PRIVACY IMPACT ASSESSMENT (PIA)
CLOSURE SUMMARY

Initiative	Microsoft Azure for Network Refresh (CISCO ICE/Landing Zone) and potentially other use cases
PIA Reference #	2025-002
PIA Completion Date	January 9, 2025
Project Sponsor	Jordan Osiowy – Cyber Security Manager
Unit	Technology Services

The purpose of a PIA is to determine whether an initiative complies with the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and JIBC's policies and procedures. This document is to advise that the PIA review of this initiative has been completed. The following outlines the scope, issues, legal basis and conclusions associated with this PIA.

Initiative Description & Scope

The current use case for Azure re: the network refresh project is that the JIBC-managed Azure tenant will be used to host virtual appliances for Cisco ISE, which links with Meraki systems and onsite network gear to facilitate dynamic assignment of network zones based on what device is connected via ethernet cable. For example, if you plus an ethernet cable into a JIBC laptop, the laptop will have access to JIBC services, network drives, etc. If you plug in a personal computer, the computer will only have access to the internet.

Please see the email correspondence at Schedule C for more detailed information about this use case.

In addition to the current use case, Technology Services would benefit from having Azure approved from a privacy-perspective for more general use.

Information Reviewed

Our review is based on the following information provided by the project team:

a) completed PIA Risk Classification Tool, the summary of which is at Schedule A.
b) completed PIA Questionnaire, completed by Jordan Osiowy, which is attached at Schedule B; and
c) email correspondence with Jordan Osiowy, which is attached as Schedule C.

Risk Classification

Based on the information in the PIA Risk Classification Tool, the proposed tool has a risk classification level of "**Medium**", with a score of 9. Please see Schedule A for more information.

Legal Basis - Privacy

According to the PIA Questionnaire, the proposed tool will not involve the collection of personal information.

According to Technology Services, to determine level of access to allow, the tool will need to access active directory, which will give it access to business contact information of employees, as well as employee IDs; and student names and numbers. Pursuant to section 32(a) of FIPPA, a public body may use personal information in its custody or under its control for the purpose for which the information was obtained, or compiled, or for a use consistent with that purpose. The use being contemplated here is to determine the appropriate level of access to technology systems based on role, which is important as users need to access technology systems for their various roles within the institution.

Pursuant to section 33(2)(d) of FIPPA, a public body may disclose personal information for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.

Pursuant to section 34 of FIPPA, a use or disclosure of personal information is consistent with the purpose for which the information was obtained or compiled if the use: (a) has a reasonable and direct connection to that purpose; and (b) is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.

On its face, the proposed use and disclosure of any personal information appears to have a reasonable and direct connection to the purpose for which any such personal information may have originally been collected. It is also necessary for the activities of the public body, as these individuals must access technology in connection with their roles at the institution.

Section 33.1 of FIPPA requires additional analysis be conducted when sensitive personal information will be disclosed to be stored outside of Canada. Technology Services has confirmed that the proposed tool utilizes data centres offsite within Canada.

No further analysis is required.

Legal Basis - Security

Pursuant to section 30 of FIPPA, a public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.

Technology services has confirmed that no personal information will be collected. Technology Services has confirmed that they believe reasonable security measures are in place, such as accessibility limitations based on role and physical location, firewall restrictions, and limited number of individuals in Technology Services having administrative access rights.

No further analysis is required.

Conclusions

Based on the information provided, our review has concluded that there are no significant privacy or security risks introduced by the use of this proposed tool for the proposed use case.

In addition, the proposed tool may be used for additional use cases without requiring a privacy impact assessment under the following conditions:

1. The proposed tool is not used to collect personal information.
2. The proposed tool either uses on premises servers, or Azure cloud-based servers.
3. Personal information is only used or accessed within Canada.
4. The type and sensitivity of personal information used or disclosed by the proposed tool does not materially vary from that of the current use case.
5. Technology Services believes that there are reasonable security measures in place to mitigate the likelihood and impact of a breach of personal information with respect to the new use case.

