FOI Request:

I am requesting a summary of the Microsoft Cloud tools and programs used by each of the ministries/ crown corporations accountable to the Ministry of Finance

Summary Details on Request

**Note this table identifies organizations that are enabled to use certain Microsoft services. Organizations may or may not be using these services depending on their business requirements.*
***This table includes organizations that may not receive services from core Provincial Government IT departments. In those cases column C indicates "No" and The Ministry of Citizens' Services does not have responsive records on their use of Microsoft services.*
**Note* the sub-organizations listed below in orange cells are the specific non-ministry organizations that the applicant listed in their request per the usage of "viz" meaning, namily or or specifically. The did however list some of them as crown corporatations, which they are not.*

Breakdown Details of Applications

Government Organization Type	Sub-Organization Category	Receives MS apps from core government IT?	Exchange Online	OneDrive	SharePoint Online	Microsoft Teams	Office Online & Mobile	EOP	Intune	Planner	Sway	Yammer	OneNote	Stream	Whiteboard	Forms	Viva Connections	Viva Topics	Viva Learning	Viva Insights	Personal	Viva Insights - Manager/Leader AAD org data only	Viva Insights - Manager/Leader with 3rd party HR data only	Viva Insights - Advanced
Ministry	Advanced Education and Skills Training	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Agriculture and Food	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Attorney General	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Children and Family Development	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Citizens' Services	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No	No	No
Ministry	Education and Child Care	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Energy, Mines and Low Carbon Innovation	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Environment and Climate Change Strategy	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Finance	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Forests	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Health	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Indigenous Relations & Reconciliation	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Jobs, Economic Recovery and Innovation	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Labour	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Land, Water and Resource Stewardship	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Mental Health and Addictions	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Municipal Affairs	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Public Safety and Solicitor General and Emergency B.C.	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Social Development and Poverty Reduction	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Tourism, Arts, Culture and Sport	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Ministry	Transportation and Infrastructure	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	BC Assessment	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	BC Council for International Education	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Family Maintenance Agency	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Financial Services Authority	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Games Society	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Housing	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Hydro and Power Authority	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Infrastructure Benefits	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Oil and Gas Commission	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	BC Pavilion Corporation	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	BC Transit	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	British Columbia Lottery Corporation	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	British Columbia Securities Commission	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Columbia Basin Trust	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Columbia Power Corporation	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Community Living BC	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	Destination BC	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	First Peoples' Cultural Council	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Forest Enhancement Society of BC	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Forestry Innovation Investment	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Crown Corporation	InBC Investment Corp	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	Industry Training Authority	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Infrastructure BC	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Innovate BC	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Insurance Corporation of British Columbia	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Knowledge Network	No	No	No	No																			
Crown Corporation	Legal Aid BC	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Crown Corporation	Royal BC Museum	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Crown Corporation	Transportation Investment Corporation	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Legislative Assembly	Government House	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Independent Operating Agencies, Boards, Commissions and Tribunals	Liquor Distribution Branch	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Independent Operating Agencies, Boards, Commissions and Tribunals	Real Estate Foundation of BC	No	No	No	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Privacy Impact Assessment for

Microsoft Teams

PIA#CITZ20028

Why do I need to do a PIA?

Section 69 (5) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a ministry to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Section 69 (5.1) requires the head to submit the PIA to the minister responsible for FOIPPA for review, during the development of any new system, project, program or activity, or proposed enactment, or when making changes to an existing one. The Privacy, Compliance and Training Branch (PCT) is the representative of the Minister for these purposes. Ministries must submit PIAs to PCT at pia.intake@gov.bc.ca for review and comment prior to implementation of any initiative. If you have any questions, please call the Privacy and Access Helpline (250 356-1851) for a privacy advisor. Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?

Ministries still need to complete Part 1 of the PIA and submit it, along with the signatures pages, to PCT even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Ministry:	Ministry of Citizens' Services		
PIA Drafter:	Danielle Naylor		
Email:	Danielle.Naylor@gov.bc.ca	Phone:	778-698-5857
Program Manager:	Dwayne Robinson		
Email:	Dwayne.Robinson@gov.bc.ca	Phone:	778-974-5200

1. Description of the Initiative

Microsoft Teams (Teams) is a cloud-based, communication and collaboration application part of the Microsoft Office 365 suite available for desktop and mobile devices. The application features bring users together through chat, meetings, calling, and file sharing. Team users can have private, one-on-one chats or group chats through the instant message feature or open conversations within a team channel.

In Teams, users create teams by adding groups of people to channels built around a specific topic and/or department. When a user creates a team, the Teams application generates a general channel for that team. The channel is where users have conversations, share files, have meetings and add apps and services. When a user shares a file in the channel, it is stored in the SharePoint site for that team and is available in the "files" tab for quick access and collaboration amongst users. Office365 applications are built into Teams and users are able to access application such as, Word, Excel and PowerPoint, which allows users to collaborate using these applications without having to leave Teams platform. The meetings feature allows users to connect through audio or video using desktops, browsers, mobiles or meeting room devices. Meeting content can be shared through the digital white board, note taking or chat. Meetings can be recorded using the recording feature, which is stored in Microsoft Stream.

Meetings can also be transcribed in real-time to provide a closed captioning option or if the recoding feature is activated, transcriptions can be recorded and translated into one of the six languages currently available. Users with the Teams application on their mobile device may also enable the location sharing feature, which provides a user-controlled, point-in time capture of their location that can be shared to a channel or chat.

Teams users interact with this service through the Teams client and Web browsers. Teams voice and video traffic is transmitted using Secure Realtime Transport Protocol ("SRTP"). The real-time communications server software provides the infrastructure for enterprise instant messaging, presence, VoIP, ad hoc and structured conferences (audio, video and web conferencing) and public switched telephone network (PSTN) connectivity through a third-party gateway or SIP trunk.

Teams has a number of collaboration features such as online meetings with audio, video or web conferences for one-on-one, larger groups or live events involving attendees from inside and outside the organization. The Live Events component enables Office 365 users to produce and broadcast a meeting on the internet with up to 10,000 attendees, who can attend from a browser on virtually any device. With Live Events, users can host large virtual meeting such as webinars, all-hands meetings, and other one-to-many presentations.

Scheduling options allow the Province to limit attendance to people within the Government tenant or open it to external users. The call-in feature can be accessed via desktop workstations or include a global dial-in number so users can access the application from any mobile device. Users also can call anyone through Teams even though the other caller(s) may not be using the Teams application.

2. Scope of this PIA

This PIA will assess the collection, storage, access, and disclosure of information through the Teams application and does not include the assessment of any other Microsoft services that may integrate with or be accompanied by the use of Teams.

3. Related Privacy Impact Assessments

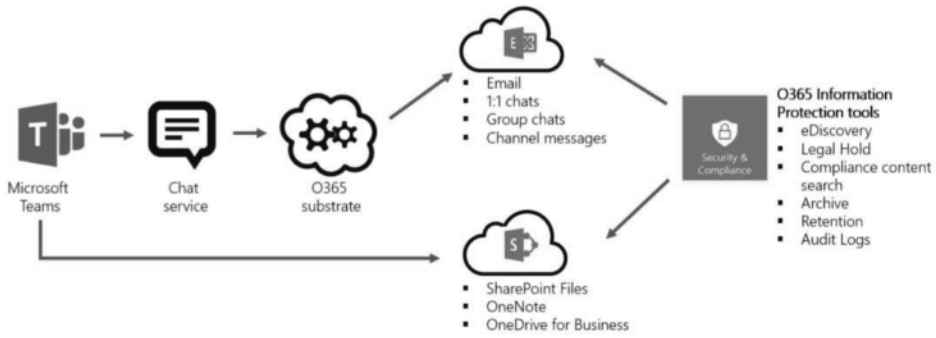
This PIA is built on the analysis within the Microsoft Cloud Service Phase II PIA (MTICS16024) and its predecessor, the Microsoft Cloud Services PIA (MTICS15048), which conceptually set out the high-level parameters of the Microsoft IaaS and PaaS offerings.

4. Elements of Information or Data

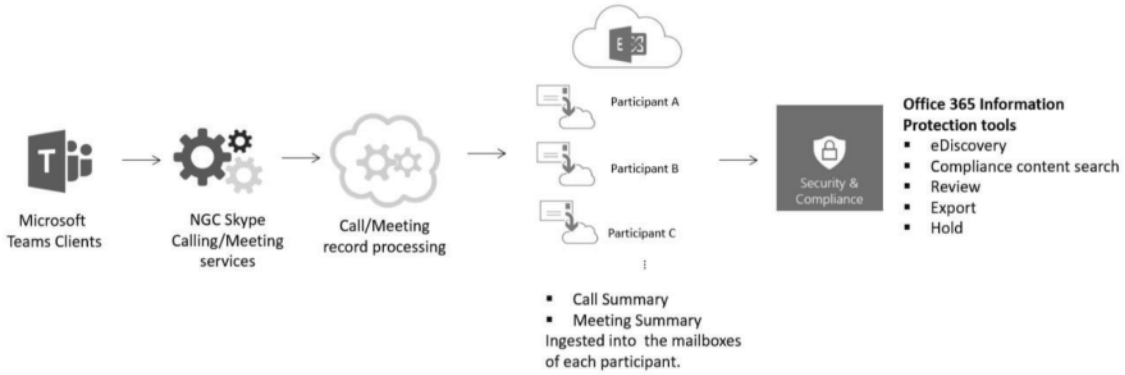
Different categories of data are treated differently with respect to storage and access. This PIA relies on the same data categories as the conceptual PIAs listed above: system data; employee contact data; and client-generated data, or customer content.

Specific to Teams, it is anticipated that broad categories of personal information may be included on Teams. The majority of the conversations that will take place on Teams will be transactional, team-based conversation that will include elements of personal information. In addition to transactional, team-based conversations, personal information may result from communication with and about clients, citizens and contracted service providers and, as a result of using it, as a venue for service delivery to the residents of BC. For clarity, this PIA does not assess the authority to collect program-specific personal information, but it does assess using Teams as a platform for communicating about it.

The following figure indicates the ingestion flow of Teams data to both Exchange and SharePoint for Teams Files and Messages.



The following figure indicates the ingestion flow of Teams Meetings and calling data to Exchange.



Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Microsoft's Canadian datacentres are located in Quebec City and Toronto. These facilities are designed to run 24x7x365 and employ a variety of measures to minimize the possibility of power failures, physical intrusions and network outages. Data is replicated three times within the primary datacentre with a fourth copy provided from the secondary Canadian datacentre.

Across its business, Microsoft stores Customer Data at rest within certain major geographic areas (a "GEO"). Canada has been defined as a "GEO", meaning that for government's purposes, all customer content will be resident within the Canadian GEO. Data processing of specific Teams features (e.g. live captioning and translation services) occur outside of Canada and are completed in accordance with the conditions of FOIPPA s.33.1(1)(p.1). However, the information is stored within the Canadian datacentres via Microsoft Stream and the processing occurs electronically, for the limited amount of time necessary and is not intentionally accessed by an individual.

All personal information will be held within Microsoft's Canadian datacentres and will not be accessible outside of Canada unless explicitly permitted by the customer using mechanisms such as the Office 365 Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with customer consent, effect temporary movement to another geo-location to ensure customer services and data are not lost.

Microsoft may also access customer content for the purposes of technical maintenance or support on a technical basis as authorized by FOIPPA s.33.1(1)(p). The contract with Microsoft has terms that outline requirements related to technical maintenance by requiring access, disclosure and storage of information only for the purpose of supporting (e.g. repairing or troubleshooting) an electronic system or for data recovery following the failure of an electronic system. Such access and storage will be temporary, for the minimal amount of time necessary and will only occur after a system has failed.

The contract also has terms to mitigate risk related to data sovereignty in that Microsoft will not disclose the Province's information to a third party (law enforcement or other agency/party) unless required by law. If a third-party contacts Microsoft with a demand for the Province's information, Microsoft will attempt to redirect the third party to request that data directly from Province. Furthermore, if Microsoft is compelled to disclose the Province's information to law enforcement, it will promptly notify the Province and provide a copy of the demand unless legally prohibited from doing so.

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
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

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);	no
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;	no
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

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
General Admin	*User information is imported into AzureAD (ADD) from Active Directory (AD)*	*Collection*	*26(c), 27(1)(b)*
	Government is disclosing Active Directory (AD) elements to AzureAD	*Disclosure*	*N/A – disclosure is of business contact information only*
	Free/busy calendar info (point in time only, not stored)	*Collection*	*26(c), 27(1)(b)*
	User (opts to) upload photo for purposes of employee/workplace engagement and familiarity	*Collection and Disclosure*	*26(c)* *33.2(a)/(c)*
	Teams collects information from users indirectly: • *When a user is not at their computer for x # of minutes,* • *When a user does not want to be disturbed,* • *When a user is adding their contact information that is specific (e.g. adding a note to their status to say "I'm on the third floor").* • *When a user types in a status note.*	*Indirect Collection* *Disclosure*	*26(c); 27(1)(a)(i)* *33.2(a)/(c)*
	Teams users search the AAD directory and add other users to their contacts list.	*Use*	*32(a)*
	Teams users add external (outside of BC Gov't) contacts and uses Teams to communicate with external contacts.	*Collection* *Disclosure*	*26 (c)* *33.2(a)*

	Users activity logs are created when users communicate with each other using Teams.	*Collection*	*26(c)*
	Teams users may share information in Online meetings.	*Disclosure*	*Only when authorized to do so under section 33.1 or 33.2 of FOIPPA.* *Disclosures of personal information beyond that assessed in this PIA will need to be assessed in program-specific PIAs.*
	Teams users are added to the team by the owner (internal gov't employee).	*Collection* *Use* *Disclosure*	*26(c)* *32(a)* *33.2(a)/(c)*
	Files are shared via channels, instant messaging/chat, video and/or audio calling, and other communication mechanisms in Teams.	*Disclosure*	*33.2(a)/(c)*
	Teams users access Exchange calendar.	*Collection* *Disclosure*	*26(c)* *33.2(a)/(c)*
	Team users access personal OneDrive data.	*Collection*	*26(c)*
	Microsoft Engineer accesses customer content for the purpose of remedying a technical issue.	*Disclosure*	*33.1(1)(p)*
	Teams logs and other data are stored on the Province's tenancy within Office365.	*Disclosure (by Province)*	*33.2(c)*
Messaging	*Teams users share information via instant message/chat (persistent).*	*Disclosure*	*33.2(a)/(c)*
	Team user adds user to persistent chat and provides access to full and/or partial chat history.	*Disclosure*	*33.2(a)/(c)*
Calling	*Teams users share information via video/audio calls.*	*Disclosure*	*33.2(a)/(c)*

	Meeting organizer records meeting by using the recording feature.	*Collection* *Disclosure*	*26(c)* *33.1(1)(p.1)*
	Meeting organizer activates live captioning feature (not saved for user access at a later date).	*Disclosure*	*33.1(1)(p.1)* *33.2(a)/(c)*
	Meeting organizer activates live captioning and meeting recording feature to generate meeting transcript which is saved to the MS Stream and posted in the team channel.	*Collection and Disclosure*	*26(c)* *33.1(1)(p.1)* *33.2(a)/(c)*
Channels	*Teams users share information via general and private channels.*	*Disclosure*	*33.2(a)/(c)*
	Teams users upload and share files and documents via channels for real-time editing.	*Disclosure*	*33.2(a)/(c)*

Note: All disclosures by Province and collections by Microsoft are of encrypted data only.

