Privacy Impact Assessment

PIA # and Name- ARPM_PIA2310

Legislative Requirement

Under Section 69 (5.3) of FIPPA UNBC is required to conduct a privacy impact assessment (PIA)and must do so in accordance with the directions of the Minister responsible for the Act.

A PIA needs to be conducted
- For a new initiative for which no PIA has previously been conducted.
- Before implementing significant change to an existing initiative, including but not limited to a change in the location in which sensitive personal information is stored.
- At the discretion of the person(s) with delegated authority under section 66 of the Act

1. Accountability

1.1 Identify Department, Branch, or Program Area involved in the initiative

IT Services, within the portfolio of the Vice President Finance and Administration

1.2 Identify UNBC role responsible for the Initiative

Manager, IT Infrastructure and Operations

1.3 Describe the Governance Model – who is accountable for the program or system.

This initiative falls within the portfolio of the VP Finance and Administration. The lead for this initiative is the Manager, IT Infrastructure and Operations. The Dean/Director providing oversight is the CIO

1.4 Timeline for the initiative

Anticipated start date for the initiative,

March 15, 2024

Is this a one-time event?

☐ Yes ☑ No

2. Overview

2.1 Describe the New Program or Service or the Change.

ITS will be using a cloud-based management tool set available from Microsoft called Intune. Intune is a product available from Microsoft that enhances the ability for organizations of all sizes to support, maintain, and ensure compliance of computers, laptops and other devices under the charge of that organization.

Intune provides a myriad of new services such as autopilot, auto-update, SSO integration, app stores, self service features, etc., that will provide a better user experience while at the same time providing increased adaptability with the evolving user requirements of remote work and the security needs of modern systems and enhanced technical support capabilities

2.2 Describe the Purposes, Goals and Objectives.

UNBC will be using Microsoft Intune for the following reasons
- Increase the capabilities of ensuring patching compliance, which is inline with the CISO and OCIO of BC's recommendations
- Provide better capabilities of managing off-campus computers like Laptops and Offsite-Work-Location devices, part of the OWL-P program.
- Increase the capabilities for ITS to respond to a variety of situations like a lost device, a compromised device, or a device that is stolen
- Empower ITS to be able to respond to incidents with devices both on and off campus, and around the world as required.
- Meet the needs of the CISO for compliance reporting for devices owned by UNBC

2.3 List any Relevant PIAs

M365 PIA, Azure PIA, Windows 11 PIA

2.4 List any relevant contracts or software purchases.

Be sure to follow UNBC guidelines regarding purchasing policies.

UNBC Micosoft Campus Agreement, specifically the academic agreement that is renewed annually.
UNBC has a corporate purchasing agreement with apple where we obtain pre-registered devices in ASM
UNBC has a corporate purchasing agreement (via BCNet) with microserve for DELL computers which will arrive pre-registered in Intune

2.5 List all interested parties impacted / Involved
(i.e. who are you collecting information from, UNBC roles accessing/using information, 3rd parties with whom you will share information)

Interested Party	Role in the initiative
ITS exempt employees	accountable for ITS department and individual units within the ITS group
ITS Staff employees	responsible for system integration, system management, and configuration of the system settings (known as compliance policies) and day-to-day work with the system
non-ITS employees	will have devices managed by the Intune system, and will have metadata about the devices that they are using incorporated into the system
Information Security Office (CISO and Security Analysts)	advise on compliance and configuration policies, can audit compliance and access system in read-only capacity
Students & Community Users	students and community users may use devices that are managed with this tool, as such some information may be collected like login time-stamps and login performance data of the device.

