Privacy Impact Assessment for

Microsoft Cloud Services - Update

PIA# CITZ17025

Part 1 – General

Name of Ministry:	Citizens' Services		
PIA Drafter:	**Matt Reed**		
Email:	Matt.Reed@gov.bc.ca	Phone:	**250-514-8870**
Program Manager:	**Derek Rutherford**		
Email:	Derek.Rutherford@gov.bc.ca	Phone:	**250-356-7915**

1. Description of the Initiative

The Government of British Columbia (BC) is moving forward with adoption of Microsoft Cloud Services with an in-Canada data residency option for the delivery of IT services to the BC public service. Adoption of Microsoft's services is being conducted in a methodical, phased approach that permits the assessment and evaluation of each level of service that is added. Microsoft Cloud Services in Canada provides an ideal opportunity for modernization, increased agility and to dramatically improve information security and privacy.

When using Microsoft's Cloud Services, government remains the sole owner of its data; government retains the rights, title, and interest in data stored in all cloud services. Across Microsoft's Cloud Services, Microsoft's role is limited to that of a data processor.

By leveraging Microsoft's cloud services located in Canada (Ontario and Quebec), the government's Office of the Chief Information Officer (OCIO) considers Microsoft Cloud Services (such as Office 365;[1] and Microsoft Azure) to be an important IT modernization strategy for the Province.

This PIA will address the updates to the previous PIA (MTICS#16024 – Microsoft Cloud Services – Phase II) where government's continuous assessment cycle has demonstrated new information or direction.

During government's continuous assessment cycle for an implementation of the size and complexity of Microsoft's Office 365 suite of services, government has opted to shift away from consuming the ExpressRoute service discussed in MTICS#16024. It may be used for future implementations/services built on Microsoft Azure, but is not compatible with the use of Outlook Exchange or SharePoint. The reason for this shift is that due to the differences between Anycast and Unicast transmission,[2] and Microsoft's application of these different methods of transmission, ExpressRoute did not provide any additional assurances of a data sovereign route to Microsoft's Canadian datacentres for Outlook Exchange or SharePoint. As such, government needed to conduct additional analysis of the routing of data in the consumption of Microsoft's services. This analysis has been included in this PIA but does not fundamentally change the conclusions or outcomes otherwise reached in the previous PIA.

[1] Note that Office 365 will be used for all government email.

[2] For a more in depth understanding of the differences in routing using Unicast or Anycast, please refer to Microsoft materials online.

The analysis in this PIA speaks to the routing of data, but there have been no changes or impacts to the analysis on data at rest, which is located within the BC Government tenancy at Microsoft's Canadian datacentres, as discussed in the previous PIA (MTICS#16024).

s.21

2. **Scope of this PIA**

The scope of this PIA is centred on government's decision to pursue Microsoft's services without the use of ExpressRoute, as assessed in the previous PIA.

The PIA's scope is restricted to the assessment within the context of the BC government network.

3. **Related Privacy Impact Assessments, and Security Threat and Risk Assessments**

Microsoft Cloud Services – Phase II, PIA #MTICS16024

Microsoft Cloud Services (Conceptual PIA) – Phase I, PIA #MTICS15048

4. **Elements of Information or Data**

The data affected by the routing changes is the same data discussed in the previous PIA (MTICS#16024). It includes Customer Content, which was previously defined as the following:

- Customer content consists of data, information, documents, spreadsheets and other artefacts that are authored, edited, communicated, maintained and eventually disposed of by the client. For the purposes of analysis, customer content is assumed to be, or assumed to contain personal information.

- Specific content will range in type, volume and sensitivity according to the client activities in using Office 365 services. Customer content is not accessible or visible to Microsoft Cloud Services administrators, except in non-routine maintenance scenarios. In these cases Microsoft, with explicit consent from government, would be able to investigate and/or fix an ongoing problem with a cloud service through a service referred to as Customer Lockbox in Office 365 or the "Just in Time and Just Enough Access" service within the Azure fabric layer.[3]

Part 2 – Protection of Personal Information

5. **(a) Storage outside of Canada**

There is no storage of personal information during the routing of information between the Province and Microsoft.

