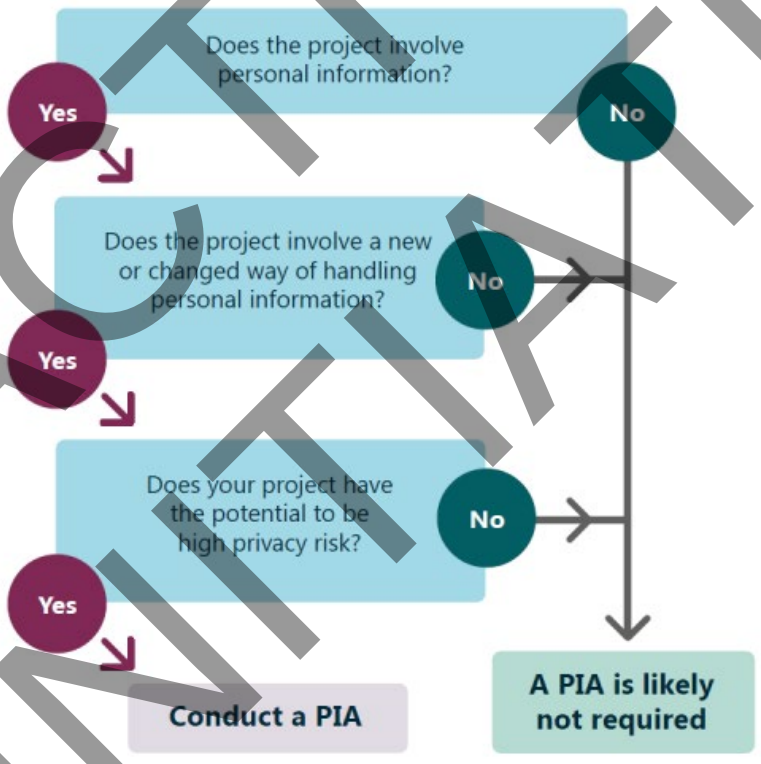
UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Here are a few examples of situations where you should consider a PIA:
•You collect, use or disclose new personal information that you did not collect, use or disclose before.
• You give access to personal information to new parties.
• You implement a new service delivery or management technology that stores, transmits, or retrieves personal information.
You implement a new or different electronic record system, or make changes to an existing one, such as adding portable devices with wireless network connections.
• You enter into an agreement with a new business partner or vendor who will have access to health information in your custody or control.
• You create a new organization that will collect, use or disclose personal information.



Please fill out PART A to determine your need for a full PIA.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PART A

1. Introduction

Answer the who, what, where, when, why and how of your initiative. Describe the initiative in full, including:

General Description

a) Name of Program or Service – Nessus internal vulnerability scanning

Information Security has purchased a Nessus vulnerability scanner.

This scan will run over our internal networks to discover vulnerabilities in our networks and allow us to fix them.

Once the scanner is set up it is a completely automated process

b) Name of Department, Branch and Program Area – Information Security

c) Name of Program or Service Representative – Annette Doyle

d) Key Program or Service Dates

We would like to have this service running by 27 May 2022

This will be a scheduled scan that will run at an interval we have not yet decided on.

This initiative will continue for at least 3 years

There is no end date planned for this initiative at this time.

1. Description

a) Description of the New Program or Service or the Change

i. Purposes, Goals and Objectives – The nessus scanner will give us the necessary insight into our internal networks to detect and remediate vulnerabilities before they can be compromised.

ii. List of All Stakeholders Impacted / Involved

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Stakeholder	Role
Dave Kubert	CISO
Trevor Fuson	CIO
Kevin Schretlen	Infrastructure Manager

iii. The Need

The Nessus scanner is necessary for the discovery of vulnerabilities in our servers, and internal systems.

iv. Governance Model

Dave Kubert will be accountable for this inititative.

v. Relevant Existing Policies

vi. Related PIAs – BCNET Nessus scan

vii. Relevant contracts

viii. Research / Health System Use

No

b) The Intended Scope (Project and PIA)

Describe how much of the initiative you will assess in this PIA.

i. Scope of PIA – I'm not sure if one is needed. The Nessus scan only looks for vulnerabilities in the system, it does not store any data other than enumerate the vulnerabilities it finds.

ii. Out of Scope of PIA

c) Definitions

Add any applicable definitions here:
See Appendix C for examples

Term/Acronym	Definition

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

2. Personal Information Flow Diagram and Explanation

If you are collecting, using, storing, sharing, disclosing or retaining Personal Information you will need to proceed with the **Part B and C** of this document.