3. Collection of Personal Information

3.1 List the data elements or personal information involved in your initiative.

Data Element name, email, id#, grade	Rationale for collection	Method of Collection	FIPPA Authorization
Computer Hardware Metadata, ie RAM, CPU, BIOS, Manufacturer, Model,	Collected by the Intune application and necessary to ensure the capabilities and patching compliance of managed devices	Direct Indirect NA	26(c)
file metadata, i.e. Filename, Created Date, Modified Date, extension, created by	Collected by the Intune application and necessary to ensure the capabilities and patching compliance of managed devices	Direct Indirect NA	26(c)
User metadata, such as UPN, username, email address, group membership, and data about the login timestamp and device login performance, AppleID	Collected by the Intune application and necessary to ensure the capabilities and patching compliance of managed devices	Direct Indirect NA	26(c)
Application Information. For example application name, version, publisher.	Collected by the Intune application and necessary to ensure the capabilities and patching compliance of managed devices	Direct Indirect NA	26(c)
Apple School Manager information collected is limited to serial number, device model (from which you can infer CPU, RAM, and other system specifications) as well as Purchase Order Number	Collected by the Intune application and necessary to ensure the capabilities and patching compliance of managed devices	Direct Indirect NA	26(c)
		Direct Indirect NA	TBD
		Direct Indirect NA	TBD

3.2 Describe how personal information is to be collected.

If you already have a collection notice, attach it as an appendix.

All personal information is synced through Microsoft's AzureAD Connect tool. When ITS integrated the ASM (Apple School Manager), an additional data source from Apple Computer Inc. was linked, however there is no personal information collected via that linking of systems.

During Enrolment if there are problems with the Autopilot process, diagnostic information will be collected that may include username and device name. This is limited to only UNBC owned devices. Microsoft Support may access this diagnostic information in the course of troubleshooting on UNBC's behalf.

The audit logs for Intune capture data about processed taken within the intune platform. For example when a technician is updating an application publication information about which technician is doing the work, the target that the work is being done one, category, name, operation type, and timestamp is all collected to be reviewed.

4. Use of Personal Information

4.1 List all users of PI and Describe how personal information is to be used.

User (UNBC Roles e.g Governance officer)	How the info is used	FIPPA Authorization
ITS Staff	within the intune workflow for troubleshooting purposes, to verify user account registration on a particular device. Information may be used for verification of action, inaction, or used to inform a report, or trigger an action as needed for regular or emergent work as required.	32(a)
Staff from the Office of the Chief Information Security Officer	used to help with incident response data collection and information we well as security auditing	32(a)
		TBD
		TBD
		TBD
		TBD
		TBD

4.2 Describe the record management of Personal information involved in the initiative.

Does the initiative involve using personal information to make a decision about an individual?	Does the initiative have a retention schedule regarding personal information used to make decisions?
☐ Yes ☑ No	☐ Yes ☑ No

If the initiative involves using personal information to make a decision about an individual, but does not have a record retention schedule, 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.

N/A

5. Research/ Health System Use of Personal Information

5.1 Will data collected through this initiative be used for research or health system use?

☐ Yes ☑ No

If "Yes" answer the following questions, if"No" please proceed to the next section.

5.2 Explain and provide details of data state (aggregate, de-identified,anonymized etc.)

5.3 If data will it be disclosed as part of Health System Use, provide details on the method of disclosure, as well as where and how personal information will be stored by 3rd party.

5.4 If data will it be disclosed as part of Research/ Open Data, provide details on the method of disclosure, as well as where and how personal information will be stored by 3rd party.

6. Storage of Personal Information

6.1 Does the initiative involve digital tools, databases, or information systems?

☑ Yes ☐ No

If yes, contact UNBC Information Security to determine whether the initiative requires a security and threat risk assessment.

6.2 As part of this initiative, will Personal information be store outside of Canada?

☑ Yes ☐ No

6.3 Describe how information will be stored during this initiative (i.e., cloud storage, SaaS, etc).

This information will be stored on Microsoft Servers located worldwide based on Microsoft's automated systems. (SaaS)
When apple devices are registered, Apple and Microsoft share data about the device using the Apple Device Enrolment Program (DEP), the Apple MDM Push Certificate (APNS), the Apple Scool Manager tool (ASM), and the Apple Volume Purchase Program (VPP). Specific accounts are created on the Microsoft and Apple systems to enable this integration for device registration.