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Users may add external parties to team channels.*	*The Teams admins will create the new Teams that are requested and approved by the program areas. The new Team Owner is responsible for adding/removing Team members.* *If the Teams is open to external parties (e.g. individuals not internal to government), the Team admins will include "external" in the team name so team members are aware of the presence of external parties.*	*High*	*Low*
2.	*When a team is created, there is also an Office 365*	*As of April 16, 2020, Teams are generated via service request through Service Now.*	*Medium*	*High*

	Group and the associated SharePoint document library and OneNote notebook, along with ties into other Office 365 cloud applications. If not managed, there could be hundreds of SharePoint team sites, and other resources, that administrators have no idea exist.	*When a service request is received, Team admins create the team for requestor (e.g. the team Owner).* *Team admins are able to create retention policies that manage Teams. The Microsoft Online Service Committee (MOSC) within the OCIO will be responsible for the governance of Teams and determining and implementing retention policies.*		
3.	*Records management of documents may be challenging as files in Teams are stored on SharePoint rather than the LAN.*	*Program areas are responsible for retaining records and/or deleting transitory records in Teams in accordance with the relevant record schedules.* *Team admins are able to create retention policies that apply to OneDrive for Business and SharePoint Online. Retention Policies can be set at the Office 365 admin console for the storage settings in SharePoint and OneDrive and for the chat settings within Team. It is noted, however, that no retention policies are currently in place as of April 16th, 2020 but OCIO is working with Government Records Services (GRS) on a records policy.*	*Medium*	*Low*
4.	*Specific content will range in type, volume and sensitivity according to the client activities in using Office 365 services.*	*Although the primary purpose of MS Teams is not meant for storing or transferring Personal Information or highly confidential material, the platform is sufficiently secure to manage this type of information. GRS has developed a records management guidance document for user awareness and the OCIO posted privacy and security page via the O356 Portal to ensure users are aware of information security and the applicable information management policies when*	*High*	*Medium*

		using Teams. It is incumbent on each team administrator to ensure diligence on an ongoing basis around adding and removing individuals from teams when access needs to be updated.		
5.	*A program area may share sensitive information, without the appropriate security controls set on the channels and for sharing of information.*	*Each program area must assess their use case to determine suitability given the current implementation and adjust security and privacy configurations available to team owners and meeting organizers for the expected data sensitivity in use by their Team.* *If a program area has a requirement for a Team to share sensitive information, then the security controls set on the channels and for sharing of files or information must be strengthened accordingly.*	*Medium*	*High*
6.	*Employees that have registered for the Microsoft Office 365 Personal Use Program and sign into an office product on their personal computer could access government information on Teams from their personal computer.*	*The OCIO is in the process of updating the Microsoft Office 365 Personal Use Program website and user guide outlining the appropriate settings for users. The OCIO will also send a communication to all government employees advising them of the appropriate use for the Personal Use Program and the applicable policies.* *The OCIO will review the conditional access configurations available in the tenancy and implement a conditional access solution once one is identified and tested.*	*Medium*	*High*
7.	*Microsoft may need access to customer content outside Canada for purposes of temporary maintenance.*	*Services are consumed out of Canadian data centre; however, if Microsoft is required to access the Province's Office 365 tenancy for support purposes (i.e. technical maintenance), they are provided with "Just in Time" access that must go through the appropriate approval process*	*Low*	*Low*

		via Customer Lockbox and is in control of the Province. *The contract with Microsoft has terms that outline requirements related to technical maintenance by requiring access, disclosure and storage of information only for the purpose of supporting (e.g. repairing or troubleshooting) an electronic system or for data recovery following the failure of an electronic system. Such access and storage will be temporary, for the minimal amount of time necessary and will only occur after a system has failed.*		
8.	*Microsoft is compelled to disclose Customer Data without notifying the Province (e.g. in response to a Foreign Demand for Disclosure).*	*Microsoft does not have standing access to the Province's information and must request and be granted access to the data via Customer Lockbox. Note: Due to the conflict of laws between BC and the USA Microsoft could receive an order from the US government to unencrypt and disclose data and to do so without the customer's knowledge or consent. This risk is adequately mitigated as there are contractual obligations to notify the Province should it received a foreign demand for disclosure and take reasonable steps to contest the request.* *The contract includes terms on Foreign Demand for Disclosure, including on how Microsoft will not disclose the Province's information unless required by law and will redirect the request directly to the Province. Furthermore, Microsoft will promptly notify the Province of any such requests unless prohibited from doing so by law.*	*Low*	*High*

9.	*Service providers need to meet contract terms as negotiated between the Province and Microsoft.*	*Teams is an O365 application which is a Microsoft SaaS service and is included in the contract between the Province and Microsoft.* *The contract notes that any service providers (e.g. subcontractors) must comply with the provisions of the privacy protection schedule and will not disclose personal information inside or outside Canada unless authorized to do so.*	*Low*	*Low*
10.	*Emails and/or phone numbers of all invitees may be exposed to each other in meetings.*	*In instances where this would not be an acceptable disclosure, this tool won't be used and another means of connecting individuals would be used.*	*High*	*Medium*

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

At a conceptual level, the Microsoft Cloud Service Phase II PIA (MTICS16024) and its predecessor, the Microsoft Cloud Services PIA (MTICS15048) discussed 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 default technology and operational procedures and policies as well as customer controls available for customization to the specific needs of the organization.

11. **Please describe the physical security measures related to the initiative (if applicable).**

Microsoft's Canadian datacentres in Quebec City and Toronto are designed to run 24x7x365 and employ a variety of measures to minimize the possibility of power failures, physical intrusions and

network outages. Data is replicated three times within the primary datacentre with a fourth copy provided from the secondary Canadian datacentre. Defense includes:

- Multi-factor authentication, including biometric scanning for datacenter access. Internal datacenter network is segregated from the external network.
- Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
- Faulty drives and hardware are demagnetized and destroyed.
- Defense-in-depth security that includes perimeter fencing, video cameras, security personnel, secure entrances, and real-time communications networks.

12. Please describe the technical security measures related to the initiative (if applicable).

Microsoft provides encryption of data in transit and at rest and Microsoft encryption uses industry standard technologies. Files are stored in SharePoint and are backed by SharePoint encryption. Notes are stored in OneNote and are backed by OneNote encryption.

Teams Administrators are internal employees from Network, Communications and Collaborations Services (NCCS) within the OCIO that have access to the Teams Admin Console. Adding users to a role requires management approval at the Global Administrator level and for Teams Administrators to enable it.

Microsoft personnel do not have standing access to any service operation ("zero standing permission"). All access is obtained through an access control technology called Lockbox. Lockbox enforces access control through multiple levels of approval in order to provide "just-in-time" access with limited and time-bound authorization ("Just-In-Time access and elevation"). All access control activities in the service are logged and audited. The Province has complemented this capability with "Customer Lockbox" which injects the Province's administrator into the lockbox approval process.

Customer Lockbox ensures that Microsoft cannot access customer data to perform a service operation without explicit approval from the Customer. For the Province, only specific internal employees in a technical role have an E5 licence with Customer Lockbox and have the ability to provide Microsoft with access to the Province's data. However, this is the final step in the approval workflow and can only be utilized once all other options have been exhausted to troubleshoot and fix issues reported by the Province.

Customer Lockbox follows a workflow and a Microsoft engineer must submit a data access request that includes the organizations tenant name, service request number and estimated time required to fix the issue (e.g. time frame the access will be granted and is automatically revoked at the expiry). This request is then sent to and either approved or denied by the Global Administrator. Global Administrators employees internal to government and there currently are two individuals designated as Global Administrators within the OCIO. If the request for access is

rejected or is not approved within 12 hours, the request expires and not access is granted to the Microsoft engineer.

Audit records that correspond to the Customer Lockbox requests are logged in the Office 365 audit log. The logs can be accessed by using the audit log search tool in the Office 365 Security and Compliance Center. Actions related to accepting or denying a Customer Lockbox request and actions performed by Microsoft engineers (when access requests are approved) are also logged in the Office 365 audit log.

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

All service provider obligations for privacy, security and confidentiality are described in the contract between Microsoft and the Province (which includes both privacy and cloud security schedules).

14. 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.

There are a number of access controls in Teams at the user (e.g. employee), owner (e.g. branch or division management) and administrator levels (the OCIO). A user can control the information that they add to a chat conversation or team channel. Owners that create a team can add and remove users to specific channels and has control over specific settings to that Team.

The Teams admin centre allows administrators to manage users, usages, settings and manage external access, guest access, resource accounts, email integration, cloud storage options and device set up, turn off and configure workloads. Team administrators can set policies for the application; however, the specific policy configurations for Teams is currently being assessed. In the interim, teams are only created via service request through Service Now. When a requestor (e.g. a Team Owner) submits a request for a new team, they are required to provide information in the service request such as team name, whether the team will include external applicants and the name of back-up owner.

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

Within Teams, audit functions can be set at the console level for application-specific audit capabilities; however, the overall audit functions are part of the Office 365 service. The Global Administrators have access to the Office 365 Security and Compliance portal and the Teams admin portal to configure the organization wide security settings. Access to audit functions are currently available to Global Administrators within the OCIO as the audit capabilities are granular and access to audit logs are not available to other administrators unless they are expressly provided by Global Administrators for authorized purposes.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. 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.

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

Given the function that Teams serves, it is unlikely and not expected that decisions about an individual will be made on this platform or with its information, however, if decisions are made, records will be retained in accordance with records management obligations.

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

Given the function that Teams serves, it is unlikely and not expected that decisions about an individual will be made on this platform or with its information, however, if decisions are made, records will be retained in accordance with records management obligations.

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. Microsoft will take all necessary, reasonable steps to aid the government in complying with its accuracy and completeness requirements. The contract with Microsoft has terms that outline requirements related to accuracy and completeness by requiring Microsoft to make every reasonable effort to ensure the accuracy and completeness of any personal information used by the Province to make a decision that directly affects the individual the information is about including correcting and/or annotating any information within five business of receiving a written request from the Province to do so.

19. 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?

Given the function that Teams serves, it is unlikely and not expected that decisions about an individual will be made on this platform or with its information, however, if decisions are made, records will be retained in accordance with records management obligations.

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

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

No. However, 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 regularly and systematically. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered. Given the function that Teams serves, it is not anticipated that ISAs will be required.

21. 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.

Given the function that Teams serves, it is unlikely and not expected that Research Agreements will be required.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact a PCT advisor.	

22. 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 program area will complete.

Given the function that Teams serves, it is unlikely and not expected that any PIBs will be created or stored there.

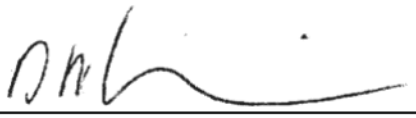
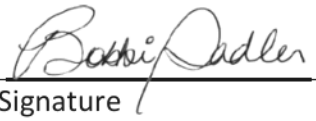
Part 6 – PCT Comments and Signatures

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.

Danielle Naylor		July 31, 2020
Manager Privacy, Compliance and Training Branch Ministry of Citizens' Services	Signature	Date

Keleigh Annau		August 6, 2020
Director Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

Dwayne Robinson		August 26, 2020
Executive Director Network, Communications and Collaboration Services OCIO Enterprise Services	Signature	Date
Garry Mierzuak		August 14, 2020
Ministry Information Security Officer Information Management Branch Corporate Services Division	Signature	Date
Bobbi Sadler		September 2, 2020
Assistant Deputy Minister Procurement and Supply Division Responsible for Enterprise Services Office of the Chief Information Officer	Signature	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.

Appendix A – Microsoft Azure Corporate PIA Checklist

What is Microsoft Azure?

Microsoft Azure is a cloud computing infrastructure and platform for building, deploying and managing applications and services through Microsoft-managed data centres. It provides both Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) services.

IaaS: Infrastructure is the lower layer in the technology stack and is responsible for the important back-end components like servers and storage, networking, security, and data centres. Traditionally, these would be the responsibility of an organization to be managed in house. IaaS gives organizations the option of having a vendor (e.g. Microsoft) provide and manage these things on their end such that organizations do not have to operate this on their own. Azure's IaaS offering has three components: Compute (computing power), Storage (data storage) and Networking (network traffic distribution). With Azure IaaS, the Province can access the amount of computing, storage and networking power needed to suit their needs and scale up or down as required. From there, ministries can take this infrastructure and build on it.

PaaS: Using PaaS, organizations can create and develop services of their own on an existing platform which users can build and run their own software. The goal of PaaS is to help create an application quickly without managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don't have to install an operating system, web server or even system updates.

Azure is available in various regions around the world, including two in Canada. Azure clients can specify where the data at rest will be stored and Microsoft will not store that customer's data outside the "geo" specified by the client except in limited circumstances (e.g. temporary technical support).

The scope of this PIA will cover the Province's use of Azure through Microsoft's Canadian data centres.

Next Steps for Program Areas Using Azure

Province/Microsoft Agreement

In order to enable use of Microsoft Azure services, the Province has signed an amended Microsoft Business and Service Agreement. For Ministries to use Azure leveraging this agreement with Microsoft, specific compliance provisions have been identified in this corporate PIA that program areas will be responsible for adhering to, or in some instances, completing on their own, in a separate Program Privacy Impact Assessment (Program PIA) to be completed and submitting to the Privacy, Compliance and Training Branch.

Corporate Privacy Impact Assessment for *Microsoft Azure Cloud Services*

PIA# CITZ20038 (Appendix A)

For illustrative purposes, details of the requirements to be included in the Program PIA are outlined below:

Microsoft Azure Program PIA Checklist			
Q.	**Topic**	**Requirement**	✓
Part 1 – General			
Q1	Description of the Initiative	• Complete specific details of the initiative • Include whether you are deploying IaaS or PaaS	
Q2.	Scope of this PIA	• Indicate here that you are leveraging this Azure Corporate PIA • Complete specific details on the scope of the Program PIA	
Q3.	Related PIAs	• List this Azure Corporate PIA here (PIA # CITZ20038) and any other related PIAs	
Q4.	Elements of Information of Data	• List detail and description of the data elements specific to your initiative	
Part 2 – Protection of Personal Information			
Q5.	Storage or Access Outside Canada	**Azure Services** • All services where personal information is involved must be deployed in the Canadian region [1]. • List any Azure services, *excluding Azure Active Directory* or *Azure Security Center* that are not deployed in the Canadian region (either other geographical regions or non-regional)[2] with a description of its use and the data elements involved (including verifying that no personal information will be included OR that your program area has a disclosure authority for outside of Canada). **Routing** • Refer to MISO for determination on routing option (refer Corp PIA page 10) based on a combination of business need and security requirements.	