Responsibilities

Technology Services is responsible for informing the General Counsel of any material omissions or inaccuracies in the information relied upon in this PIA, and submitting to the General Counsel a new PIA request if there are any significant changes to this initiative. Technology Services is also responsible for informing the General Counsel of subsequent use cases for the proposed tool that fall outside of the criteria of the criteria described above under “Conclusions”.

If you have any questions or concerns about this PIA, please contact the General Counsel.

SCHEDULE A
PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

Please see attached.

IMPACT			Score
1	How many individual records will be stored, accessed or used?	Less than 10; may be more in very limited situations	1
2	What is the most sensitive type of Personal Information in these records?	No PII; in limited situations, may have access to student name and ID	3

PROBABILITY			Score
3	Where will the information be stored?	Off-campus (inside Canada)	3
4	How many users will have access to the information?	1-20	2

PIA Priority Rating Table					
Impact	Probability				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Colour Coding Key
LOW
MEDIUM
HIGH
VERY HIGH

Classification for this Project	
9	
Medium	

Justice Institute BRITISH COLUMBIA

LEARNING THAT TAKES YOU BEYOND

Legend

CLASSIFICATION	
Risk_No.	Risk_Rank
1	LOW
2	LOW
3	LOW
4	LOW
5	MEDIUM
6	MEDIUM
7	MEDIUM
8	MEDIUM
9	MEDIUM
10	MEDIUM
11	MEDIUM
12	MEDIUM
13	MEDIUM
14	MEDIUM
15	MEDIUM
16	HIGH
17	HIGH
18	HIGH
19	HIGH
20	HIGH
21	VERY HIGH
22	VERY HIGH
23	VERY HIGH
24	VERY HIGH
25	VERY HIGH

1- NUMBER OF RECORDS	
Records	Rec_Rank
1-1000	1
1,001-10,000	2
10,001-100,000	3
100,001-1,000,000	4
1,000,000+	5

2- INFORMATION TYPE	
PI_Risk	PI_Type
N/A - No Personal Information	0
Student Information	3
Donor, Alumni & Other Third Party Information	3
Credit Card Information	5
Employee Information	7
Health Information	7

4- LOCATION OF INFORMATION	
Location	Loc_Rank
On-campus (UBC IT data centre)	1
On-campus (other)	2
Off-campus (inside Canada)	3
Off-campus (outside Canada)	5

5- NUMBER OF USERS	
Users	Use_Rank
1-10	1
11-100	2
101-1,000	3
1,001-10,000	4
10,001+	5

SCHEDULE B
PIA QUESTIONNAIRE

Please see attached.

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

for

Microsoft Azure for Network Refresh (CISCO ICE/Landing Zone)

1. Purpose of the Privacy Impact Assessment Questionnaire

This form is used by JIBC to provide a high-level overview of the potential privacy risks of a current or proposed policy, system, project, program or activity. The results of these screening questions help judge the level of potential risk, the extent to which risk mitigation strategies may be needed and when completion of a privacy impact assessment is required under the *Freedom of Information and Protection of Privacy Act* (British Columbia) (the "**Act**").

2. Privacy Questions

Questions	Answers
Does the program involve personally identifiable information (PII) (as defined by the Act)? [Y/N]	N
Will the program involve the collection or creation of new information about individuals? [Y/N]	N
Will personal information about individuals be disclosed to organizations, programs, processes or people who have not previously had routine access to the information? [Y/N]	N
Will personal information about individuals be used for a purpose it is not currently used for, or in a way it is not currently used? [Y/N]	N
Will the program require contacting individuals in ways that they may find intrusive? [Y/N]	N
Does the program have a collection notice or use policy? [Y/N]	Y