Information collected in the Apple School Manager includes the Serial Number of the Device, the Part Number, Model, and Order Number, and the date added to the system. This information is shared directly with the Intune platform via the integration mentioned earlier in section 6.3

7. Disclosure of Personal Information

7.1 Does the initiative involve disclosing information to 3rd parties (i.e. non-unbc employees?

☑ Yes ☐ No

If "Yes" answer the following questions, if "No" please proceed to the next section.

7.2 Provide details on the disclosure,including to whom, purpose, method of disclosure, and how personal information will be stored by 3rd party.

UNBC IT Services may engage Microsoft Support technicians to address specific technical issues. Only at the time that UNBC ITS requests service will Microsoft employees seek access to the information within the UNBC tenant.

There will be no other disclosure to other parties

Within UNBC, ITS will not disclose information found, collected, or amalgamated in the intune management console.

7.3 If disclosing information to anyone outside of Canada, Provide details regarding to whom purpose , method of disclosure,and how personal information will be stored by 3rd party.

The access by the 3rd party will be incidental as part of a technical troubleshooting and resolution process. Microsoft will not store personal information about systems managed within the system, but may collect troubleshooting logs and pertinent information to address the issue presented.

8. Accuracy and Correction of Personal Information

8.1 How will you make sure that the personal information collected is accurate and complete?

The information collected by Intune is collected directly from the computers, there is no intervening process or translation. The system will automatically update information as it is collected.

ITS does not change, manage or update personal information manually, rather ITS relies on UNBC's ERP (Ellucian Banner) as the authoritative record repository for personal information and is referenced regularly by automated scripts to apply the appropriate updates.

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

☑ Yes ☐ No

8.3 If yes, please describe your process below?

Automatically done by script when updated by the appropriate record holder (HR or Registrar's Office)

8.4 Describe the process of how you will make a note on the record, if you're not able to correct the record itself.

N/A

8.5 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, how will you ensure that you conduct these notifications when necessary?

UNBC does not disclose personal information outside the Intune/Azure system so no notifications are required.

9. Personal Information Bank

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

9.1 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.

9.2 Describe the business purpose for the information bank (i.e., account management of clients/ students).

9.3 If aggregate reports are generated from the information bank, explain how Personal Information will be de-identified or anonymized.

9.4 Describe the category of users and the information to which the user will have access

Category of Users (i.e., system admin, clerk, etc.)	Information accessed (i.e. contact info, grades, fee etc.)

9.5 Identify the UNBC role(s) responsible for managing user accounts and audit user access.

9.6 Describe the process for auditing user access.

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

9.7 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

☐ Yes ☐ No

9.8 Are the audit logs immutable?

☐ Yes ☐ No

9.9 Is the system responsive or passive?
Is it possible to put a monitor on particular individuals? Will access produce an immediate response/notification or a log entry for review?

9.10 How will those found to abuse access privileges be sanctioned ?

10. Common or Integrated Program or Activity

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.

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

☐ Yes ☑ No

10.2 Does this initiative involve a program or activity that provides a service(s) through UNBC that is working on behalf of one or more other public bodies or agencies?

☐ Yes ☑ No

10.3 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

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.

11. Privacy and Security Safeguards

11.1 Describe administrative safeguards(i.e. policy documents, procedures, or training).

[redacted]

11.2 Describe physical safeguards(i.e. locked, filing cabinets, locked doors, or restricted areas).

[redacted]

11.3 Describe the controls in place to prevent unauthorized access to personal information(i.e. role-based access to software, access logs).