[1] A list of services available in the Canadian Geographic Region: https://azure.microsoft.com/en-us/global-infrastructure/services/?regions=canada-central,canada-east&products=all

[2] A list of services and their associated regions can be found here (click on "select all products"): https://azure.microsoft.com/en-us/global-infrastructure/services/?products=all

		Access Temporary Processing: • Indicate if it is known that any of the conditions (refer Corp PIA page 11) for use of Temporary Processing of personal information outside of Canada (within the Canadian region) are not met. **Access Controls: Barriers to Access** Indicate whether additional access controls are implemented including rationale (refer Corp PIA page 12). Customer Lockbox: • To strengthen your access controls, Customer Lockbox is available, in public preview, for a limited number of Azure services (Azure Storage, Azure SQL DB, Azure Data Explorer, Virtual Machines, Azure subscription transfers). Details that must be followed to enable its service is located in Corp PIA (page 12). Key Vault (Bring-Your-Own-Keys): • To strengthen transparency of access to your data, Key Vault may be enabled. To enable logs, appropriate configuration of Key Vault must be completed (refer MISO or Security as a first point of contact for this). **Authentication** • Indicate details on which authentication method(s) are being used in your initiative (e.g. Active Directory, Azure Active Directory, Multi-Factor Authentication (MFA), Hybrid AAD Join – refer Corp PIA page 15). *Note: Personal information cannot be used as attributes in Azure Active Directory or MFA.* • If MFA is being used, confirm second factors are USB token, smartphone app or have been assessed separately in the Program PIA.	
Q6.	Data-linking Initiative	• Complete detail specific to your initiative	
Q7.	Common or Integrated Program		
Q8.	PI Flow Table		

Q9.	Risk Mitigation Table	• Complete detail specific to your initiative **Executive Communication** • It is important that the risks included in the Corp PIA (in particular, access controls on page 11 and foreign demand risks on page 14) are communicated and understood by the program area's executive in order for them to make an informed decision on accepting the risks outlined in the risk mitigation table. Document in Program PIA that executive communication has been completed.	
Q10.	Collection Notice	• Complete detail specific to your initiative	
Part 3 – Security of Personal Information			
Q11.	Physical Security	• Complete if there is any additional detail specific to your initiative (refer to MISO)	
Q12.	Technical Security		
Q13.	Other Security Policies		
Q14.	Access Controls		
Q15.	Tracking Access to PI		
Part 4 – Accuracy/Correction/Retention of Personal Information			
Q16.	Updating / Correcting Information	• Complete detail specific to your initiative	
Q17.	PI used to make decisions on individuals		
Q18.	Accurate and Complete		
Q19.	Records Retention and Disposition		
Part 5 – Further Information			
Q20.	Systematic Disclosure PI	• Complete detail specific to your initiative	
Q21.	Research or Statistical Purpose		
Q22.	Personal Information Bank		

Corporate Privacy Impact Assessment for *Microsoft Azure Cloud Services*

PIA# CITZ20038

Part 1 – General

PIA Drafter:	Chris Quon		
Email:	Chris.Quon@gov.bc.ca	Phone:	778-698-5841
Program Manager:	Stephen Gidden		
Email:	Stephen.Gidden@gov.bc.ca	Phone:	250-415-0340

1. Description of the Initiative

The government of British Columbia is moving forward with the adoption of Microsoft Cloud Services (Microsoft Azure, Microsoft Office 365 and Microsoft Dynamics CRM) with an in-Canada data residency option for the delivery of IT services to the BC public service.

When using Microsoft's Cloud Services, government remains the sole owner of our 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.

When talking about cloud computing, there are three major categories that are important to understand. They are described here in more detail[1]:

1. Infrastructure-as-a-Service (IaaS):
Infrastructure is the lower layer in the technology stack and is responsible for the important back-end things like servers and storage, networking, security, and data centres. Traditionally, these would be the responsibility of an organization to be managed in house. IaaS gives organizations the option of having a vendor (e.g. Microsoft) provide and manage these things on their end as opposed to having to operate this on their own. Azure's IaaS offering has three components: Compute (computing power), Storage (data storage) and Networking (network traffic distribution). With Azure IaaS, the Province can access the amount of computing, storage and networking power needed to suit their needs and scale up or down as required. From there, ministries can take this infrastructure and build on it.

2. Platform-as-a-Service (PaaS):
Using PaaS, organizations can create and develop services of their own on an existing platform which users can build and run their own software. The goal of PaaS is to help create an application quickly without managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don't have to install an operating system, web server or even system updates.

[1] https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/5-types-of-cloud-services

3. Software-as-a-Service (SaaS):

SaaS is software that is centrally hosted and managed for the end customer. It is usually based on an architecture where one version of the application is used for all customers and licensed through a monthly or annual subscription.

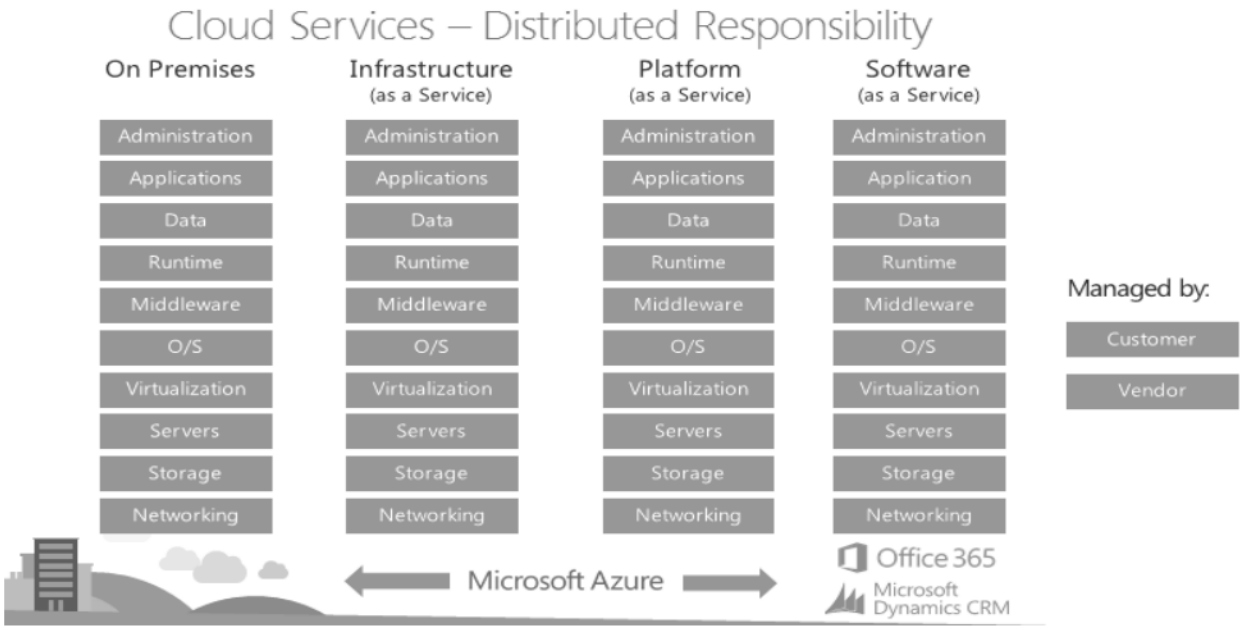
IaaS vs PaaS vs SaaS: Using an example of creating an app for a business illustrates the relationship between the 3 categories. The IaaS product is the infrastructure and would host the app. The PaaS product would be the platform that developers can use to build and custom design the app. Once the app is finished, it could be considered a SaaS if it was then to provide a service for its users.

Shared Responsibility Model

Shared responsibility in the cloud comes with hosting resources on a cloud service provider's infrastructure. Responsibility for each aspect of security depends on which cloud service model is used (IaaS/PaaS/SaaS). With Azure IaaS, Microsoft, the cloud service provider, is responsible for the core infrastructure security, which includes compute, storage and networking, at the underlying base operating level (the physical level).

It is also important to understand that these categories layer on top of each other. As customers move from IaaS to PaaS and then to SaaS, the Province (as the customer) becomes responsible for less and the cloud service provider is responsible for more.

The figure below describes how shared responsibility works across the cloud service model where the Cloud Customer is the Province ("Customer" in blue) and the Cloud Provider is Microsoft ("Vendor" in green).



- IaaS requires the most user management of all the cloud services. The user is responsible for managing the operating systems, data, and applications.
- PaaS requires less user management. The cloud provider manages the operating systems, and the user is responsible for the applications and data they run and store.
- SaaS requires the least amount of management. The cloud provider is responsible for managing everything, and the end user just uses the software.

Microsoft Cloud Services' portfolio consists of three basic offerings: Microsoft Azure (IaaS and PaaS), Office 365 (SaaS - Email, Document Authoring & Collaboration, VOIP services), and Microsoft Dynamics CRM (SaaS - CRM/Case, HR and Financial Management). These state-of-the-market information technology offerings will provide government with a strategic opportunity to achieve better outcomes for the province through:

- Industrial Grade Security;
- Greater Agility and Service Modernization; and
- Lower Costs through Shared Infrastructure and Converged Communications Technologies.

Microsoft Azure

The scope of this PIA is centred on Microsoft Azure (IaaS and PaaS), which is a cloud computing platform and infrastructure for building, deploying, and managing applications and services through Microsoft-managed data centres.

Office 365 (SaaS) and Microsoft Dynamics CRM (SaaS) will be covered in separate PIAs.

When using Azure (IaaS), the shared responsibility means that while the cloud provider (Microsoft) is responsible for ensuring the cloud infrastructure is functioning correctly, equally important is that the cloud customer (Province) is responsible for ensuring the service they are using is configured correctly, is up-to-date and is available.

A key premise to note is that the customer controls and owns their content, Microsoft has zero standing access to the service components that the government is responsible for. The service provider only interacts with customer data under exceptional circumstances for the purpose of providing support services when a problem cannot be self-remedied by the customer's own IT or in-house support teams (and as authorized under FOIPPA s. 33.1(1)(p)).

Microsoft's introduction of public cloud services to the Canadian market in 2016 is a significant opportunity for the BC public sector. These in-Canada services will provide services that meet international security and privacy certifications such as ISO 27001, ISO 27018, PCI, SOC1 and SOC2. This level of compliance coupled with a regular schedule of audits and attestations, results in a suite of in-Canada IT services capable of meeting or exceeding the BC government's privacy and security requirements.

2. Scope of this PIA

The scope of this PIA will cover the government use of Microsoft Azure, including Microsoft Azure Infrastructure as a Service (IaaS) and Microsoft Azure Platform as a Service (PaaS), through data resident Canadian data centres.

Note that Office 365 and Microsoft Dynamics CRM are Software as a Service (SaaS) products and while they are hosted on Azure, will be covered in separate PIAs.

The intention of this PIA is to establish that the foundational infrastructure and platforms of Azure on which government programs will develop are compliant with BC's Freedom of Information and Protection of Privacy Act (FOIPPA).

Government programs that are built on Microsoft Azure, both IaaS and PaaS, will still be required to conduct a separate PIA that addresses their specific programs (Program PIA). Refer Appendix A - Microsoft Azure Corporate PIA Checklist for more details.

It should be noted that the Azure portfolio serves as a foundation both for itself and in support of Microsoft's SaaS offerings, such as Office 365 and Microsoft Dynamics CRM. Therefore, the privacy and security provisions of Azure can be applied to an analysis of Office 365 and Microsoft Dynamics CRM. At the next level, Office 365 builds on top of the international standards-based security foundation provided by Azure, with additional controls (like the Customer Lockbox) which are designed to maximize security and ensure privacy of user content. Refer diagram and descriptions above under Shared Responsibility Model for a visual representation of the responsibilities associated with each of Microsoft's services.

3. Related Privacy Impact Assessments

This PIA is built on the analysis within the Microsoft Cloud Services PIAs listed below, which conceptually set out the high-level parameters of the Microsoft IaaS and PaaS offerings.

MTICS15048 – Microsoft Cloud Services

- Conceptual PIA centered on the exploration of Microsoft Cloud Services

MTICS16024 – Microsoft Cloud Services - Phase II

- Addresses the Microsoft Service offerings within the context of the BC government network

CITZ17025 – Microsoft Cloud Services – Update

- PIA Update that addresses routing (BC Government's use of Microsoft's services without the use of ExpressRoute)

CITZ18047 – IDIR Multi-Factor Authentication Service

- Examines the collection, storage, access, use and disclosure or information for the IDIR MFA Service

4. Elements of Information or Data

Regardless of the government programs that are built on Microsoft Cloud Services, including Infrastructure-as-a-Service and Platform-as-a-Service, Microsoft will hold 3 basic categories of data, which consist of: 1. Service or System Data; 2. Employee Contact Data; and 3. Customer Content. Basic definitions of the three data types follow:

NOTE: For the purposes of this PIA, Service or System data and Employee Contact Data contain no personal information while Customer Content does. Any data that is not considered Customer Content but might reveal personal information or is determined to be personal information by the mosaic effect, Microsoft is contractually obligated to treat such data as they would Customer Content (e.g. when at rest, it will be stored in Canada).

From the Province/Microsoft contract:

"As between the parties, Customer retains all right, title and interest in and to Customer Data…. Personal information contained within log records or telemetry data or metadata of any kind will be stored, protected and used by Microsoft only in the same manner as Customer Data. To the extent information is derived by Microsoft and includes personal information and such personal information is not Customer Data, such personal information will be stored, protected and used by Microsoft only, and be accessible to Customer, in the same manner as Customer Data under the applicable Enrollment and these Online Services Terms."

Service or System Data

- System or Service Data is data about, and generated by, an information system or cloud service. Typical examples of service data include: remaining storage capacity, system health indicators, network traffic volume, bandwidth consumption, all of which are examined or used solely for the purpose of providing the cloud service. System data is not personal information and is distinct from user generated content. System data is used solely for the purpose of providing, operating and maintaining the service, or diagnosing and/or troubleshooting in the event of problems or system outages.

- This non-personal data is accessed by authenticated system administrators, service technicians and operators with the appropriate and minimized levels of access. As a rule, technicians are granted just-in-time[2] minimum privileges necessary to troubleshoot the system on an exceptional basis, and only for a fixed period of time. Upon completion of any maintenance task, administrative privileges and access to service data are revoked, and all associated data around these activities are logged.

[2] "Just-In-Time (JIT) access and elevation" refers to Microsoft's policy that limits staff access based on the actual time required to address an identified problem at a specified time.

