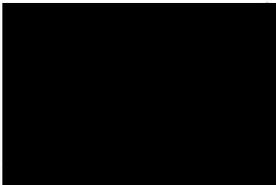
Name of Chief Information Security Officer

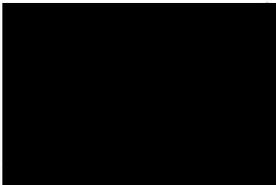
I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that satisfactorily comply with the information security standards of the University of Northern British Columbia.

Signature: _____ Date: _____

Name of Privacy Officer: Rahim Somani

Position: VP Finance & Administration

I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that comply with British Columbia's Freedom of Information  Privacy Act.

Signature:  _____ Date: February 6, 2023

ACTIVE
INITIATIVE

11 APPENDIX A: DEFINITIONS

Confidentiality	The assurance that information about identifiable persons, the release of which would constitute a privacy breach, will not be disclosed without consent, except as allowed by law.
Consent	Consent, in the context of personal information, means the agreement of someone to provide their personal information for the purposes identified to them. In some cases, consent may not be possible (e.g., medical emergency) or may not be required (e.g., collection by police of information relating to a suspect where the collection is not a search or seizure). Consent is generally given by a specific act of the individual, but sometimes it can be implied. In the public sector, consent is not always a requirement for the collection of personal information – having the legal authority to collect personal information is.
Core privacy principles	<p>In March 1996, the Canadian Standards Association (CSA) developed a national, voluntary code that sets basic principles for safeguarding personal data. The Code establishes 10 basic principles for all organizations that collect or use personal information. In some cases, certain principles may not apply to public sector regimes. For example, in the public sector, the “consent” principle listed as number three below is often substituted for “legal authority”.</p> <ol style="list-style-type: none"> 1. <i>Accountability</i> - An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. 2. <i>Identifying Purposes</i> - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. 3. <i>Consent</i> - The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Privacy Impact Assessment Form

4. *Limiting Collection* - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. *Limiting Use, Disclosure and Retention* - Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.
6. *Accuracy* - Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.
7. *Safeguards* - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. *Openness* - An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.
9. *Individual Access* - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. *Challenging Compliance* - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Data (information) flows	Mapping the flow and manipulation of information within and across systems or business processes.
<hr/>	
Data matching	An activity that involves comparing personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the
<hr/>	

Privacy Impact Assessment Form

data pertains. Included in this definition of data-matching is data linkage, also known as data profiling.

Personal information For data to be categorized as *personal* information (rather than just information, in general), it must have details sufficient to identify an individual. Individual identification is thus the threshold for transforming general information into personal information and where rights, protections, and requirements associated with the proper handling of personal information are triggered.

Without restricting the generality of the foregoing, personal information may include, for example:

information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

any identifying number, symbol or other particular assigned to the individual,

the address, fingerprints or blood type of the individual.

the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations.

correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence.

the views or opinions of another individual about the individual.

the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e),

Privacy Impact Assessment Form

but excluding the name of the other individual where it appears with the views or opinions of the other individual, and,

the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

In some jurisdictions, personal information **may not include** information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

- the fact that the individual is or was an officer or employee of the government institution,
 - the title, business address and telephone number of the individual,
 - the classification, salary range and responsibilities of the position held by the individual
 - the name of the individual on a document prepared by the individual in the course of employment, and,
 - the personal opinions or views of the individual given in the course of employment.
 - information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,
 - information relating to any discretionary benefit of a financial nature, including the granting of a license or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and
 - information about an individual deceased for more than twenty years.
-

Privacy Impact Assessment Form

Privacy Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

Privacy officer A privacy officer is a person within an organization whose job it is to:

- encourage compliance with sound privacy principles, prevailing privacy policies and privacy laws;
- respond to requests for access to and correction of personal information and general issues within a public body concerning personal information; and
- work with information and privacy commissioners during the investigation of a privacy complaint against an organization.

Privacy officers may also be responsible for managing changes to an organization's:

- information management practices, policies and procedures;
 - staff training, vis-a-vis privacy and information handling;
 - privacy policies and procedures; and
 - inquiry and complaint processes.
-

Privacy protection Preventing unauthorized collection, use and disclosure of an individual's personal information.

Program manager The person responsible for managing and directing the projects of a public body, with emphasis on coordinating and prioritizing resources, and managing the risks which emanate from projects in development or underway. Program managers are responsible for ensuring that the projects they lead or direct are compliant with government policies and the law.

Privacy Impact Assessment Form

Risk assessment The process of quantifying the impact of implementing a particular idea, process, system or strategy.

Threat and Risk Assessment (TRA) A risk management process used to evaluate the security threats associated with information technology projects, including potential system vulnerabilities and impacts on data integrity and confidentiality. TRAs, when completed in conjunction with a PIA, can help provide recommendations to lower information and privacy risks to acceptable levels.