5. **(b) Access outside of Canada**

There is no access outside of Canada contemplated as a part of this update. Given the importance of this issue, the following provides more fulsome details around the protections government will have in place with Microsoft in order to protect against unauthorized access outside of Canada.

[3] To access customer data, Microsoft employees must go through the Customer Lockbox tool. This tool uses a request and approval process to ensure that no Microsoft Engineer has access to customer data without their consent. Once approval is given to the Microsoft Engineer, the duration of time (up to four hours) required to complete the request or resolve the issue is provided.

Given the service provider relationship with Microsoft, the Province will be using the contract as one means through which the appropriate level of protection can be ensured for personal information. At base, the contract will reinforce the relationship that underpins the totality of services offered by Microsoft: Microsoft provides the physical storage of and processing power for any personal information government stores within the Office 365 system; however, once this space is established, Microsoft will relinquish any ability to access that information without cracking the encryption scheme applied to government's data. Any access Microsoft will have to Government's Customer Content will be provided through the BC Government–controlled Customer Lockbox.

The Province will include privacy provisions in the contract to ensure that personal information is protected from unauthorized collection, use and disclosure. These protections are established through various mechanisms to create a balanced, networked and integrated means of ensuring FOIPPA compliance.

The implications of these contractual provisions will be:

- The customer content belongs to the Province;
- The customer content is encrypted;
- The customer content is located in Canada;
- The contract is governed by the laws of British Columbia and Canada; and
- The contract specifies that, to the extent possible, the Province must be informed of any request for disclosure.

With the contract governed by Canadian law, the customer content belonging to the Province, the customer content being encrypted, and the customer content being located in Canada, the risk that personal information could be disclosed in response to a foreign demand without the Province being aware and able to challenge such a request would be low. This kind of request would require Microsoft to breach the contract, break the encryption keys, and break Canadian law on Canadian territory.

With respect to the use of the internet for transmission of encrypted data, government is satisfied that this information is not accessible, is not processed, and remains encrypted from end to end. Government has assessed this option to be sufficient in meeting its FOIPPA requirements regarding disclosure of, access to, and storage of personal information outside of Canada.

6. Data-linking Initiative*

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. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.

1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No

7. 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.

1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Office 365 General Authorities and Data Protections

Government access to Office 365 services begins at internet-enabled locations and ends at a Microsoft datacentre. Microsoft has committed to the fact that the Province's content will be used only to provide the Province with the Microsoft Online Services, including purposes compatible with providing those services. It should be noted that as a contracted service provider providing core IT services, Microsoft will be operating under the following authorities for collection and disclosure regarding the flow of personal information between Microsoft and the Province:

- s.26(c);
- s.33.2(c); and
- s.33.1(1)(p), where applicable.

In support of this, the conditions of these authorities will be explicitly provided as the only conditions under which Microsoft may collect/access personal information (i.e. the information relates directly to and is necessary for a program or activity of the Province), or under which the Province may disclose/provision access to personal information (e.g. the information is necessary for the performance of the duties of the [Microsoft] employee [as service provider to the Province]).

Although Microsoft has physical/technical custody of client-generated data, the technical infrastructure assessed in the Conceptual PIA (MTICS15048), the Security Threat and Risk Assessment (STRARS3262) and discussed at a high-level in Part 3 of this PIA substantiate that Microsoft can only access customer content through Customer Lockbox.