- Object metadata is information provided by the customer or on the customer's behalf that is used to identify or configure Online Service resources, such as software, systems, or containers, but does not include their content (Customer Content) or user identities (Employee Contact Data). Examples of object metadata include the names and technical settings of Azure Storage accounts, Virtual Machines, SQL Databases and their tables, column headings, and forms. Customers should not include personal data or other sensitive information in object metadata because object metadata may be shared across global Microsoft systems to facilitate operations and troubleshooting. Any metadata that could be characterized as personal information would be treated as customer content as per the contract terms above.

Employee Contact Data

Employee Contact Data is basic information used to identify or differentiate users within the cloud service. Examples include User ID, Organizational ID and basic user contact information such as phone number or email address. This information is used by Microsoft staff in order to troubleshoot service and an employee's access (e.g. jsmith cannot access file A).

The vast majority of Employee Contact Data is considered either non-personal information, or [business] Contact Information under FOIPPA. There are however opportunities amongst these open fields for personal information to present, namely and most prominently the "user photo". If information is determined to be personal information (including by the mosaic effect), Microsoft will treat it as Customer Content.

Employee Contact Data includes the following categories of data classified in Microsoft's whitepaper on "Achieving Compliant Data Residency and Security with Azure"[3]:

- Administrator data is the information about customer administrators that is supplied during signup, purchase, or administration of Microsoft services, such as administrator names, phone numbers, and email addresses. It also includes aggregated usage information and data associated with the administrator account, such as the controls that are selected. Microsoft uses administrator data to provide services, complete transactions, service the account, and detect and prevent fraud.

- Payment data is the information customers provide when making online purchases with Microsoft. It may include a credit card number and security code, name and billing address, and other financial data. Microsoft uses payment data to complete transactions, as well as to detect and prevent fraud.

- Support and consulting data means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by or on behalf of a customer (or that the customer

[3] https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Achieving_Compliant_Data_Residency_and_Security_with_Azure.pdf (page 5)

authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include descriptions of problems, files transferred to Microsoft to resolve support issues, automated trouble-shooters, or information obtained by accessing customer systems remotely with customer permission. It does not include administrator data or payment data. It is possible that support and consulting data may include personal information and if so, as per above, Microsoft will treat it as Customer Content as stated in above contract language.

Customer Content (Customer Data)

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

- Content is considered sensitive in nature. In Microsoft Cloud Services, customers control their own content data. Microsoft's role is limited to that of data processor, a position that is further reinforced in the Microsoft Online Privacy Statement, and their security audits, third party attestations and certifications such as ISO 27001.
- Specific content will range in type, volume and sensitivity according to the government programs that are making use of Microsoft Cloud Services. ***Individual programs using Microsoft Cloud Services will be assessed through individual PIAs specific to their implementation (Program PIA).***
- Customer content is not accessible or visible to Microsoft Cloud Services administrators, except in non-routine maintenance scenarios. Refer Q5 (Access) below for more details.

Part 2 – Protection of Personal Information

Contractual Protections

Given the service provider relationship with Microsoft, the Province has agreed to an amended Microsoft Business and Service Agreement (contract). This amendment is an extension of terms signed in 2018 related to the use of hyper scale cloud services however now includes the use of personal information. The Province will be using the contract as one means through which the appropriate level of protection can be ensured in relation to personal information. The contract includes provisions that ensure 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 compliance with FOIPPA.

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.

The other means of ensuring an appropriate level of protection is through the technical details (e.g. storage and access, security etc.) as described below in the rest of the PIA. ***Therefore, the Province relies on the combination of the contractual language and technical details to ensure adequate levels of protection and compliance with FOIPPA.***

Law Enforcement Disclosures are addressed later in this PIA under *Access – Foreign Demands for Disclosure.*

5. Storage or Access outside Canada

It is the intention where personal information is involved that ministries only utilize Regional Services that can be deployed in the Azure Data Centres located in Toronto and Quebec City, otherwise referred to as the Canadian Geographic Zone or Canadian Geo[4]. Any resource consumption that occurs within this zone is guaranteed by the Azure platform to stay within the zone. Azure may add additional data centres to the Canadian Geo in the future, and these data centres would be located in other areas of Canada.

From Microsoft: If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo.

Some Azure services (i) are deployed in other geographical regions or (ii) do not enable the customer to specify the region where the service will be deployed because they rely on global architecture (non-regional services). The only non-regional services covered under this Corporate PIA are Azure Active Directory and Azure Security Centre.

By default, a tenant level policy has been set up so that only services in the Canadian Region are available to ministries. ***Ministries may request other geographic or non-regional services be utilized. These requests go through the OCIO and will require additional assessment through their program specific PIA(s).***

A list of services and their associated regions can be found here (click on "select all products"): https://azure.microsoft.com/en-us/global-infrastructure/services/?products=all

[4] List of Azure services in the Canadian Geo: https://azure.microsoft.com/en-us/global-infrastructure/services/?regions=canada-central,canada-east&products=all

Storage

Microsoft's Canadian datacentres are located in Quebec City (Microsoft Azure Canada East) and Toronto (Microsoft Azure Canadian Central). These facilities are designed to run 24x7x365 and employ a variety of measures to minimize the possibility of power failures, physical intrusions and network outages. Data is replicated three times within the primary datacentre with a fourth copy provided from the secondary Canadian datacentre.

With respect to location and storage of data, each of the three basic categories of data (System or Service Data, Employee Contact Data and Customer Content) in Azure are treated individually.

1. System or Service Data comes from the ongoing operation of Azure. System data is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. All service and maintenance data are accessed and contained within Microsoft's global, private network.

2. Employee Contact Data (non-PI) will be entered into Microsoft Azure Active Directory (AAD). All replication of AAD data around the globe happens within Microsoft's global, private network.

3. Across its business, Microsoft stores Customer Content at rest within certain major geographic areas (a "Geo"). Canada has been identified as a "Geo", meaning that for government's purpose, all customer content will be resident within Microsoft's Canadian Geographic Zone (Canadian Geo). As customer content is generally the only category of data likely to contain personal information, this information's storage criteria is held to a higher standard. As such, all personal information will be held within the Canadian Geo and will not be accessible outside of Canada unless explicitly permitted by the customer or under specific FOIPPA provisions (such as for the purposes of technical maintenance, data recovery or the temporary processing of data when these disclosures meet the conditions of the legislation as outlined in FOIPPA s. 33.1(1)(p) and (p.1)).

NOTE: The above storage descriptions will not apply where (i) System or Service Data or (ii) Employee Contact Data reveal personal information (refer Microsoft's contractual obligations). In such instances, system or service data or employee contact data that is personal information will be treated by Microsoft as customer content (e.g. when at rest, storage will be in Canada).

Routing

The following options are available regarding the network connection used between the Province and Microsoft's datacentres.

1. **Public Internet:** The Province can choose to use a general internet connection. With this option, however, the Province will be unable to dictate where the network traffic gets routed across the internet.

2. **Microsoft ExpressRoute:** ExpressRoute extends on-premise networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. These connections do not go over public internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies and higher security than typical connections over the internet.

From a FOIPPA compliance perspective, either public internet or ExpressRoute are acceptable as assessed in this PIA. Ministries will need to base their decision on which of the two options to move forward with based on their business needs and security assessment (through their MISO).

Access

All personal information will be accessed from inside Canada unless explicitly permitted by the Province or with the exception of:

1. **Technical Maintenance/Data Recovery** – personal information may be disclosed (temporarily) outside of Canada for the purposes of technical maintenance or data recovery in accordance with section 33.1(1)(p) of FOIPPA. The contract with Microsoft has terms that outline requirements related to technical maintenance by requiring access, disclosure and storage of information only for the purpose of supporting (e.g. repairing or troubleshooting) an electronic system or for data recovery following the failure of an electronic system.

   Technical Maintenance: Under circumstances where the Province is not able to self-remediate an issue using available resources or with the assistance of an internal government call centre technician, a trouble ticket can be registered in the service portal to have the problem fixed by Microsoft. This Microsoft Engineer may be located outside of Canada (access controls for this are outlined below).

   Data Recovery: Such access and storage will be temporary, for the minimal amount of time necessary and will only occur after a system has failed.

2. **Temporary Processing** – personal information may be disclosed outside Canada for temporary processing in accordance with section 33.1(1)(p.1) of FOIPPA. This provision sets limits on this disclosure, including:

   a. The processing cannot involve intentional access by a human.
   b. The processing cannot result in storage of personal information outside of Canada, unless otherwise specified.
   c. Where the processing happens outside of Canada, the disclosure must be for the minimum amount of time necessary.

   To support compliance under the temporary processing conditions above, Microsoft terms state that they may process, work on, maintain, etc. customer data outside of Canada but as soon as this customer data returns to the state of being "data at rest", then it would have

to be back in the Canadian data centre. The processing that occurs would be temporary in nature and thus not considered data-at-rest (i.e. not stored outside of Canada) and considered to be for the minimum amount of time necessary. Lastly, Microsoft does not have "eyes-on-data" (intentional human access) on data within the Canadian Geo that is being processed outside of Canada.

Access Controls: Barriers to Access

Under the shared responsibility model, the key premise is that the Province controls and owns their own content and as such, Microsoft, as the cloud service provider, performs the role of data processor and has zero standing access to customer content. Zero standing access means all access requests go through a privileged access workflow, allowing just-in-time and just-enough access for the task they need to perform (e.g. no one administrator can access data on their own, at any time).

In the event a situation involving a user's content requires the assistance of a Microsoft technician or support engineer, an Incident Management ticket would be created by the Province from within Canada and the task would be assigned to the pertinent team explaining the reason for access and assigning a severity rating of the task. The technician or support engineer assigned to the ticket must be pre-authenticated and undergo dual approvals within Microsoft to be able to respond to the Client issue. They would use a Secure Administrative Workstation and upon completion of remediation activities, the administrative permissions are withdrawn. "Data Minimization" is used to minimize the amount of client data that is managed on the client's behalf by a process of tiering to specify which Microsoft internal teams can access what data. All activities conducted by the Microsoft technician would be logged and audited.

Additional access controls listed below to increase privacy protection measures for the Province may be available depending upon the Azure service that is being consumed. The decision on which access controls are implemented is a risk-based decision which balances the operational needs with the sensitivity of the information that is being protected and is to be included in the **Program PIA**.

1. **Customer Lockbox for Microsoft Azure**

Availability: For Azure, Customer Lockbox is currently only available[5] (in public preview[6]) for the following Azure services:

- *Azure Storage*
- *Azure SQL DB*
- *Azure Data Explorer*

[5] https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

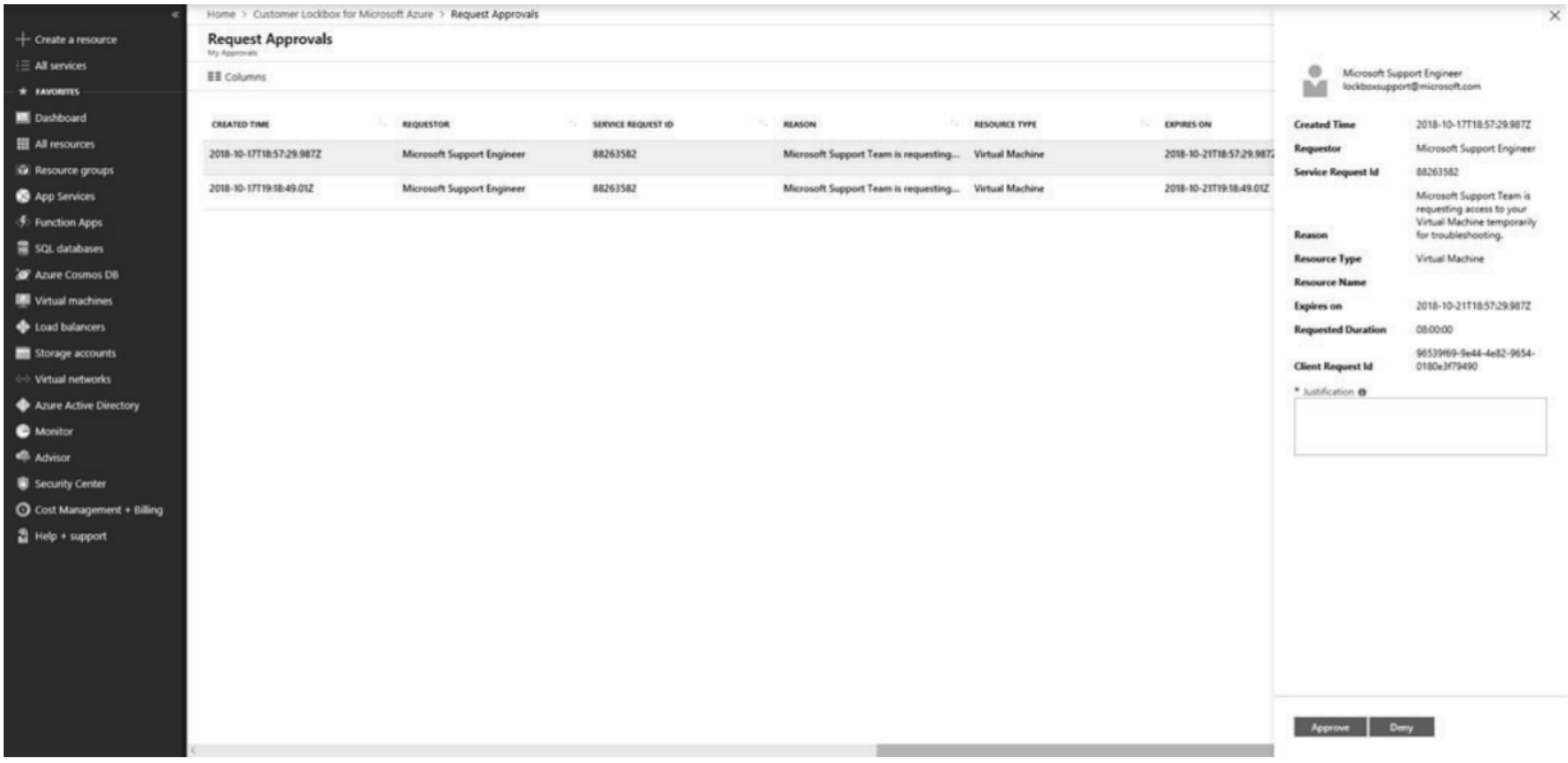
[6] "Public preview" requires an administrator to switch Preview features on or fill out a form for almost "automatic" approval. https://azure.microsoft.com/en-us/blog/approve-audit-support-access-requests-to-vms-using-customer-lockbox-for-azure/

- *Virtual Machines*
- *Azure subscription transfers*

Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data during a support request.