If not, please sign and send this determination document to the University Governance Office at privacy@unbc.ca

Think about the information you'll collect, use, store or share as part of your initiative and list it here. A major part of the PIA process is to make sure that you have authority under the *Freedom of Information and Protection of Privacy Act (FOIPPA)* to collect, use, store and disclose each of these pieces of information. Limit your collection of personal information to only what is necessary to complete the initiative.

In the table below, complete the Data Element (personal information usually) rationale and method for collection, use, or disclosure highlighting separately by row each instance that information is collected, used, stored, protected, disclosed and disposed of during this initiative.

Unless not possible, ensure these steps are arranged how they would occur chronologically in order to make a transparent workflow. The Privacy Officer will review your steps and determine which type of information management practice each entry is and ensure that the practice is compliant with sections under the Act.

a) List of Personal health information / personal information / sensitive information to be Collected, Used and/or disclosed and the Rationale for each.

Please identify each source of data that you intend to access and its business owner. Also indicate that you have contacted the owner and received permission to access the data.

EXAMPLE:

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure
Individual's Name	Required to register and correctly identify individual.	Direct
Individual's Phone Number	Required for notifying individual of test result.	Direct

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure

If you do not use personal information in your initiative: how will; you reduce the risk of unintentionally collecting personal information?

For example, if you are collecting opinions as part of a public engagement strategy, participants may offer personal information about themselves or others, even though you've instructed them not to. If you do inadvertently receive or collect personal information, what steps will you take to:

- Destroy it
- Return it
- Transfer it to the correct recipient

FOIPPA section 27.1 describes under what circumstances personal information is considered not collected, despite you having received it. As long as you do nothing with the personal information you receive other than read and delete or return it, or transfer it to the appropriate public body, you have not collected the information according to FOIPPA.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

However, if you take any other action, including storing the information or using it in your own work, under FOIPPA you have collected personal information without authorization and that is considered a privacy breach.

I am not collecting, using, storing, sharing, disclosing, or deleting any personal information for this initiative.

Staff Name_____Annette Doyle_____

Signature___ [redacted]_____

Date_____

PRIVACY OFFICE USE ONLY

This initiative does not require a full PIA document.

Doris Marshall Greenlaw
Governance Officer name

[redacted]
_____
Governance Officer Signature

30 May 2022

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

PART B

3. Collection, Use and Disclosure of Personal Information

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.*

a) Collection

As you work through the description of the information flows, consider whether each element of personal information is necessary for delivering your initiative, or whether you could collect less personal information without risking the success and efficacy of your initiative.

Collect only the information you need for your initiative to work. Collecting more personal information than you need to do your work may lead to a privacy breach.

Section 26 states that 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.

Purpose for which personal information may be collected
26 A public body may collect personal information only if

(a) the collection of the information is expressly authorized under an Act,

(c) the information relates directly to and is necessary for a program or activity of the public body,

(d) with respect to personal information collected for a prescribed purpose,

(i)the individual the information is about has consented in the prescribed manner to that collection, and

(ii)a reasonable person would consider that collection appropriate in the circumstances,

(e)the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

How personal information is to be collected
27 (1)A public body must collect personal information directly from the individual the information is about unless

(a)another method of collection is authorized by

(i)that individual,

(ii)the commissioner under section 42 (1) (i), or

(iii)another enactment,

Collection is only permitted through knowledgeable implied or express consent.

PIA Determination and Template

PIA#: (assigned by Privacy Office)

b) Consent

Whenever possible, position your collection notice so that people read it or hear it before they are asked for their information. For example, you can include a collection notice as part of the preamble to an online form or read it over the phone before you begin asking for information. If it's not possible to put your collection notice at the top, position it where people have the best possible chance of hearing or reading it before giving their information so that they understand how you'll use their information.
When you collect information from people, you must tell them:

- Your purpose for collecting personal information
- Your legal authority under FOIPPA or other legislation for collecting personal information
- Contact information for a person in the public body who can answer questions about why you're collecting personal information, how it's used and how people can update or correct their information

You can edit the following sample collection notice to suit your initiative.
We are collecting your personal information to [purpose]. If you have questions about our collection of your information, please contact us at [contact information].
We are collecting your personal information under section [e.g. 26(c)] of the Freedom of Information and Protection of Privacy Act.