3. Technology Questions

Questions	Answers
Does this program involve the implementation of a new electronic system or use of a new application or software to support the creation, collection, updating or storing, backing-up or disposition of personal information? [Y/N]	N
Does this program require any modifications to existing information technology (IT) systems (e.g., integration with or consolidation of other IT systems)? [Y/N]	Y
Will a new or modified electronic system change the existing business workflow? [Y/N]	Y
Does the program involve the use of new technology that might be perceived as being privacy intrusive? [Y/N]	N

4. Impact Questions

Questions	Answers
What are the purpose of collection, use and/or disclosure of the personal information? [Internal/External/Both]	Both
Will personal information about the same individual that was previously maintained separately now be aggregated and stored together? [Y/N]	N
How would you describe the information classification level of the personal information? (Select all that apply) • Highly Confidential • Confidential • Public	No PII bit Network configurations should be confidential
What are the type(s) of personal information? (Select all that apply) • Bio/demographic information • Academic/education Information • Employment information • Medical/health Information • Financial Information • Criminal information • Images • Opinions about individuals • Individuals' personal views and opinions • Business contact information • Personal contact information • Other	Business Contact Info
What are the type(s) of individuals? (Select all that apply) • Prospects • Applicants • Students • Employees • Donors/alumni/other 3rd parties • Volunteers • Service providers • Other	<10 TS Employees

How many records documenting individuals will be stored, accessed, used or disclosed? [1-1000], [1001-5000], [5,001-50,000], [50,001-100,000], [100,000+]	
How many JIBC employees, volunteers and service provider employees will be able to access, collect, use or disclose the information? [1-10], [11-50], [51-100], [101-250], [251-500], [501-1,000], [1,000+]	<20 Tech Services Employees
Is any of the information owned by another organization? [Y/N]	N

5. Probability Questions

Questions	**Answers**
Where will the information be stored? (Select all that apply) • On campus – JIBC servers • On campus – other • Off-campus – inside Canada • Off-campus – outside Canada	• Off-campus – inside Canada
Is any of the information accessed from outside of Canada? [Y/N]	N
Will personal information be transmitted? (Select only one) • Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled) • Personal information is used in a system that has connections to at least one other system • Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed • Personal information is transmitted using wireless technologies	• Personal information is used in a system that has connections to at least one other system
Will a third party (e.g., vendor or service provider) have access to the information? [Y/N]	N
Will the program result in different record keeping systems converging? [Y/N]	N

SCHEDULE C
EMAIL CORRESPONDENCE

Please see attached.

From: Osiowy, Jordan
To: Deacon, Derek
Cc: Pakula, Roman; Gregorowicz, Peter; Flipse, Brigid
Subject: Re: PIAs for network refresh
Date: November 27, 2024 7:55:17 AM

Thanks Derek

Meraki is a sub-brand of Cisco that provides cloud-managed networking solutions (compared to traditional Cisco products where the control plane is hosted on customer infrastructure). It provides centralized management of Meraki-branded network equipment, with the management platform hosted in the cloud on Cisco's infrastructure located inside Canada. The information that gets stored in Meraki is all network configuration information and wouldn't be information about any individual. For support purposes, there would be business contact information for Roman and members of his team that gets shared with Meraki.

The Azure use case for the network project is [redacted] S. 15(1)(l)
[redacted] For example - if you plug a network cable into your JIBC laptop, you get network access to servers, network drives, etc. but if you bring a personal device to work and plug it in you just get internet access. S. 15(1)(l) [redacted]

For the Azure use case above, the servers in Azure would be [redacted] S. 15(1)(l)

All of the Azure infrastructure that is part of this network project would be hosted in our existing Azure tenant that we manage ourselves and would be located in Azure's Canada-Central geo which represents two Microsoft datacenters located in Canada. Microsoft doesn't

access the data in customer tenants themselves (only we do), and we apply access controls and security features there that are similar to what we have on-premises. We are getting deployment support from Compugen for this project that includes work to build out landing zones in Azure that follow best practices from an architecture perspective. Also, none of the systems we are putting in Azure for this project would be reachable from the public internet - only from JIBC, and firewall rules would restrict access to/from our Azure tenant to only allow the specific uses required. Management of the systems in Azure would be restricted by role, with only a couple people in TS having management access to the platforms.