In such cases, Microsoft engineers use just-in-time access service that provides limited, time-bound authorization with access limited to the service. While Microsoft has always obtained customer consent for access, Customer Lockbox now gives customers the ability to review and approve or deny such requests from Azure Portal. Until the request is approved, Microsoft Support Engineer will not be granted access. As such, use of the Customer *Lockbox feature ensures that the Microsoft Engineer does not get access to government's content without government's explicit approval. This process cannot be initiated by Microsoft and must be initiated through a ticket by government.*

The entire process is audited so the Province maintains full visibility and control. All Customer Lockbox activity will be available in Azure Portal. While Customer Lockbox will be in the portal by default, during public preview, a few steps would need be taken to enable the feature as noted above.



2. Key Vault – Bring Your Own Keys (BYOK)

Azure Key Vault enables Azure applications and users to store and use data through the protection of encryption keys. To implement BYOK for Key Vault, the Province would generate their own key onsite and then transfer it to Azure. One copy of the key is "put" in the cloud and the other copy is held by the Province. It will be inserted into a hardware security module (HSM) build on technology that the key cannot be extracted from. Data flows through this and is decrypted. Under BYOK, Microsoft can't remove the key from the HSM (which is a physical device). There is a risk that Microsoft could run data through it to decrypt the data which would be mitigated through the use of audit logs.

When generated in a customer's managed vault in Azure Key Vault, these keys are by design protected by a hierarchy of keys that ends up in hardware security modules (HSMs). For added assurance, you can import (or generate) these keys in HSMs. The import of the key into HSMs for a customer's managed vault is referred as to the **Bring-Your-Own-Key** (BYOK) capability.
With this option, and thanks to its reliance on industry proven, FIPS compliant HSMs from Thales:

- The Province generates their tenant cryptographic key on its premises, using tools of its choice, in compliance with its own Security and IT policies in place.
- The key is securely transferred from an HSM in the Province's possession to HSMs in Microsoft's possession for the Azure Key Vault service. The key never leaves the hardware protection boundary. HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management.
- While in Microsoft's possession, the Province's key stays protected by Thales HSMs. Microsoft and Thales have worked together to ensure the Province's key cannot be recovered from Microsoft's HSMs.

These are the assurances that Microsoft operators cannot see or leak the key during the import as well as during the running steady state.

Additionally, in terms of transparency, the Province has the ability to setup logs that can be viewed at any time related to the keys. Events are logged immediately but is up to the Province to determine how to take action on the event so that near real-time logging is configured and thus receive near real-time usage logs from the Azure Key Vault service. You can layer this on top of BYOK to see how and when your key is being used to access a service.

The ability for the Province to see activity of a log every time a key is used, coupled with the contractual terms, partially reflects mitigation of the data sovereignty risk. Through these logs, the Province is intended to be able to view if Microsoft uses the key without Province knowledge or consent.

While all uses of the Key Vault are available, the use is dependent on the technical design of the Province's consumption of the service (e.g. appropriate configuration of the logs)[7]. The properties

[7] The following link provides a list of all the properties that are logged associated with Key Vault activities: https://docs.microsoft.com/en-us/azure/key-vault/general/logging

include what transactions lead to a log entry as well as the complete date and time down to less than the millisecond of the request, the request type (what kind of transaction), whether it was successful, the outcome, the duration of the request (how long did it take to run), the IP address of the requestor and the identity of the requestor.

Foreign Demands for Disclosure

Distinct from data residency, data sovereignty refers to authority or control over the personal information in the ministry's control.

Microsoft, as a non-Canadian company, raises the issue of data sovereignty even though it can establish data residency (e.g. its data centres are hosted in Canada). This arises because there is law in the USA that enables its government to make a legal demand for information that a vendor from that country (as is in the case with Microsoft, an American company) has in its system (i.e. a government may have the legal ability to compel companies within its jurisdiction to provide it with information regardless of the information's country of origin). In this way, Microsoft has a "conflict of laws" issue should the vendor's own government make such a legal demand for the information. Therefore, risks associated with data sovereignty are mitigated through a combination of (1) contractual protections (* see below) and (2) technical measures described above regarding access controls.

***Executive Communication*: It is important that this risk is communicated and understood by the program area's Executive in order for them to make an informed decision on accepting the risk and moving forward with the use of Azure.**

**Contractual Protections (in addition to those mentioned above):* With the contract governed by Canadian law, the customer content belonging to the Province, the customer content being encrypted and its activity logged, 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. Additionally, Microsoft agrees not to disclose Customer Data to law enforcement agencies unless required by law. Microsoft will attempt to redirect any law enforcement requests to the customer and, in doing so, may provide basic contact information to the law enforcement agency. If compelled to disclose Customer Data and notice to the Province is not permitted by applicable law, Microsoft will take reasonable steps to challenge the compelled disclosure, including, by presenting such evidence as may be appropriate to a court or other applicable judicial authority their role and obligation as service providers to the Province under FOIPPA.

Authentication

On-Premise Active Directory and Azure Active Directory

The on-premises, tenanted-Active Directory (AD) is a directory service that controls access to government's domain through authentication. AD is data resident but will sync with Microsoft's Azure Active Directory (AAD) service which controls access to government's data within Microsoft's systems.

Only IDIR accounts can be synchronized, and not the accounts for BCeID or other third-party identity providers. AAD enables employees to log in for the other Azure services. For use of ADD, the PIA and contract contemplate that there will not be any PI exchanged, only business contact information and that the authentication is happening on premise. ADD data is replicated worldwide. Attributes that may contain personal information are collected and reviewed by the Province (Access and Directory Management Services - ADMS) and will not be synced from the Active Directory (data resident) to the Azure Active Directory (non-regional service).

An additional feature that is available for environments that operate under both on-premise AD and AAD is **Hybrid Azure Active Directory Join (Hybrid Join)**. Hybrid Join can be used to make devices that are used in the Azure environment more secure and more transparent. Similar to the use of AAD, use of Hybrid Join is enabled only when non-PI elements are involved so its use under this Corporate PIA is enabled under the same conditions as AAD.

Note: any personal information stored in Azure Active Directory (e.g. usernames/contact information from citizens that are used to access Azure) would be stored and accessed outside of Canada.
Azure Active Directory is a component of the IaaS and PaaS Microsoft Cloud Service. It is included within the scope of this PIA because employee contact data is entered into AAD and is used to provide identity and access management services. It combines core directory services, advanced identity governance, security and application access management. All replication of AAD data around the globe happens within Microsoft's secure global, private network. The information is not disclosed to the public, rather it remains accessible only to the authorized users' community in the same customer tenant.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a method of identity assurance in which a user must present two or more pieces of evidence (factors) for their identity. These factors may include something you know (typically a password), something you have (such as a mobile phone or token) or something you are (biometrics like a fingerprint scan).

The two factors planned for the Province's use of MFA for cloud access under the Corporate PIA are:

1. Something you know – which is *a password*
2. Something you have – which is the option of either:
   - *A USB token with a button on it (to be provided by the Province)*. User will connect the USB, input a PIN (which is setup upon token registration), and once the PIN is accepted as correct, the user will be asked to push the button on the USB to finalize authentication.
   - *An app downloaded to a smartphone*. It will be linked to IDIR. The user will log-in with their password and accept on the app to authenticate.

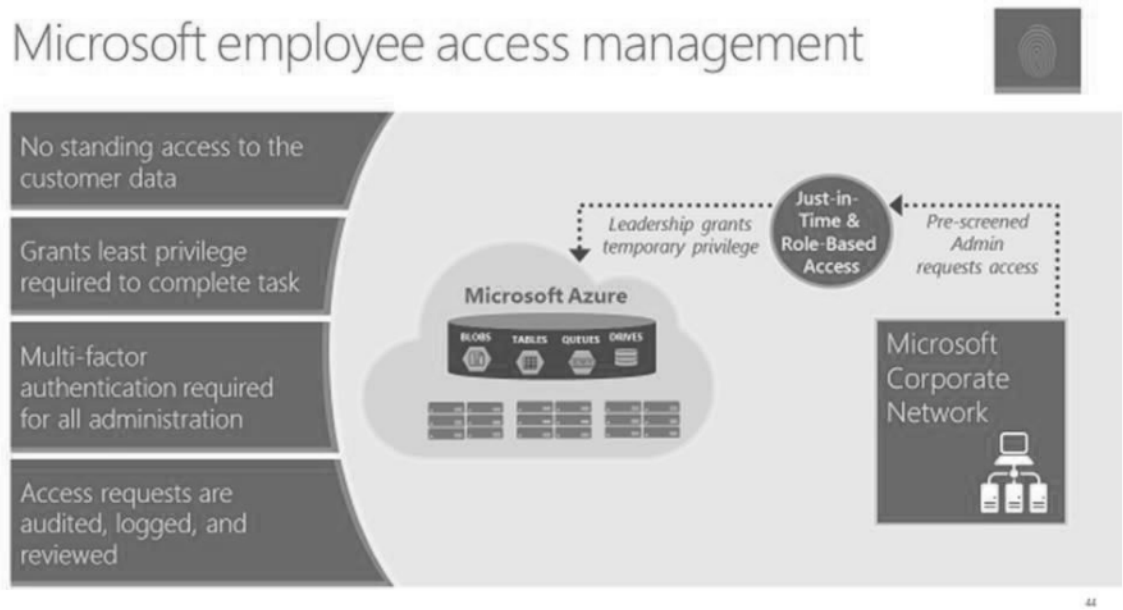
MFA preferences, including metadata such as mobile number, email address, etc., would be stored in the directory. Microsoft explained that "Azure MFA uses the attributes associated with a user's account from the AAD attributes that would be synced by the customer". These preferences would be protected with the basic encryption outlined above. Information that would link an identifiable individual to their username or account are collected and reviewed by the Province (ADMS). ADMS collected personal information is stored at a data-centre inside and accessed only from Canada.

AAD Support

The Province controls the flow of directory information to AAD. Customer content is only accessed when necessary to support the Province's use of AAD. Although there is no personal information present, Microsoft has zero standing access to this information, except when the Province allows it, through a process referred to in the Azure fabric layer as "Just in Time and Just Enough Access" services, or JIT/JEA.

A support case can be requested through the Azure Portal. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of Azure Active Directory and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). As highlighted in the below graphic, Microsoft supervisory approval is required prior to granting elevated credentials and access for resolving the support ticket. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. When granted (requires leadership approval), access is carefully managed and logged. These audit logs are available to the Province for review.

Microsoft Azure Access Control Standard Operating Procedure was reviewed by British Standards Institution in the course of Microsoft Azure ISO 27001 certification. Microsoft Azure relies on Microsoft Corporate Active Directory, managed by Microsoft IT, to control access to key information systems. Multi-factor authentication is required, and access is only granted from secure consoles. All access attempts are monitored and can be displayed via a basic set of reports. The processes mentioned rely on Just in Time (JIT) and Just Enough Access (JEA) as it relates to Azure support actions.



6. Data-linking Initiative

The use of Azure is not a data-linking initiative as defined in FOIPPA. Any initiative specific detail is to be included and assessed in the **Program PIA**.

7. Common or Integrated Program or Activity

The use of Azure is not a common or integrated program or activity. Any initiative specific detail is to be included and assessed in the **Program PIA**.

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

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Ministry interested in using Azure under this Corp PIA will engage the Hosting Team who will see what pre-built subscriptions are available to match Ministry needs. Ministry would then be added as a "Resource Group" under which OCIO can manage the account (track usage, billing etc) and begin use under that subscription.	No personal information	N/A
2.	Program area populates resource group with data (customer content that likely includes personal information). Ministry organizations have the ability to transfer entire applications, granular application capabilities, files, and/or databases to the Azure cloud	Use Disclosure	32(a) 33.2 (a) or (c)

	service. Data stored in Azure is owned, controlled and accessed by the Ministry and the data elements and flow specific to the program initiative is to be assessed separately in the **Program PIA**.		
3.	Microsoft Support for Technical Maintenance (General): i. Government employee identifies or experiences an issue which cannot be resolved internally and requires a Microsoft technician to access customer data. ii. Government employee initiates a service request with Microsoft. A Microsoft technician or support engineer will be pre-authenticated and undergo dual approvals within Microsoft. The request for access will include only the data required to perform the required troubleshooting (purpose, duration and data location). iii. Once the internal Microsoft process approved is received, the Microsoft technician accesses customer content for the purpose of remedying a technical issue. Once the predetermined time limit has expired, the technician will be locked out cannot access again without repeating the internal Microsoft process again. iv. After a service request has been completed, all access is logged and a detailed record of all activities performed is available to the government.	No personal information No personal information Disclosure No personal information	N/A N/A 33.1(1)(p) N/A
4.	Microsoft Support for Technical Maintenance (Customer Lockbox), *if applicable*: i. Government employee identifies or experiences an issue which cannot be resolved internally and requires a Microsoft technician to access customer data. ii. Government employee initiates a service request with Microsoft. Microsoft technician submits a request to a Microsoft Manager for access to the Customer Lockbox, which contains only the data required to perform the required troubleshooting.	No personal information No personal information	N/A N/A

	The request for access details the purposes, duration and data location for the request. iii. Once the request to Microsoft Manager is approved, government administrators are notified via email that there is a request for access. Government administrators then have the option of either approving or rejecting the Customer Lockbox request for access. If the administrators do not respond within 12 hours, the request will expire (by default). Expired requests do not result in access to customer content. iv. If the government administrators approve the request, the Microsoft technician accesses customer content for the purpose of remedying a technical issue. Once the predetermined time limit has expired, the technician will be locked out and cannot access the Customer Lockbox again without repeating the approval process (and being carefully scrutinized as to why the additional time is required). v. After a service request has been completed, all access is logged and a detailed record of all activities performed is available to the government.	No personal information Disclosure No personal information	N/A 33.1(1)(p) N/A
5.	The use of Azure services may result in temporary processing outside Canada. The temporary processing will not involve intentional access by an individual; will not result in storage of personal information outside Canada (unless otherwise specified); and will be for the minimum amount of time necessary.	Disclosure	33.1(1)(p.1)

Personal Information Flow Table – Authentication			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	BC government imports a limited CHIPs data element into the on-premise Active Directory attributes.	No personal information	N/A

2.	Limited attributes of non-personal information are synced from the on-premise Tenanted- Active Directory (AD) to the global Azure Active Directory (AAD).	No personal information	N/A
3.	BC Government uses AD attributes in order to authenticate users, ensure system security, encourage employee engagement and workplace collaboration	Use	32(a)
5.	By not syncing the AD attributes that may contain personal information, the Province is avoiding any disclosure of this type of personal information to Microsoft, and is also avoiding any potential storage of, or access to this information by Microsoft outside of Canada.	No personal information	N/A
5.	Multi-Factor Authentication (MFA), *if applicable*: User is prompted during the sign-in process for two or more factors of identification (e.g. password and a mobile phone or token)	No personal information (business contact information)	N/A