You may not need a collection notice if:

- You collect personal information indirectly, meaning you get the information from another public body and not from the individual who owns the information
- You collect personal information for law enforcement
- You collect information by observing a person at a public event

FOIPPA section 27(3) and (4) tells you more about when you do not need a collection notice. If you determine that you do not need a collection notice, explain why.

Copy/Paste or Fill in your Privacy/Consent Notice here:
(See Appendix C for an example)

c) Use

FOIPPA was amended effective November 26, 2021 and those amendments affect this section.

Who will be using the personal information and for what purpose??
Use of Personal Information
Section 32
A public body may use personal information in its custody or under its control only

(a)for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),

(b)if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

(c)for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

PIA Determination and Template

PIA#: (assigned by Privacy Office)

d) Disclosure

To whom will you be disclosing personal information?

Will it be disclosed to anyone outside of Canada?

Disclosure of personal information

33 *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*

i. Health System Use

ii. Research / Open Data

e) The Sources and Accuracy of the Personal Information

It is your responsibility to make sure that the personal information you collect, store, use and disclose is accurate and complete, especially if the information will be used to make a decision that affects an individual. Ways to make sure personal information is accurate and complete include verifying the information with the person it is about prior to recording it.

- Who is providing the information – the individual or another source (e.g. another government department, a family member, provincial program database)?
- Is the information as accurate and up to date as is necessary for the purposes for which it would be used and disclosed?

FOIPPA section 29 states that a person can ask you to correct any of their personal information in your custody or control. If you cannot correct the record itself, you must make a note on the record (annotate the record). If you've disclosed the personal information to any other public body or third party in the last year, you must also notify them of any corrections you make.

f) Storage and Location of the Personal Information

FOIPPA was amended effective November 26, 2021 and those amendments affect this section.

Disclosure inside or outside Canada
33. A public body may 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;

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Is personal information stored by a service provider?
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.

Provide details on the disclosure, including where and how personal information will be stored. Is the personal information being disclosed outside of Canada?

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.

Are you relying on an existing contract? Please provide details.

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

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

Data Linking

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.

Is personal information from one database linked or combined with personal information from another database?)

Is the purpose for the linkage different from the original purpose for which the personal information in each database was originally obtained or compiled?

Is the data linking is occurring between either two or more public bodies or one or more public bodies and one or more agencies?

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

Common or Integrated Program or Activity

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

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.

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?

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?

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

Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC) as well. Contact the Governance Officer – Access, Privacy and Records Management to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.

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.

g) The Retention Schedule and Method of Destruction for Personal Information

Retention of personal information

31 *If an individual's personal information*

(a)is in the custody or under the control of a public body, and

(b)is used by or on behalf of the public body to make a decision that directly affects the individual,the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.

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

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Keeping information for one year after it is used to make a decision that affects an individual is a minimum requirement under FOIPPA.

You may have other operational or administrative requirements that dictate how long records must be kept and when they must be disposed of. It's important to maintain the records in your initiative according to an approved records schedule.

Answer here or state N/A:

If you answered yes above, please describe retention schedules that apply where retention exceeds the one-year requirement under the Act. Please contact the Governance Officer – Privacy, Access and Records Management if you require assistance.

Answer here or state N/A:

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

Briefly describe your personal information bank and the partners and organizations involved.

Name:

Location:

Description:

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)*.

Purpose:

Category of Users:

Will a database or series of folders be created in this initiative that organizes information by name, identifying number, symbol, or other particular identifier of each individual involved.

If yes, will the records or information collected about the individual contain similar types of personal information. If yes, I will contact the Privacy Officer to ensure that I am identifying that this is a Personal Information Bank (PIB) and identifying the legislatively required descriptors listed in section 69 (6) of FOIPPA.

h) Method of De-identification/Anonymization/Aggregation for Personal Information

PIA#: (assigned by Privacy Office)

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

i) Users of Personal Information

Please list all users of PI including third parties

j) Audits

- 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?
- Are the audit logs immutable?
- Who reads the audit logs, and how long are they kept?
- Who is responsible for oversight of user access?
- 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?)
- 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?
- Will those found to abuse access privileges be sanctioned in a meaningful (and visible) way?

4 Access Rights for Individuals to their Personal Information

Access Request Management

Section 4 of FOIPOP gives individuals the right to access any record under the custody or control of a public body. UNBC is a public body under the Act.

How will you manage access to information requests?

If only aggregate or de-identified data to be released, who is responsible to do so and how is that done?

Request for Personal Information from Persons to Whom It Relates

How will personal requests for access be managed?