In terms of a more general Azure PIA - we don't have specific timelines or use cases that are well defined, but every team in TS has an appetite to make broader use of Azure. If we were to make a more general-purpose PIA for Azure that allows folks in TS to make use of Azure services as long as they meet certain criteria (for example that the chosen services are located in Azure's Canada geo, make use of our existing landing zones, etc.) it would help facilitate those efforts as they move forward. Some examples of potential Azure use cases in the future would be moving databases from our on-premises SQL servers to an Azure SQL service, converting virtual machines from our VMWare infrastructure into Azure virtual servers, or hosting offline replicas of servers to be used for disaster recovery or business continuity purposes. Microsoft has more privacy information here: https://azure.microsoft.com/en-us/explore/trusted-cloud/privacy

If you think this is better to talk through in a call let me know and I'll set something up for us.

Thank you!

Jordan Osiowy (He/Them)
CYBER SECURITY MANAGER
TECHNOLOGY SERVICES

OFFICE: 604.528.5561
jibc.ca

From: Deacon, Derek <ddeacon@jibc.ca>
Sent: Wednesday, November 20, 2024 2:07 PM
To: Osiowy, Jordan <JOsiowy@jibc.ca>
Cc: Pakula, Roman <rpakula@jibc.ca>; Gregorowicz, Peter <pgregorowicz@jibc.ca>; Flipse, Brigid <BFlipse@jibc.ca>
Subject: RE: PIAs for network refresh

Hi Jordan,

Thanks for sending these over and sorry to only now be looking at them closely. Might be a good opportunity for us to chat briefly, unless you can provide some clarity on a few

things over email here. The Meraki one seems very simple – no PII. Can you tell me a bit more about what Meraki is and what it does?

The Azure one seems simple as well, though I note that while it says no PII in several spots, it mentions the use of PII in others. For this specific CISCO ISE context, is there no PII (meaning nothing except for perhaps business contact information, which is what appears on your email signature or your business card)? Further to that, if you think it might make sense to do a more generic, future-proof PIA for Azure because you foresee some further use cases, would those use cases involve PII and how (if at all) would/could those use cases change re: nature and quantum of PII collected/used/disclosed, where stored, etc.?

Again, please feel free to respond here or suggest that we set up a time to chat in the next week or two. I'm good either way.

Cheers.

Derek

Derek Deacon (he, him, his), JD, BBA
General Counsel

office: 604.528.5897

jibc.ca

From: Osiowy, Jordan <JOsiowy@jibc.ca>
Sent: October 29, 2024 4:25 PM
To: Deacon, Derek <ddeacon@jibc.ca>
Cc: Pakula, Roman <rpakula@jibc.ca>; Gregorowicz, Peter <pgregorowicz@jibc.ca>; Flipse, Brigid <BFlipse@jibc.ca>
Subject: PIAs for network refresh

Hi Derek

Roman and I went through the PIA questionnaire for Meraki Dashboard and Microsoft Azure. Questionnaire forms are attached. Neither the Meraki dashboard or the Cisco ISE software that will be running in Azure will be handling PII and both are hosted in Canada.

We filled out the Azure one specifically for the CISCO ISE but we were thinking we may

want to go through a more generic PIA for Azure to cover future use cases. The longer term goal not directly related to this immediate project will be to move existing services from our onprem datacenter into Azure so it would be helpful to be able to consider the Azure platform as an extension of our existing server infrastructure. Is that something we could discuss when you're back in the office?

Jordan Osiowy (he/them)
Cyber Security Manager
TECHNOLOGY SERVICES