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Service or system data may become Personal Information (PI) by mosaic effect	Contractual mitigation that Microsoft will treat any PI like customer content regardless of if it is categorized as such.	Low	Medium
2.	That there is not proper flow-through of privacy requirements from government to service provider	Province has agreed to contractual terms with Microsoft. The contract notes that any service provider (e.g. subcontractors) must comply with FOIPPA.	Low	High
3.	Microsoft is compelled to disclose Customer Data without notifying the Province (e.g. in response to a Foreign Demand for Disclosure)	Risks associated with data sovereignty are mitigated through a combination of (1) contractual protections based on agreement with Microsoft and (2) technical measures outlined in this PIA	Low	High

		under Foreign Demands for Disclosure).		
4.	Ministry uses services that are not deployed in the Canadian GEO	OCIO has set a tenant level security policy that restricts users from using services outside the Canadian Geo by default. Requests for use of services outside the Canadian GEO will need to be requested through OCIO and be assessed in a separate **Program PIA**. Program areas can confirm which services are available in the Canadian GEO using the updated Azure Region List from Microsoft's website.	Med	High
5.	Azure service deployed in the Canadian Geo may be subject to change (service will move to non-regional or to another region).	Microsoft guarantees that regional services deployed are guaranteed by Azure platform to stay within that Geo. Any deviation or change to that (notification and recourse) has been covered in the Province agreement.	Med	High
6.	Significant change in updates made to Microsoft Online Services Terms may result in Province contract no longer aligning with the newer version.	Province's contract amendment includes a provision to outline that Microsoft's obligations to store, protect and use Customer Data remain in effect until the Customer Data is deleted from Microsoft's systems.	Med	High
7.	Microsoft may access customer content outside Canada for purposes of temporary maintenance outside of the FOIPPA conditions (only for prescribed purposes for the minimum time necessary).	Microsoft has zero standing access to customer content. When access by Microsoft technician is required, they must be pre-authenticated and undergo dual approvals within Microsoft in order to gain access to respond to the issue.	Low	High

8.	Personal information may need to flow outside Canada for temporary processing purposes	Compliance with FOIPPA 33.1(1)(p.1): Microsoft has no eyes on data (no human interaction) and the momentary nature of the processing is not considered data-at-rest and considered for the minimum time necessary.	Low	High
9.	Metadata could be characterized as personal information	Under Province agreement with Microsoft, any information that is derived by Microsoft as personal information will be treated in the same manner as Customer Content (i.e. treated as personal information).	Low	Medium
10.	Key Vault – data may be unencrypted without Province consent or notice	Near real-time logging can be used with Key Vault. This ability to view the logs at any time related to the keys is intended to notify the Province of any access to data.	Low	High
11.	Authentication – synchronization of information between BC Government's Active Directory (AD, on prem) and Azure Active Directory (AAD, cloud) results in personal information outside of Canada.	Decisions regarding which attributes are synced is reviewed and collected by Access and Directory Management Services (ADMS) to ensure they contain no personal information.	Low	Medium
12.	When in the context of an employee's at home personal use of Microsoft services, access is granted across devices to work content.	Hybrid Azure AD Join feature of Azure Active Directory may be used to address this risk as it disables access to work content through personal use of Microsoft services. Use of Hybrid Join and the attributes associated with its use showed that only non-PI elements are synced to the non-regional Azure Active Directory.	Med	Med

		OCIO will review the conditional access configurations available in the tenancy and implement a conditional access solution once one is identified and tested.		
13.	Tool is used or configured incorrectly so that processing of personal information outside of Canada does not meet the FOIPPA conditions for temporary processing.	This PIA provides clear guidance on which services comply including instruction that services which don't fall under this Corp PIA are assessed in the **Program PIA**. Appendix A – Microsoft Azure Corporate PIA Checklist helps provide this guidance on what assessment is required on the part of program areas.	Low	High

10. Collection Notice

As Microsoft will not be collecting any personal information directly, they will not be providing any 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) / 27(1)(b) of FOIPPA. Compliance of this requirement will be assessed in the **Program PIA**.

Part 3 – Security of Personal Information

Microsoft's approach for security compliance with regards to physical measures, technical measures and security policy have been covered at a conceptual level in this Corporate PIA.

A more detailed Security Threat and Risk Assessment (#02-2020) has also been completed on this initiative.

An example of Defense-in-Depth

At the service level, Microsoft uses a defense-in-depth strategy that protects data through layers of security (at the physical, logical and data layers) in the service. At a high level, the layers of defense can be visualized as:

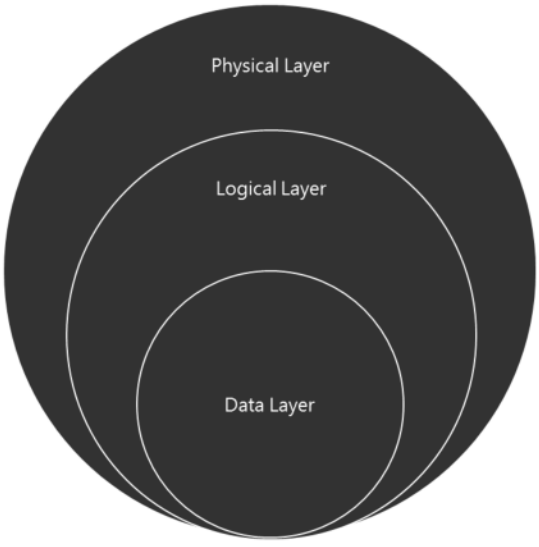


Figure 1 Defense in depth

A defense-in-depth strategy ensures that security controls are present at various layers of the service and should any one area fail there are compensating controls to maintain security.

How these safeguards are operationalized within Azure will be assessed in the Security Threat Risk Assessments (STRA).

The strategy also includes tactics to detect, prevent, and mitigate/treat a security breach before it happens. This involves continuous improvements to security features, including:

- Port scanning and remediation
- Vulnerability scanning at all different levels
- Operating system security patching
- Network-level DDOS (distributed denial-of-service) detection and prevention
- Multi-factor authentication for service access

- Regular penetration testing

With regards to people and process, preventing breaches involves:

- Auditing all operator/administrator access and actions
- Zero standing permission for administrators in the service
- "Just-In-Time (JIT) access and elevation"
- Segregation of the employee email environment from the production access environment
- Mandatory background checks for high privilege access. These checks are a highly scrutinized, manual-approval process. Additionally, Microsoft conducts background verification checks of certain operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification.
- Automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration or create a process for review of stale accounts (including non-automatically expiring accounts)
- Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services

Effective Security is the product of attention to all physical, logical, network and operational dimensions of a cloud service. A holistic approach to security ensures that all elements of a sound security strategy are addressed both individually and for the system as a whole, covering not only technology, but people and processes as well.

***11.* Please describe the physical security measures related to the initiative (if applicable).**

At the global infrastructure level, a long list of physical security measures is provided by Microsoft Azure. They are operated by Microsoft personnel and all activities are logged and can be audited. Services comply with the common engineering criteria for physical security of Azure assets and are built on an internationally certified global infrastructure foundation. Additional Information on Microsoft security, audits and certifications can be found here.

Azure Physical Security Measures

Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical data centres that house it all. Azure addresses security risks across its infrastructure.

The Canadian Microsoft facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These data centres, including Canadian facilities, comply with industry standards (such as ISO 27001) for physical security and availability. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where data is stored. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

- Access request and approval. You must request access prior to arriving at the datacenter. You're required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the datacenter required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.
- Facility's perimeter. When you arrive at a datacenter, you're required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass the perimeter. There are cameras around the datacenters, with a security team monitoring their videos at all times.
- Building entrance. The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter and monitor the videos of cameras inside the datacenter.
- Inside the building. After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacenter. If your identity is validated, you can enter only the portion of the datacenter that you have approved access to. You can stay there only for the duration of the time approved.
- Datacenter floor. You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacenter floor, you again must pass through full body metal detection screening. To leave the datacenter, you're required to pass through an additional security scan.

Microsoft requires visitors to surrender badges upon departure from any Microsoft facility.

Physical security reviews

Periodically, Microsoft conducts physical security reviews of the facilities, to ensure the datacenters properly address Azure security requirements. The datacenter hosting provider personnel do not provide Azure service management. Personnel can't sign into Azure systems and don't have physical access to the Azure collocation room and cages.

12. Please describe the technical security measures related to the initiative (if applicable).

Microsoft Cloud Services contain numerous technical controls and measures to ensure proactive and ongoing security of cloud services. For Microsoft Azure these include:

- Logical and physical network segregation/isolation and controls (regions and policies for Province specific)
- Vulnerability scans, web application scans, and penetration tests at different levels of infrastructure
- Security Update management
- Endpoint protections: firewalls, routing, identity access, Azure hybrid joined devices, DDOS protection, load balancers
- Network Protection and isolation through network security groups, policies network level
- Virtual networks governance and policy for login access and attempts
- Logging and monitoring for access controls, backups and retention for VPN and Express Route traffic
- Data Protection encryption for data at rest and transit against IM/IT standards
- Data Isolation (within tenant environment)
- Tagging aka Service Tags of asset/inventory management with metadata for audits and records management
- Governance and implementation of Role Based Access Controls (RBAC) or Attribute Based Access Controls (ABAC) to resources
- Network Security Groups (NSG), including conditional access controls for access to systems/resources, policies and traffic monitoring (ports Inbound/outbound)
- Network security and architecture: design, make baselines, application access, hardening applications, and firewalls, virtual networks (VNets), subnets, routing
- Governance, monitoring, and review of 3rd party applications data sharing with Azure against security standards

- Governance around password management

Use of government firewalls, document encryption, or user access profiles assigned on a need-to-know basis, protected by government authentication.

Azure is a multi-tenant service, where deployments of virtual machines of multiple clients are stored on the same physical hardware. Data storage and processing involves the logical segregation of clients of the same service through the structure and capabilities of Active Directory – specifically developed to help build, manage and secure multi-tenant environments.

Azure code development adheres to Microsoft's Security Development Lifecycle (SDL), a process that allows developers to build more secure software and address security compliance requirements. SDL is a Microsoft-wide, mandatory software development process with the objective of reducing the number and severity of vulnerabilities in Microsoft software.

Azure Security Center

Azure Security Center[8] provides a unified view into the security posture of the Azure services utilizing it. It enables the Province to assess security by using automation to identify and mitigate risk. For example, the user applies parameters depending upon what needs to be done and Security Center monitors for any deviations outside of the norm. As a non-regional service, the data passing through Azure Security Center may travel inside or outside of Canada. However, the data required by Security Center is considered metadata – data taken off of behaviour (i.e. passive observational data or data about data) and not the actual data itself. As such, Security Center's use is in accordance with section 33.1(1)(p.2) of FOIPPA which allows for disclosure inside or outside Canada. Any metadata that could be characterized as personal information would be treated as customer content as per the contract.

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

All service provider obligations for privacy, security and confidentiality are described in the agreement between Microsoft and the Province.

14. 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.

Identity and Access. Microsoft has strict controls that restrict access to Azure by Microsoft employees. Azure also enables customers to control access to their environments, data and applications among other access controls.

[8] https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction

Multi-Factor Authentication. Microsoft Azure provides Multi-Factor Authentication. This helps safeguard access to data and applications and enables regulatory compliance while meeting user demand for a simple sign-in process for both on-premises and cloud applications.

Enterprise cloud directory. Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management.

Access monitoring and logging. Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure Security Center and use third-party monitoring tools to detect additional threats.

Customer Lockbox (when applicable). Customer Lockbox gives customers explicit control of the very rare instances when a Microsoft technician may need access to customer content to resolve a customer issue.

Controls/polices at the various levels. Network security groups (NSG), Application security groups, Service tags, End point policies, Kubernetes/container polices, DDOS/end point protection, Appropriate/secure usage and configurations.

Nearly all service operations performed by Microsoft are fully automated and the human involvement is highly controlled and abstracted away from customer content. All access control activities in the service can be logged and audited.

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

Access to Province data is strictly controlled and logged, and sample audits are performed both by Microsoft and third parties to attest that access is only for appropriate business purposes.

Microsoft recognizes the importance of the Province's content. If someone—Microsoft personnel, partners, or government administrators—accesses government content on the service, the Province can obtain reports regarding that access. Microsoft has provided the ability for Security Information and Event Management (SIEM) vendors to create connectors for integration of their SIEM tools and the download of Azure logs. This is a pull event from Azure event logs by the SIEM tools[9] which enables government to monitor access to our data.

Part 4 – Accuracy/Correction/Retention of Personal Information

[9] https://docs.microsoft.com/en-us/azure/security/security-azure-log-integration-overview.

16. **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 in the **Program PIA**.

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

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

Given the function that Azure services, it is unlikely and not expected that decisions about an individual will be made on this platform or with its information. However, if decisions are made, records will be retained in accordance with records management obligations with details to be included the **Program PIA**.

18. **If you answered "yes" to question 17, 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 Azure is accurate and complete. The **Program PIA** will assess compliance with this requirement.

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.

19. **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 Azure is appropriately retained and destroyed. Compliance with this requirement will be assessed in the **Program PIA**.

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

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

Any government program using the data resting on Azure will be responsible for the required Information Sharing Agreements in the event that personal information is disclosed regularly and systematically. Compliance with this requirement will be assessed in the **Program PIA**.

21. 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 Azure 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 in the **Program PIA**.

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

Any government program using the data resting on Azure will be responsible for providing the Privacy, Compliance and Training Branch with information on any Personal Information Banks, should they rest on Azure's services. This provision of information will occur as a standard step in the Privacy Impact Assessment process that will be assessed in the **Program PIA**.

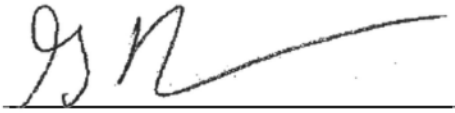
Part 6 – PCT Comments and Signatures

Any program area intending to use Microsoft Azure under this Corporate PIA must submit a separate **Program PIA**. Please see **Appendix A – Microsoft Azure Corporate PIA Checklist** for more information.

PCT is signing with the understanding that the STRA is substantially complete and that, with respect to confidentiality, reasonable security has been attained. If these findings are to change, this PIA will need to be updated to reflect the change in assessment.