Please note*

Individuals do not have to make a formal FOI request to access their own personal information held by UNBC.

5 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 the personal information is safely secured in both physical and technical environments.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

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

a) Security Safeguards

- **Administrative Safeguards**

[redacted]

- **Technical Safeguards**

[redacted]

- **Physical Safeguards**

This question is to identify how you reduce the risk that you store personal information in a computer system or physical location where unauthorized access can happen.

Technical records are records that are stored electronically, including but not limited to records stored:

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

- In a database
- On a LAN (local area network)
- On a hard drive
- On a mobile device or laptop

Technical security includes any digital or electronic system set up to keep your records secure, including:

- Using UNBC firewalls
- Encrypting personal information before it is stored or transferred
- Relying on how your cloud service provider protects information in the cloud
- Using passwords to protect digital files and laptops

If your records are not stored on UNBC servers, use this question to list technical security on the system where records are stored.
Physical records include but are not limited to:

- Paper records
- Film or video
- Photographs
- Audio recordings
- Maps

Physical security is anything you do to keep physical records safe and secure, including:

- Locking filing cabinets and rooms
- Having security guards that patrol the building
- Restricting access to rooms or buildings where information is stored
- Using alarm systems in the building or room where information is stored

If your physical records are not kept in UNBC buildings with standard UNBC security, use this question to list the physical security in the building and rooms in which records are kept. IF there re not physical records you can skip this section.

[redacted]

- **Identify any outside partners or companies involved that may have access to the personal information**

- **Website Domain Ownership (if applicable)**

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

6 Privacy Risk Identification and Mitigation

Risk Rating Overview			
Factor	**Risk Rating**		
	Low	Medium	High
Nature of personal information	✓ Publicly available personal information not associated with any other information	✓ Personal information unique to the organization that is not medical or financial information	✓ Medical, psychological, counselling, or financial information or unique government identification number
Relationships	✓ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	✓ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	✓ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers ✓ Theft by stranger
Cause of breach	✓ Technical error that has been resolved	✓ Accidental loss or disclosure	✓ Intentional breach ✓ Cause unknown ✓ Technical error – if not resolved
Scope	✓ Very few affected individuals	✓ Identified and limited group of affected individuals	✓ Large group or entire scope of group not identified

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Risk Rating Overview			
Factor	**Risk Rating**		
	Low	Medium	High
Containment efforts	✓ Data was adequately encrypted ✓ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	✓ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	✓ Data was not encrypted ✓ Data, files or device have not been recovered ✓ Data at risk of further disclosure particularly through mass media or online
Foreseeable harm from the breach	✓ No foreseeable harm from the breach	✓ Loss of business or employment opportunities ✓ Hurt, humiliation, damage to reputation or relationships ✓ Social/relational harm ✓ Loss of trust in the public body ✓ Loss of public body assets ✓ Loss of public body contracts or business ✓ Financial exposure to public body including class action lawsuits	✓ Security risk (e.g. physical safety) ✓ Identify theft or fraud risk ✓ Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances ✓ Risk to public health or safety

Please 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.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Please explain the risks in detail using the associated CSA Model Code (Appendix B).

EXAMPLE

Risk # 1 Data that is no longer needed is at risk of being breached because it is being retained in the IT platform longer than necessary. **Related CSA Principle:** **Safeguards**	**Cause:** Data is not being deleted from the IT platform in a timely manner once it is no longer needed.
	Probability: Low
	Impact: High
	Mitigation: Implement a process on the IT platform that automatically deletes data once it is no longer needed, per the policy established by X

Risk # 1 **Related CSA Principle:**	**Cause:**
	Probability:
	Impact:
	Mitigation:

Risk # 2 **Related CSA Principle:**	**Cause:**
	Probability:
	Impact:

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

	Mitigation:

Risk # 3 **Related CSA Principle:**	**Cause:**
	Probability:
	Impact:
	Mitigation:

PART C

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: _____
I confirm the information management practices in this initiative have been documented on Form A, and B as applicable, 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:_____

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.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

Signature:_____Date:_____

Chief Information Security Officer

Signature:_____Date:_____

Governance Officer: _____

I confirm that this initiative to the best of my knowledge as written in Form A, and B as applicable, has information management practices that comply with British Columbia's Freedom of Information and Protection of Privacy Act.