Personal Information Flow Table

	Description/Purpose	Type	FOIPPA Authority
1.	*Email created and sent.*	*Disclosure*	*33.2(c)*
2.	*Message is sent over TLS encrypted connections to Microsoft*	*Disclosure (by Province)* *Collection (by Microsoft)*	*33.2(c)* *26(c)*
3.	*Message processed: message header used to determine sender's Exchange server.*	*Use*	*32(a)*
4.	*Message is forwarded over TLS encrypted connections and delivered to appropriate tenant.*	*Disclosure*	*33.2(c)*

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
There are no additional risks found that were unique to this update, therefore the risks discussed in the previous PIA have been included below for fullness of reply.				
1.	*USA Freedom Act permits bodies under the Foreign Intelligence Surveillance Act (FISA) to issue a sealed order for access to an individual's data.*	*The USA Freedom Act has broader reasons for arguing against the order in court than the USA Patriot Act formerly contained, permitting Microsoft more latitude in fighting against requests for access to information. In all cases, Microsoft will attempt to reject and/or redirect a request for access (as they have been successfully able to do from 2014 until present). In cases where this is not successful, Microsoft will challenge such orders in court.* *If Microsoft was to lose all challenges and was required to obtain data from within Office365, Microsoft would need to write specific code (e.g. unencrypt the data) to override the Customer Lockbox system. It is anticipated that this would take Microsoft approximately 6 months, thereby reducing the attractiveness of using Microsoft as a source for information.* *If Microsoft was required to obtain data from the Azure PaaS/IaaS,[4] this would be encrypted data as government is the only one that can unencrypt the data held by Microsoft in these instances (due to the Bring-Your-Own-Keys protection measure where government holds the only encryption keys). The strength of encryption will be such that it significantly reduces the attractiveness of using Microsoft as a source for information.* *The Law Enforcement Access to Data Stored Abroad (LEADS) Act was introduced in February 2015 to a Congressional Committee. This Bill has been put forward by multi-national IT*	*Very Low*	*Variable*

[4] Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

		companies in order to reduce or eliminate extra-jurisdictional access requests to personal information and to increase transparency.		
2.	*Lack of governance relating to government data*	*Government will enforce or develop as necessary corporate policies, procedures and standards with respect to security and privacy (e.g. the Privacy Management and Accountability Policy).*	*Low*	*Variable*
3.	*Lack of identity and access management*	*Government will implement controls surrounding access by cloud provider employees as well as government employees (through the Customer Lockbox) and users of the government systems. Microsoft utilizes controls to manage employee access, such as their two-factor authentication and their internal Lockbox approval process, which grants specific permission to perform a specific change for a specified period of time.*	*Low*	*Variable*
4.	*Lack of infrastructure security*	*Microsoft will manage and provide ongoing maintenance of the network system and ensure the highest standard of application security including layered security controls and patch management. Microsoft will continually monitor and audit infrastructure security and integrity to ensure compliance with international standards, such as ISO 27018 and ISO 27001 among others.*	*Low*	*Variable*
5.	*Data security*	*All data will be encrypted during transmission between government and Microsoft. Data will also be encrypted while at rest in Microsoft's facilities.*	*Low*	*Variable*
6.	*Proper flow-through of privacy requirements from government to service provider.*	*Government will ensure that a contract with Microsoft supports compliance with FOIPPA.*	*Low*	*Variable*

10. Collection Notice

As Microsoft will not be collecting any personal information directly, they will not be providing collection notices. All collection of personal information will be done by the government programs opting to use Microsoft's services. It is the responsibility of these government programs to provide collection notices, as appropriate, to the individual from whom they collect personal information. As

such, there is no collection notice required here, as per section 27(3)(c) and 27(1)(b) of FOIPPA. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

Part 3 – Security of Personal Information

11. Physical and Technical Security Controls

All of Microsoft's relevant physical security measures and all of Azure and Office 365 technical security measures are addressed in PIA #MTICS15048, which includes details on Microsoft's approach for security, compliance and privacy with regards to physical measures, technical measures and security policy. Microsoft has constructed a multi-dimension approach that addresses security, compliance and privacy holistically through industry best-practices, default technology and operational procedures and policies as well as customer controls available for customization to the specific needs of the organization. Microsoft has committed to maintaining compliance certifications for global security standards.

