UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment ("PIA")

PIA # __21-004_ [Minitab Software]

Form B

Please review the entire form before you answer any questions. Providing more information than the questions asks, providing information answering the wrong questions, or leaving sections blank will delay Privacy Officer approval.

In the following questions, answer the open ended questions in the "Answer here" prompts. Keep bold font on all answers provided. Answer **Yes / No** questions by deleting the answer that does not apply. Do not add open ended text to **Yes / No** responses.

Name of Department: **Information Technology Services**

PIA Drafter: **Lori Olson**

Email: **lori.olson@unbc.ca** Phone: **250-960-6730**

Oversight Provided by: **Trevor Fuson**

Email: **trevor.fuson@unbc.ca** Phone: **250-960-5687**

Institutional Approvals and Assessments

I have contacted the Chief Information Security Officer to complete all required physical and technical security assessments to ensure my initiative complies with industry standards as applicable to my initiative. **Yes**

I have contacted the Contracts and Supply Chain Management department to complete a review that ensures the purchasing agreement, service agreement, contract, MOA, MOU or other contractual agreement with any external parties involved ensures the compliant management of any information that UNBC provides about its stakeholders. **Yes**

Does the initiative involve systematic disclosures of personal information outside of UNBC? If yes, I will contact the Privacy Officer to ensure that an Information Sharing Agreement is in place. **No**

Does the program involve access to personally identifiable information for research or statistical purposes? If yes, I will contact the Privacy Officer to ensure that an Access to Restricted Records Agreement is in place **No**

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment ("PIA")

PIA # __21-004_ [Minitab Software]

Data-linking Initiative

In FIPPA, "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? **No**

Is the purpose for the linkage different from the original purpose for which the personal information in each database was originally obtained or compiled? **No**

Is the data linking is occurring between either two or more public bodies or one or more public bodies and one or more agencies? **No**

If I have answered yes to the above three questions, I will work with the Privacy Officer to ensure I meet the requirements for a data-linking initiative? **N/A**

Common or Integrated Program or Activity

In FIPPA, "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? **No**

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? **No**

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

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 Information Governance Officer to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment ("PIA")

PIA # __21-004_ [Minitab Software]

Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, complete the Description / Purpose 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 work flow. 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. This table must be accompanied by a workflow diagram if practices are not transparent or if the PIA is related to a common or integrated program or activity or a data-linking initiative.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*UNBC ITS set up accounts using Student UNBC login credentials.*	*Collection*	*26(c)*
2.	*Student inputs username and password.*	*Collection*	*26(c)*
3.	*Minitab single sign on gets authentication from the active directory file system (first name, last name and email)*	*Protection*	*30*
4.	*Students access Minitab to complete assignments as directed by the instructor.*	*Use*	*32(a)*
5.	*Students complete assignments and the work is saved on UNBC servers as the software is hosted in VDI.*	*Collection*	*26(c)*

Risk Mitigation Table

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.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	[redacted]			
2.				
3.				

4.				

Collection / Consent Notice

If your initiative is collecting personal information directly or indirectly from individuals, you must ensure that all individuals involved are told the following:

- The purpose for which the information is being collected
- The legal authority for collecting it, and
- The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please include your proposed wording for a collection & consent notice and where it will be located for individuals to read before collection takes place in the space below. The Privacy Officer will review and provide feedback.

Copy/Paste or Fill in here – N/A Minitab does not store any personal information.

Information Management Controls

Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information. How is access to information monitored and logged?

SINGLE SIGN ON

Students will be required to sign in using Single Sign On (SSO) to use the software to complete assignments. The software is hosted in VDI on UNBC servers and can be used on local machines.

DATA ENCRYPTION

ENCRYPTION IN TRANSIT AND AT REST

[redacted]

PASSWORD ENCRYPTION

[redacted]

SECURITY LOGS AND PATCHES

[redacted]

CERTIFICATE VALIDATION

The desktop application uses the underlying Windows network infrastructure, which uses both OCSP and CRLs, to validate certificate paths. Browsers also validate certificate paths in accordance with their individual standards.

How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated. If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

Updates to personal information are done through Active Directory, which is a UNBC system.

User accounts are established in the Minitab License Portal by UNBC authorized representative(s). The following features exist to support the security of UNBC's accounts:

• **Privilege Levels:** User accounts can be segregated to provide different privilege levels for individual user accounts.

• **Automatic sign out (web):** When a user signs in through a browser, the application session continues until the browser session is closed or the user signs out of the application. If the browser is closed without explicitly signing out, the application will check to see if a user is still active after 15 minutes and if not, the user will be signed out.

• **Keep me signed in (desktop):** The desktop application has a "Keep me signed in" feature that allows users to remain authenticated after closing and reopening the application. To support this feature, the desktop application encrypts the authentication token it receives when the user signs in, then saves the encrypted token to the user's hard drive. The token is encrypted using the machine crypto key, the user's Windows sign-in credentials, and a key that Minitab determines. The user must explicitly turn this feature on and has the option to turn it off.

• **Failed Log-Ins:** After 5 failed sign-in attempts within 1 hour, the application disables accounts for 1 hour.

Information Disposal

Does your initiative use personal information to make decisions that directly affect an individual(s)? **No**

If you answered "yes", please explain the efforts that will be made to ensure that information management from collection to disposal will ensure that information used to make a decision about someone is accurate, complete, available when needed and disposed of to meet legal requirements. Describe the records retention timeline for the records generated from this initiative.

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 Information Governance Officer if you require assistance.

N/A

Personal Information Banks

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. **No.**

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 FIPPA. **No**

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment ("PIA")

PIA # __21-004_ [Minitab Software]

Privacy Officer Comments, Conditions & Concerns

This PIA is based on a review of the material provided to the Senior Project Consultant (Privacy Officer) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA update and submit for approval.