Signature:_____Date:_____

PIA Determination and Template

PIA#: (assigned by Privacy Office)

APPENDIX 1
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	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". 1. *Accountability* - 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. *Identifying Purposes* - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. 3. *Consent* - The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate. 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,

PIA Determination and Template

PIA#: (assigned by Privacy Office)

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.
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 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), 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.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

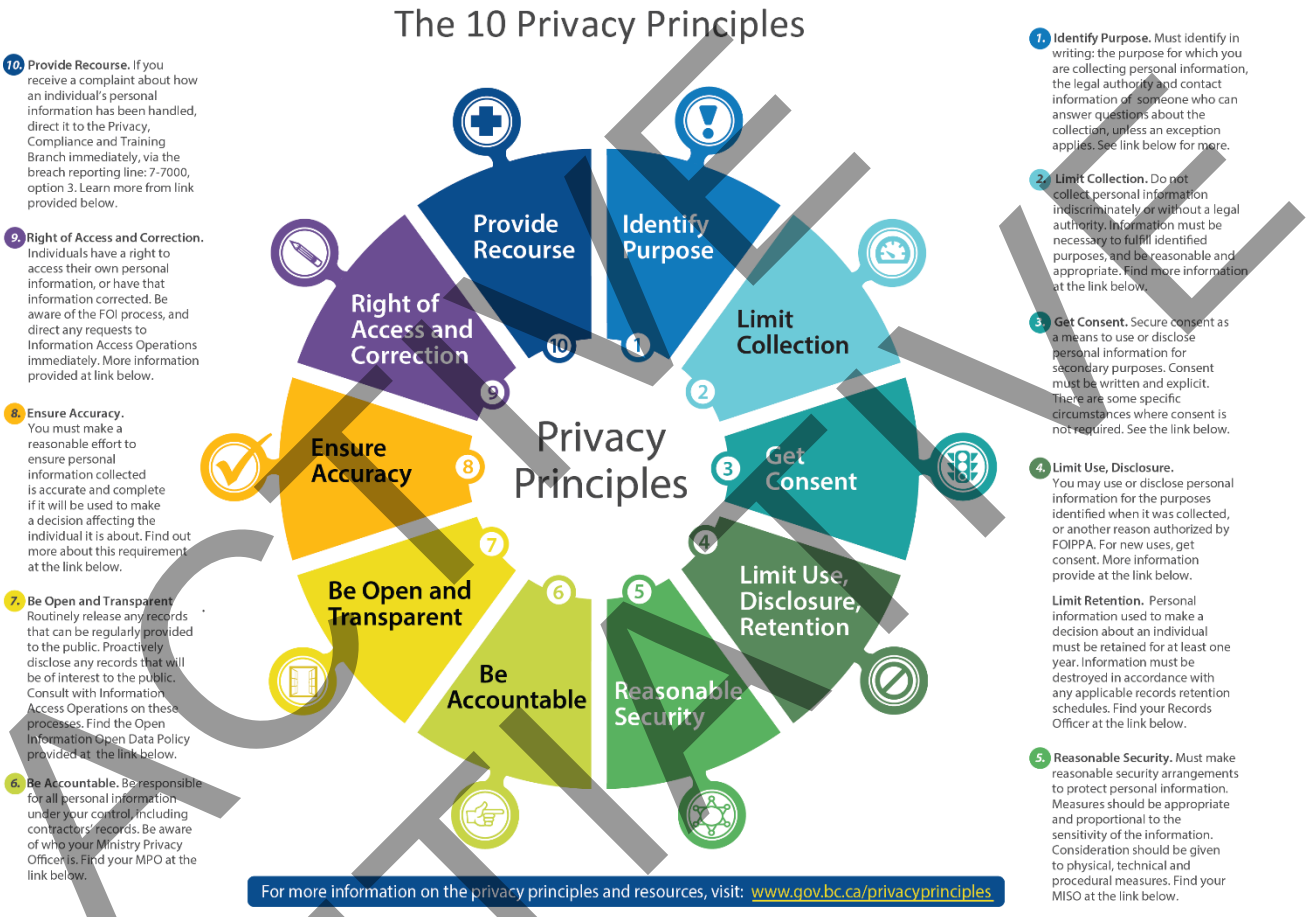
Privacy	Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.
Privacy officer	A privacy officer is a person within an organization whose job it is to: • encourage compliance with sound privacy 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.
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.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

APPENDIX B
CSA MODEL CODES



UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

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 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?

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office)

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

If you still have questions or concerns, please contact: Doris Marshall-Greenlaw, Governance Officer for Access, Privacy and Records Management at 250-960-5139 OR 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.

Signature: _____ Date: _____