It is of particular relevance to note here that data is secured using TLS encrypted connections during transit from BC Government users to the Microsoft datacentres.

12. Does your branch rely on security policies other than the Information Security Policy?

See #11 above

13. 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.

See #11 above

14. Please describe how you track who has access to the personal information.

See #11 above

Part 4 – Accuracy/Correction/Retention of Personal Information

15. 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 ministry notify them of the update, correction or annotation?

The updating and correction of personal information will be the responsibility of the government programs that are using Microsoft's services. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

There are no barriers within the Microsoft system that would preclude government from being able to correct, update or annotate personal information.

16. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Government programs using Microsoft's services may use the personal information resting on this system to make decisions that directly affect an individual. Given the scope and range of this initiative, it is likely that this will be the case. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

17. If you answered "yes" to question 18, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Government programs will be responsible for ensuring that the personal information stored on Microsoft's systems is accurate and complete. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

Microsoft can provide assurances that the accuracy and completeness of the data resting on their systems is not affected by data integrity issues, for which they would have responsibility. Microsoft will take all necessary, reasonable steps to aid the government in complying with its accuracy and completeness requirements.

18. If you answered "yes" to question 17, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Government programs will be responsible for ensuring that the personal information stored on Microsoft's systems is appropriately retained and destroyed. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

Microsoft can provide assurances that the data resting on their systems will not be retained beyond 90 days following contract termination or expiration. Microsoft will provide at least 90 days for administrators to confirm all data migrations have been completed, at which point the data will be destroyed to make it unrecoverable. Further, Microsoft provides guidelines to administrators to personally destroy data if that is the preferred approach.

Customer data is not destroyed without a specific request from government to do so. Microsoft will take all necessary, reasonable steps to aid the government in complying with its retention and disposition requirements.

Part 5 – Further Information

19. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Any government program using the data resting on Microsoft's services will be responsible for the required Information Sharing Agreements in the event that personal information is disclosed routinely or systematically. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

20. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

Any government program using the data resting on Microsoft's services will be responsible for the required Research Agreements in the event that personal information is disclosed for research or statistical purposes. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered.

21. Will a personal information bank (PIB) result from this initiative?

Any government program using the data resting on Microsoft's services will be responsible for providing the Privacy, Compliance and Training Branch with information on any Personal Information Banks, should they rest on Microsoft's services. This provision of information will occur as a standard step in the Privacy Impact Assessment Process that the government program will have to go through.

Part 6 – PCT Comments and Signatures

This PIA is based on a review of the material provided to PCT as of the date below. If, in future any substantive changes are made to the scope of this PIA, the ministry will have to complete a PIA Update and submit it to PCT.

Given this file's complexity and the strategic importance of the initiative itself, this PIA was submitted to the Office of the Information and Privacy Commissioner for BC (OIPC) for their review and comment. The resulting comment is attached as Appendix A (following the signatures pages).

Matt Reed		April 25, 2018
A/Executive Director Privacy, Compliance and Training Branch Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Derek Rutherford Executive Director Architecture, Standards and Planning Branch, OCIO Ministry of Citizens' Services	Signature	June 8, 2018 Date
Ken Prosser Ministry Contact Responsible for Security	Signature	March 27, 2018 Date
Ian Donaldson Assistant Deputy Minister or Designate	Signature	July 30/18 Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to PCT for its records to complete the process. PCT is the designated office of primary responsibility for PIAs under ARCS 293-60.

PCT will publish the ministry name, business contact details and a brief summary of the PIA to the Personal Information Directory (PID) as required by section 69(2) of FOIPPA. If you have any questions, please contact your privacy advisor at PCT or call the Privacy and Access Helpline at 250 356-1851.

Page 113

Withheld pursuant to/removed as

s.3