ACTIVELY
INITIATIVE

12 APPENDIX B CSA MODEL CODES

The 10 Privacy Principles

- 10. **Provide Recourse.** If you receive a complaint about how an individual's personal information has been handled, direct it to the Privacy, Compliance and Training Branch immediately, via the breach reporting line: 7-7000, option 3. Learn more from link provided below.
- 9. **Right of Access and Correction.** Individuals have a right to access their own personal information, or have that information corrected. Be aware of the FOI process, and direct any requests to Information Access Operations immediately. More information provided at link below.
- 8. **Ensure Accuracy.** You must make a reasonable effort to ensure personal information collected is accurate and complete if it will be used to make a decision affecting the individual it is about. Find out more about this requirement at the link below.
- 7. **Be Open and Transparent.** Routinely release any records that can be regularly provided to the public. Proactively disclose any records that will be of interest to the public. Consult with Information Access Operations on these processes. Find the Open Information Open Data Policy provided at the link below.
- 6. **Be Accountable.** Be responsible for all personal information under your control, including contractors' records. Be aware of who your Ministry Privacy Officer is. Find your MPO at the link below.



- 1. **Identify Purpose.** Must identify in writing: the purpose for which you are collecting personal information, the legal authority and contact information of someone who can answer questions about the collection, unless an exception applies. See link below for more.
- 2. **Limit Collection.** Do not collect personal information indiscriminately or without a legal authority. Information must be necessary to fulfill identified purposes, and be reasonable and appropriate. Find more information at the link below.
- 3. **Get Consent.** Secure consent as a means to use or disclose personal information for secondary purposes. Consent must be written and explicit. There are some specific circumstances where consent is not required. See the link below.
- 4. **Limit Use, Disclosure.** You may use or disclose personal information for the purposes identified when it was collected, or another reason authorized by FOIPPA. For new uses, get consent. More information provide at the link below.
Limit Retention. Personal information used to make a decision about an individual must be retained for at least one year. Information must be destroyed in accordance with any applicable records retention schedules. Find your Records Officer at the link below.
- 5. **Reasonable Security.** Must make reasonable security arrangements to protect personal information. Measures should be appropriate and proportional to the sensitivity of the information. Consideration should be given to physical, technical and procedural measures. Find your MISO at the link below.

For more information on the privacy principles and resources, visit: www.gov.bc.ca/privacyprinciples

13 APPENDIX C SAMPLE PRIVACY AND CONSENT NOTICE

WE NEED TO COLLECT INFORMATION FROM YOU

UNBC Continuing Studies needs to collect information from you to:

1. Enroll you
2. Confirm sponsorship arrangements
3. Process your payment
4. Generate a class list for instructors
5. Ensure that grades and certificates are assigned to the correct student
6. Assist our partners in verifying certificate validity

WE HAVE PERMISSION TO DO THIS

The University of Northern British Columbia collects, uses, shares, discloses, maintains and when applicable deletes and destroys Personal Information provided on this form according to the *Freedom of Information and Protection of Privacy Act* [RSBC 1996 c. 165].

HOW WE WILL USE AND SHARE YOUR INFORMATION

Continuing Studies must directly disclose some information on this form and your course completion status to your sponsor, including your employer if you are sponsored through your job. Continuing Studies may need to share the information on this form with anyone repairing or maintaining electronic systems involved in this Continuing Studies course.

UNBC Continuing Studies is the training agency chosen to deliver the Wildlife Dangerous Tree Assessor courses on behalf of the Wildlife Dangerous Tree Committee of BC (WDTC). Under the terms of our agreement with the WDTC, Continuing Studies

Privacy Impact Assessment Form

provides a list of current assessors upon request. Under the terms of this agreement UNBC also provides a list of current Fire assessors to BC Wildfire Services (BCWS), twice a year to support certificate verification. Personal information on this form will be shared confidentially with members of the WDTC. Certificate status, certificate number and copies of certificates may be shared upon request by contractors and employers for the purpose of confirming qualifications.

You have the right to revoke consent to the collection, use, retention, and disclosure of personal information at any time, but doing so will result in consequences including, but not limited to, forfeiting registration in the course.

HOW WE WILL PROTECT YOUR INFORMATION

UNBC is obligated to protect your personal information and has various processes in place to ensure it is secure.

HOW LONG WE WILL KEEP YOUR INFORMATION

The *Freedom of Information and Protection of Privacy Act* allows us to keep your Personal Information for at least one year after collection and when its period of usefulness is over we will securely delete or destroy it. In the case of the Wildlife Dangerous Tree Assessor Certificate Program, hardcopy materials are kept for the life of the Certificate, which is four years, before being destroyed.

WHAT TO DO IF THE INFORMATION WE HAVE COLLECTED FROM YOU IS INCORRECT, OR YOU HAVE QUESTIONS?

Please contact UNBC Continuing Studies at: 250-960-5980 OR cstudies@unbc.ca

If you still have questions or concerns, please contact: Governance Officer for Access, Privacy and Records Management at privacy@unbc.ca

By registering for this course, you indicate you have read, understand, and agree to the privacy statement. You also understand that you have the option to ask questions about any part of this statement before registering.

Privacy Impact Assessment Form

Signature: _____ Date: _____

ACTIVE
INITIATIVE