Keleigh Annau		November 12, 2020
Director, Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Signatures

Stephen Gidden		November 25, 2020
Program Manager	Signature	Date
Garry Mierzuak		November 18, 2020
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date
Alex MacLennan		November 29, 2020
Assistant Deputy Minister or Designate **(if Personal Information is involved in this initiative)**	Signature	Date

Privacy Impact Assessment for
Azure Self Service Password Reset (SSPR)

PIA# CITZ20075

Part 1 – General

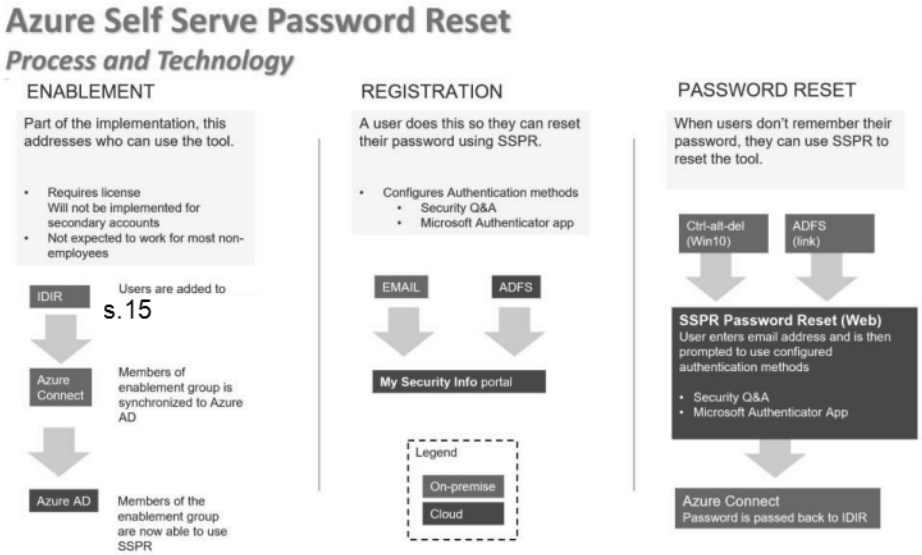
Name of Ministry:	Ministry of Citizen's Services		
PIA Drafter:	Roxanna Dehghan		
Email:	Roxanna.dehghan@gov.bc.ca	Phone:	**250-818-8829**
Program Manager:	**Marc Schafers**		
Email:	Marc.schafers@gov.bc.ca	Phone:	**778 533 0133**

1. Description of the Initiative

Device Services is shifting its technology that provides self-serve password reset capability. The intent behind the shift is to reduce costs while improving the user experience with a modern toolset. The previous technology in use was a product from Courion and had been in place for the duration of the IBM contract. At Courion's inception, it was cutting edge and successfully eliminated effort needed to support users in resetting their password when they had forgotten it. Over time the self serve capability has become commoditized and has been bundled into other technology frameworks like ServiceNow and Azure. s.13

s.13

Azure self service password reset is a cloud-based solution that is a component of Azure Active Directory and based out of the US. Given the province uses Active Directory for storing passwords, a combination of on-prem and cloud technology components are used.



This is the actual password reset process initiated by the end user. For the password reset to be initiated, the user needs to get to the SSPR reset page. The user can get to this page using one of 3 primary ways:

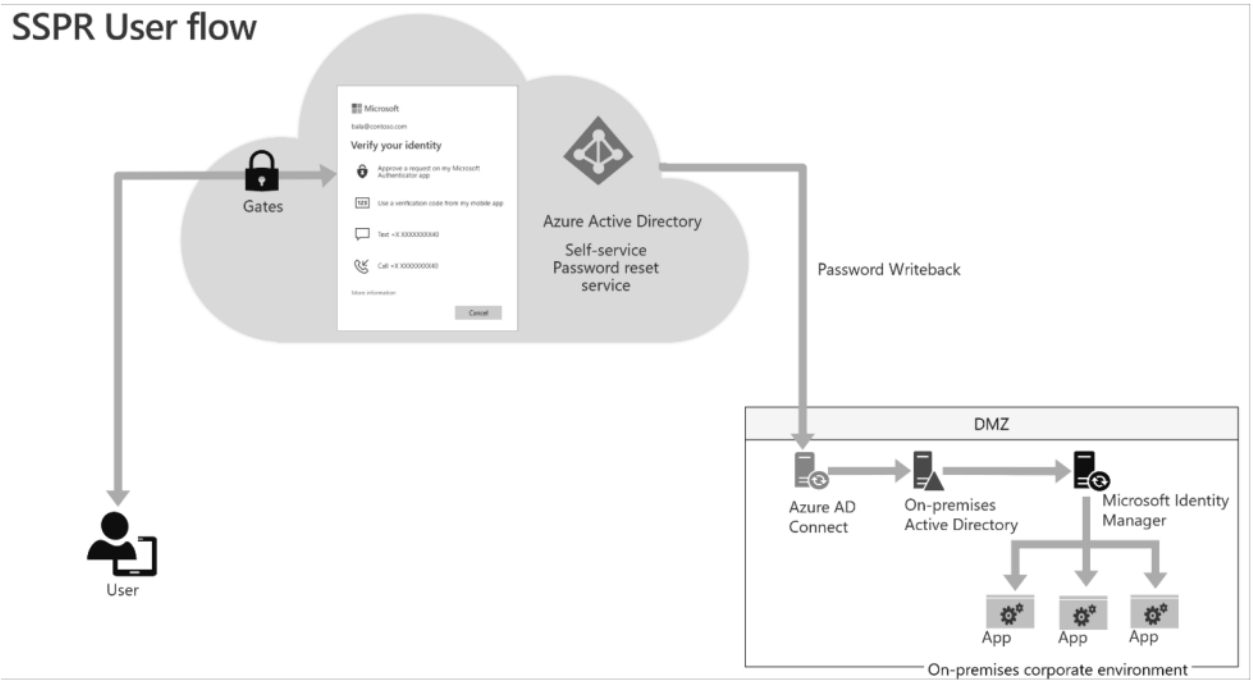
1. By navigating directly to https://passwordreset.microsoftonline.com on any device.
2. From being redirected from ADFS logon page on any device when trying to authenticate to web applications (like O365 and others).
3. From the control-alt-delete screen on Windows devices.

The user will be prompted to choose the method in which they want to reset their password. This requires that they have already configured the authentication method they planned on using. At this time this means the Security Q&A and optionally the Microsoft Authenticator app.

- **Security Q&A** – If the user has followed the registration process, they can leverage the security Q&A to reset their password. When prompted the user will need to answer 3 of the 5 or more questions they have configured during registration; the service desk does not have the ability to view these questions and answers.

- **Microsoft Authenticator App** – If this user has followed the registration process and installed the app on their personal or corporate phone, they can use this method.

This is a diagram that Microsoft provides showing the high-level flow based on an environment that has both Azure AD and Active Directories involved:



Unlike Courion, the service desk will not have the ability to view these questions and answers. This eliminates the ability for the service desk to use this method verbally with the user over the phone, which will mean that the service desk will have to use other security protocols to verify the user.

The questions and answers registered in Courion can not be imported into Azure SSPR; therefore, the user will need to configure these themselves.

2. Scope of this PIA

This purpose of this PIA is to examine the collection, storage, access, use and disclosure of information for the Azure Self Service Password Reset. Azure SSPR is one facet in which an IDIR password can be reset, other methods of resetting IDIR password is out of scope of this PIA. The Azure Self Service Password Reset can be used when the user knows their password; there are other methods not explored in this PIA where the user is able to reset their password.

3. Related Privacy Impact Assessments

CITZ18047 – Multifactor Authentication

4. Elements of Information or Data

The following 2 methods are configured as authentication for when a user needs to change/unlock a password. The user can choose either one:

- **Security Q&A** – If the user has followed the registration process, they can leverage the security Q&A to reset their password. When prompted the user will need to answer a minimum of 3 of the 5 or more questions (the User will need to answer maximum 5) they have configured during registration. The list of questions that a user can select from are shown in Appendix A: there will be a drop-down menu with limits/parameters.

- **Microsoft Authenticator App** – If the user has followed this registration process and installed the app on their personal or corporate phone, they can use this method.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Self Serve Password Reset details are stored on cloud, Azure is a global product managed by Microsoft. No personal information is stored on the Azure Active Directory cloud server. Although no personal information is accessed on the Azure cloud server, Azure Self Serve Password Reset information and metadata is stored and accessed outside Canada (Specifically in the United States).

Information that would link an identifiable individual to their username or account are collected and reviewed by Access and Directory Management Services (ADMS). ADMS' collected personal information is stored at a datacentre inside the United States however, access is restricted to Canada. Microsoft may access customer content for the purposes of technical maintenance or support on a technical basis as authorized by FOIPPA s.33.1(1)(p).

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
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

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;	No
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

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Enrollment information (IDIR only) collected from employees stored in Azure Active Directory	Collection	26(c)
2.	Password Reset Questions and Answers will be stored on the Azure Active Directory; however no personal information is accessed on the Azure Active Directory cloud server.	Use	32 (a)
3.	Microsoft may access content for the purposes of technical maintenance or support on a technical basis.	Disclosure	s.33.1(1)(p)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Employees could access personal information and use or disclose it for personal purposes	Role-based access The answers to the Q/A are only accessible by the users who input it into the system. CITZ Ministry Privacy Training Information Incident Management Policy IIMP	Low	High
2.	Request may not actually be from client (Password request may be falsified)	Implementation of identification verification procedures (similar to MFA CITZ18047)	Low	High
3.	Client's personal information is compromised when transferred to the service provider	Transmission is encrypted, hashed, and over a secure line	Low	High
4.	Unauthorized MS access	MS will only access if there is an issue (tech support) under s.33.1(1)(p)	Low	Low

10. Collection Notice

This information is collected by the Ministry of Citizens' Services (CITZ) under section 26(c) of the Freedom of Information and Protection of Privacy Act and will be used for the purposes of enabling enhanced identity and security functions through the use of Multifactor Authentication. Should you have any questions about the collection of this personal information, please contact:

Chief Information Security Officer, PO Box 9412 Stn Prov Govt, Victoria BC, V8W 9V1
Kadriye Graham, Director of Technical Stewardship (Device Services), 250 818 0768, Kadriye.Graham@gov.bc.ca

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your Ministry Information Security Officer (MISO) when filling out this section. Your MISO will also be able to tell you whether you will need to complete a separate assessment called a Security Threat and Risk Assessment (STRA) for this initiative.

11. Please describe the physical security measures related to the initiative (if applicable).

The Azure SSPR is hosted in the Microsoft Azure SaaS Cloud and therefore the infrastructure supporting the service is in the control of the vendor and is not in scope for this assessment. Identifying and log data is stored on BC Government servers using in Canada datacentres operating under 24-hour surveillance by security personnel, biometrically secured points of entry and physically/technically controlled servers with backup power systems. As stated, in-depth in PIA#MTICS16024, Azure's defense-in-depth security strategy ensures that controls are layered in order to detect, prevent and mitigate security risks in the physical, logical and data layers of the service. This is intended to ensure, in the event of the failure of one security measure, that compensating controls maintain data security. The Azure Active Directory (AAD) Service STRA (RS3265) contains further details pertinent to AAD. AAD information has not been included as AAD does not store personal information pertinent to the Azure SSPR project.

12. Please describe the technical security measures related to the initiative (if applicable).

SSPR data is securely stored using TLS encryption, firewalls and limited access for admin staff only.

Microsoft will promptly notify customers of a security incident (unlawful access to any customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure or alteration of client data), will investigate the incident and provide the client with detailed information and will take reasonable steps to mitigate the effects and to minimize damage.

The Azure Active Directory (AAD) Service STRA (RS3265) contains further details pertinent to AAD. AAD information has not been included as AAD does not store personal information pertinent to the MFA project.

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

    No the branch will not rely on security policies other than the ISP.

14. **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.**

    Access to SSPR information is restricted to a limited number of admin with limited role-based access. On the AAD, Tenant isolation based on the Azure Active Directory authorization and role-based access controls to prevent data leakage or unauthorized access across tenants and prevents the actions of one tenant from adversely affecting the service for another tenant.

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

    Audit logs track who has had access to all information in the SSPR systems. AAD Audits all operator/administrator access and actions.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. **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?**

    Users will have access to update own SSPR information.

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

    No

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

    N/A

19. 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?

N/A

Part 5 – Further Information

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

No

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

No

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

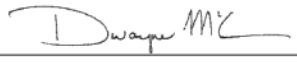
Yes, enrollment information will be accessible by name

Personal Information Bank – Required Information	
Description	SSPR Enrollment Database
Primary ministry/government agency involved	CITZ
All other ministries/government agencies and public bodies involved	None
Business contact title	Kadriye Graham, Director of Technical Stewardship (Device Services)
Business contact telephone number	250 818-0768

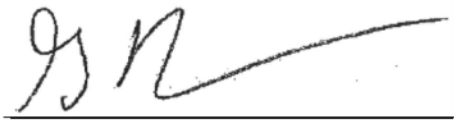
Please ensure Parts 6 and 7 are attached unsigned to your submitted PIA.

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.

Joann Berekoff Privacy Analyst Privacy, Compliance and Training Branch Ministry of Citizens' Services	 Signature	26 November 2020 Date
Dwayne McCowan Manager, Privacy Operations Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	 Signature	November 30, 2020 Date

Part 7 – Program Area Comments and Signatures

James D. Argue (for Kadriye Graham)		July 19, 2021
Program Manager	Signature	Date
Garry Mierzuak		July 21, 2021
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date
Alex MacLennan		July 21, 2021
Assistant Deputy Minister or Designate **(if Personal Information is involved in this initiative)**	Signature	Date
Executive Director or equivalent **(if no Personal Information is involved in this initiative)**	Signature	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.

Appendix A

1. In what city did you meet your first spouse/partner? In what city did your parents meet?
2. In what city does your nearest sibling live?
3. In what city was your father born?
4. In what city was your first job?
5. In what city was your mother born?
6. What city were you in on New Year's 2000?
7. What is the last name of your favorite teacher in high school?
8. What is the name of a college you applied to but didn't attend?
9. What is the name of the place in which you held your first wedding reception?
10. What is your father's middle name?
11. What is your favorite food?
12. What is your maternal grandmother's first and last name?
13. What is your mother's middle name?
14. What is your oldest sibling's birthday month and year? (e.g. November 1985)
15. What is your oldest sibling's middle name?
16. What is your paternal grandfather's first and last name?
17. What is your youngest sibling's middle name?
18. What school did you attend for sixth grade?
19. What was the first and last name of your childhood best friend?
20. What was the first and last name of your first significant other?
21. What was the last name of your favorite grade school teacher?
22. What was the make and model of your first car or motorcycle?
23. What was the name of the first school you attended?
24. What was the name of the hospital in which you were born?
25. What was the name of the street of your first childhood home?
26. What was the name of your childhood hero?
27. What was the name of your favorite stuffed animal?
28. What was the name of your first pet?
29. What was your childhood nickname?
30. What was your favorite sport in high school?
31. What was your first job?
32. What were the last four digits of your childhood telephone number?
33. When you were young, what did you want to be when you grew up?
34. Who is the most famous person you have ever met?

Privacy Impact Assessment for

Microsoft SharePoint Online and OneDrive for Business

PIA# CITZ20078

Part 1 – General

Name of Ministry:	Citizens' Services		
PIA Drafter:	Danielle Naylor		
Email:	Danielle.Naylor@gov.bc.ca	Phone:	778-698-5758
Program Manager:	Dwayne Robinson		
Email:	Dwayne.Robinson@gov.bc.ca	Phone:	778-974-5200

1. Description of the Initiative

Microsoft Office 365 (O365) Online Services is a Software-as-a-Service ("SaaS") collaboration and productivity suite, consisting of:

- SharePoint Online
- Office Online (e.g. Word, Excel, PowerPoint, Outlook), and
- OneDrive for Business.