[redacted]

11.4 Describe technical safeguards(i.e. firewalls, encryption, or intrusion prevention systems).

[redacted]

12. Privacy Risk Identification and Mitigation

Identify any privacy risks and the corresponding mitigation strategies that will be implemented. Try to include at least one risk related to each step in the information cycle (collection, use, storage, disclosure,and retention. Refer to the risk classification table to assist with likelihood and impact rating.
If you are disclosing or storing data outside of Canada you will need to identify additional risks related to storage/disclosure outside of Canada.

12.1 Risk Description	Likelihood	Impact	Risk level	Mitigation Strategy Describe how above safeguards could be used to mitigate the risk
[redacted]				
	Certian Likely Moderate Unlikely Rare	Severe Major Significant Minor Insignificant		

13. Collection Notice

All collection notices must include the:
- Purpose for the collection
- Legal authority for the collection
- Contact information for an employee of UNBC who can answer the individual's questions about the collection.

The employee responsible for responding to data collection questions should be able to explain why the personal information is being collected and how it will be used, retained, and disclosed.

The contact method should suit the collection method. For example, if you collect personal information through an online form, you could include an email contact.

13.1 Privacy notice

Be sure to include all 3 required parts of the notice

UNBC IT Services uses Microsoft Intune to continue to meet the ever present needs to provide a well managed, up to date, and secure computing ecosystem at UNBC. This system enables robust management capabilities for devices on campus and off campus. In addition, this tool will help ITS and UNBC ensure that devices that are lost, or stolen can be properly managed according to the classification of the device. Additionally this system will empower ITS to be able to respond to cyber security incidents on enrolled devices regardless of the location of the device.

UNBC ITS takes precautions to protect the data collected by the system in the course of its use. The type of data collect by the system is metadata, or data-about-data. For example, this system will collect information about the device that you are using including some information about the files on the device. This information will be used to ensure that the device you are using is compliant with the security and patching expectations outlined by the CISO and the OCIO of BC.

Should you have questions about this, you can contact the Manager of Infrastructure and Operations at ManagerITIO@unbc.ca

13.2 Location of Privacy Notice

If the notice is to be posted on the website please include url of webpage.

This notice will be provided as part of the purchase and acquisition process.

14. Signing and Approval

Individual leading the Program/Project: Kevin Schretlen

Position: Manager, IT Infrastructure and Operations

I confirm the information management practices in this initiative have been documented as accurately as I am aware. I commit to communicating appropriate information management practices to all individuals participating in this initiative. 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: [redacted] **Date:** March 17 2024

Trevor Fuson

Director/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: [redacted] **Date:** March 15, 2024

Lisa Haslett

Vice-President authorizing the Program/Project:

I confirm that this initiative to the best of my knowledge as written in the above sections,has information management practices that complies with policies and procedures of the University of Northern British Columbia.

Signature: [redacted] **Date:** March 15, 2024

Privacy Officer reviewing the Program/Project: Christopher Ross

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 and Protection of Privacy Act.

Signature: [redacted] **Date:** March 18, 2024

15. Reference Tools

"**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,

(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.

Privacy Impact Risk assessment:

Likelihood that identified risk will occur / Probability	Impact: Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
almost certain 5	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
Likely 4	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
Moderate 3	Low 3	Medium 6	Medium 9	High 12	Very High 15
Unlikely 2	Very low 2	Low 4	Medium 6	Medium 8	High 10
Rare 1	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Risk Rating	*Risk Levels	Description	Actions Required
1-4	Minimal	Unlikely that associated risk would result in harm to privacy	Review of safeguards to be done at PIA review date
5-9	Moderate	Unlikely that associated risk would result in significant harm to privacy	annually review existing safeguards required
10-16	Elevated	Likely that associated risk would result in harm to the privacy	Routine monitoring of data processing or additional safeguards required
17-25	Unacceptable	Associated Risk would likely cause significant and immediate harm to the privacy	Must not proceed as existing safeguards and controls are insufficient

Return to Risk Matirix