O365 uses a set of services provided by Microsoft Azure (Azure) and Microsoft's Cloud Infrastructure and Operations (MCIO). MCIO provides the datacenters for hosting client data and networks support solutions for the O365 environment and Azure provides support service for the O365 applications, including authentication, virtual server hosting and system data storage.

SharePoint Online (SharePoint): SharePoint allows customers to share and manage content, knowledge, and applications to facilitate teamwork, find information, and collaborate across the organization. Users access SharePoint through their web browsers.

Office Online: Office Online offers the use of Microsoft Office applications (e.g. Word, Excel, PowerPoint, OneNote) via web browser and desktop integration. Office Online provides customers the ability to view and edit, via web browser, documents in Office 365. Examples include Exchange Online attachments, Teams meeting attachments, and SharePoint documents. Office Online also includes the Office Collaboration Service ("OCS") that allows users to collaborate in real-time on SharePoint-hosted documents no matter which client the user is using (e.g. Desktop, Web).

OneDrive for Business (OneDrive): OneDrive is a file hosting service that will allow clients to sync and store files from their desktop to their own personal cloud-based client, which is accessible via web-browser and mobile devices.

2. Scope of this PIA

This PIA will assess the collection, use, disclosure storage, and access of information through the SharePoint, Office Online and OneDrive applications and does not include the assessment of any other Microsoft Office 365 services that may integrate with or be accompanied by the use of these applications. Given that Teams recordings will soon be stored in SharePoint and OneDrive, Stream is also outside the scope of this PIA.

Support for the Microsoft Office 365 SaaS services noted above is provided and hosted by Azure; however, Azure (IaaS and PaaS) is not within the scope of this PIA and is assessed in the Microsoft Azure PIA (CITZ 20038).

3. Related Privacy Impact Assessments

This PIA is built on the analysis within the Microsoft Cloud Services PIAs listed below:

- CITZ20038 – Microsoft Azure Cloud Services,
- CITZ20028 – Microsoft Teams,
- MTICS16024 – Microsoft Cloud Services – Phase II, and
- MTICS15048 – Microsoft Cloud Services.

4. Elements of Information or Data

Different categories of data are treated differently with respect to storage and access. This PIA relies on the same data categories as the conceptual PIAs listed above: system data, employee contact data and customer content.

Customer Content consists of data, information, documents, spreadsheets and other artifacts that are authored, edited, communicated, maintained and eventually disposed of by the government. 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 government programs that are making use of Microsoft Office 365 Services and the collection, use and disclosure of program-specific personal information will be assessed through PIAs specific to the program area's function and operations.

Specific to SharePoint, Office Online and OneDrive, it is anticipated that broad categories of personal information may be included in the applications. For clarity, this PIA does not assess the authority to collect, use or disclose program-specific personal information, but it does assess using SharePoint, Office Online and OneDrive applications as platforms for generating records about it.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Microsoft's Canadian datacentres are located in Quebec City and Toronto. Across its business, Microsoft stores Customer Data at rest within certain major geographic areas (a "GEO"). Canada has been defined as a "GEO", meaning that for government's purposes, all customer content will be resident within the Canadian GEO. Data processing of specific Office 365 features occur outside of Canada and are completed in accordance with the conditions of FOIPPA s.33.1(1)(p.1). However, the information is stored within the Canadian datacentres and the processing occurs electronically, for the limited amount of time necessary and is not intentionally accessed by an individual.

All personal information will be held within Microsoft's Canadian datacentres and will not be accessible outside of Canada unless explicitly permitted by the customer using mechanisms such as the Office 365 Lockbox or Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with customer consent, effect temporary movement to another geo-location to ensure customer services and data are not lost.

Microsoft may also access customer content for the purposes of technical maintenance or support on a technical basis as authorized by FOIPPA s.33.1(1)(p). The contract with Microsoft has terms that outline requirements related to technical maintenance to mitigate risks related to data sovereignty For more information storage and access of personal information and related the protective terms, please see in depth analysis in the Microsoft Azure Cloud Services PIA (CITZ20038) and the Microsoft Teams PIA (CITZ20028).

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
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

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 Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
General Admin	*User information is imported into AzureAD (AAD) from Active Directory (AD).*	*Collection*	*26(c), 27(1)(b)*
	Government is disclosing Active Directory (AD) elements to Azure AD.	*Disclosure*	*N/A – disclosure is business contact information*
	User (opts to) upload photo for purpose of employee/workplace engagement and familiarity (which may include a consent-based model as reflected, if enabled).	*Collection* *Disclosure*	*26(c)* *33.1(1)(b)*
	Microsoft Engineer accesses customer context for the purpose of remedying a technical issue.	*Disclosure*	*33.1(1)(p)*
SharePoint	*User creates SharePoint site (user is SharePoint site owner).*	*Disclosure*	*33.2(c)*

	Owner (internal gov't employee) searches the AAD and adds other users (members) to SharePoint site. Users are visible to other users of that SharePoint site. **Note: In most cases this will be business contact but including authorities for completeness.*	*Collection* *Use* *Disclosure*	*26(c)* *32(a)* *33.2(a)/(c)*
	Owners add external (outside of BC Gov't) members (e.g. contractors) to SharePoint site. **Note: This feature is only available to the SharePoint sites that are connected to teams set up with MS Teams. In most cases this will be business contact but including authorities for completeness.*	*Collection* *Disclosure*	*26(c)* *33.2(a)/(c)*
	SharePoint sites are used by site members to share information and collaborate on work-related projects, activities and initiatives. *Collaboration may include document sharing and revisions, surveys and work-product histories respecting a project and/or document (e.g. eApprovals history).*	*Disclosure*	*33.2(a)/(c)*
	SharePoint logs and other data are stored on the Province's tenancy within Office 365.	*Disclosure (by Province)*	*33.2(c)*
Office Online (e.g. MS Word, Excel, PowerPoint)	*All documents created within the Office Online Suite will be stored in the SharePoint /OneDrive.*	*Disclosure*	*33.2(a)/(c)*
OneDrive	*Documents created by users containing personal information may be stored on OneDrive.*	*Disclosure*	*33.2(a)/(c)*
	Users invite another user(s) (internal gov't employee) to access document stored on an individual's OneDrive account.	*Disclosure*	*33.2(a)/(c)*
	OneDrive logs and other data are stored on the Province's tenancy within Office 365.	*Disclosure (by Province)*	*33.2(c)*

Note: All disclosures by Province and collections by Microsoft are of encrypted data only.

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*If technical retention policies are not managed, there could be hundreds of SharePoint sites that administrators are not aware exist.*	*Currently, there are default technical retention policies in place for SharePoint as a service (excluding SharePoint sites connected to Teams). OneDrive currently has a 93 day default setting for files and a 30 day default retention for user accounts that are marked for deletion.* *Compliance administrators can create technical retention policies to support records management requirements. The Microsoft Online Service Committee (MOSC) within the OCIO will be responsible for the governance of Office365 Services and determining and implementing technical retention policies. To manage the number of SharePoint sites that are created, the MOSC may consider a centralize process for creating SharePoint sites.* **Note: the technical retention policies referred to in this section are distinct from the records schedules established with Government Records Services (GRS). Technical retention policies should be established in consultation with GRS.*	*Medium*	*High*
2.	*Users may share documents stored on SharePoint and OneDrive with internal and external users.*	*External sharing is not enabled for OneDrive. Links shared by OneDrive users can only be accessed when sent to internal users within BC Gov't.* *SharePoint has different levels of permissions. Each SharePoint site has an owner or owners that manage the level of access the site members have and can add and remove members. Owners can view the names of people who viewed their files and provide differing levels of access such as editing permission or read-only permission.* *Users in SharePoint can only share with approved external users that have been added to the BC Govt Azure Active Directory (AAD), which is a*	*Medium*	*High*

		separate government-managed process. External users that already exist in the BC Govt AAD must accept sharing invitations using the same account that the invitations were sent to.		
3.	*Records management of documents and records may be challenging as files are stored on SharePoint and OneDrive rather than the LAN.*	*Program areas are responsible for retaining records and/or deleting transitory records stored on SharePoint and OneDrive in accordance with the relevant record schedules.* *Office 365 admins can create technical retention policies that apply to SharePoint and OneDrive. Technical retention policies can be set at the Office 365 admin console for the storage settings in SharePoint and OneDrive. SharePoint and OneDrive currently have the 93-day default setting for files and OneDrive has a 30-day default retention for user accounts that are marked for deletion. This can be modified to a maximum of 10 years if user accounts are required to be kept longer. OCIO is working with GRS to develop records management policy and procedures which will help inform the technical retention policies in future.*	*Medium*	*Low*
4.	*A program area may share sensitive information, without the appropriate security controls set on SharePoint sites for sharing of information.*	*Each program area must assess their use case to determine suitability given the current implementation and adjust security and privacy configurations available to owners and meeting organizers for the expected data sensitivity in use by the SharePoint members.* *If a program area has a requirement to share sensitive information via SharePoint, then the security and access controls configured for the site must be strengthened accordingly.*	*Medium*	*High*
5.	*The sign-on process for OneDrive only requires user name and password, which*	*In consultation with Information Security Branch in the OCIO, the use of multifactor authentication (MFA) when signing into the OneDrive would adequately mitigate the risk identified. There may*	*Medium*	*High*

	may impact the security of the information.	*be other controls considered in future that could adequately mitigate the risk identified.*		
6.	*Employees that have registered for the Microsoft Office 365 Personal Use Program and sign into an office product on their personal computer could access government information on SharePoint and OneDrive from their personal computer.*	*The OCIO is in the process of updating the Microsoft Office 365 Personal Use Program website and user guide outlining the appropriate settings for users. The OCIO will also send a communication to all government employees advising them of the appropriate use for the Personal Use Program and the applicable policies.* *The OCIO will review the conditional access configurations available in the tenancy and implement a conditional access solution once one is identified and tested.*	*Medium*	*High*
7.	*Microsoft may need access to customer content outside Canada for purposes of temporary maintenance and/or be compelled to disclose information without notifying the Province (e.g. in response to a Foreign Demand for Disclosure). Also, service providers need to meet the contract terms between the Province and Microsoft where applicable.*	*These risks are mitigated as described in the Microsoft Teams PIA (CITZ20028).*	*Low*	*High*

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. **Please describe the physical and technical security measures related to the initiative (if applicable).**

Microsoft encrypts data in transit and at rest and Microsoft personnel do not have standing access to the Province's data. All access is obtained through Customer Lockbox available for Office 365 Administrators within the OCIO, which enforces access control through multiple levels of approval to provide "just-in-time" access and injects the Province's administrator into the lockbox approval process. All access control activities in are logged and audited. For physical and technical security measures related to Microsoft Services, please see in depth analysis in the Microsoft Azure Cloud Services PIA (CITZ20038) and the Microsoft Teams PIA (CITZ20028).

SharePoint and OneDrive use advanced data-encryption methods between the client and the data centre, between servers in the data centre, and at rest. At rest, SharePoint and OneDrive uses disk encryption through BitLocker Drive Encryption and file encryption.

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

All service provider obligations for privacy, security and confidentiality are described in the contract between Microsoft and the Province.

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.

The SharePoint and OneDrive admin centre provides access to a central location to manage security and compliance configurations for these services. Administrators, who are internal employees from Network, Communications and Collaborations Services (NCCS) within the OCIO, log in with their regular IDIR account to configure organizational site settings. There is an internal approval process an administrator must follow before implementing infrastructure changes that impact organizational service delivery. Furthermore, Administrators can configure settings at their site level through the SharePoint or OneDrive admin centre. The Global Administrators also have access to the Office 365 Security and Compliance portal and can configure the organization wide security. Currently, there are two Global Administrator accounts.

OneDrive users can share links to documents with other BC Government users. External sharing capabilities have not been enabled for OneDrive. Users can manage access by adding and removing users that have permission to access documents stored on their OneDrive account.

Each SharePoint site has an owner or owners and SharePoint has different levels of permission that can be managed by the owner. The owner manages the level of access the site members have and are able to add and remove members, view the names of members who viewed the files and

provide differing levels of access such as editing permission or read-only permission. Users in SharePoint can only share with approved external users that have been added to the BC Govt Azure Active Directory, which occurs through a separate government managed process. External users must accept sharing invitations using the same account that the invitations were sent to.

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

Within each Office 365 application, audit functions can be set at the console level for application-specific audit capabilities; however, the overall audit functions are part of the Office 365 service. The Global Administrators have access to the Office 365 Security and Compliance portal and the admin portal to configure the organization wide security settings. Access to audit functions are currently available to Global Administrators within the OCIO as the audit capabilities are granular and access to audit logs is not available to other administrators unless they are expressly provided by Global Administrators for authorized purposes.

OneDrive has detailed reporting and auditing capabilities for files it stores as well as for those files stored through other services that use OneDrive or SharePoint, such as Teams. In addition, audit capabilities include auditing individual file actions, including downloads, renames, and views. Reporting allows administrators to view historical information such as storage usage by user and for the organization, total file and active accounts and account activity. This is managed through the Office 365 Security and Compliance Centre and provides the ability to set alerts on specific user or administrator activity, and to report on audit events by exporting the events or reports of interest.

For more information on tracking access to personal information, please see in depth analysis in the Microsoft Azure Cloud Services PIA (CITZ20038) and the Microsoft Teams PIA (CITZ20028).

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 the efforts that will be made to ensure that the personal information is accurate and complete and whether there is an 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.

Given the function that SharePoint, Office Online and OneDrive serve, it is unlikely and not expected that decisions about an individual will be made on this platform or with its information, however, if decisions are made, records will be retained in accordance with records management obligations.

Government programs will be responsible for ensuring that the personal information stored on Microsoft's systems is appropriately retained and destroyed and is accurate and complete. Compliance with this requirement will be assessed by PIAs completed by the government programs using the Microsoft services offered. For more information, please see the Microsoft Teams PIA (CITZ20028).

Part 5 – Further Information

17. Does the program/initiative involve systematic disclosures of personal information, access to personally identifiable information for research or statistical purposes or result in a personal information bank (PIB)? If yes, please explain.

No. However, any government program using the data resting on Microsoft's services will be responsible for the required Information Sharing Agreements or Research Agreements in the event that personal information is disclosed regularly and systematically or for research or statistical purposes as well as providing the Privacy, Compliance and Training Branch with information on any Personal Information Banks. Compliance with these requirements will be assessed by PIAs completed by the government programs using the Microsoft services offered.

Given the function that SharePoint, Office Online and OneDrive serve, it is unlikely and not expected that Research Agreements or Information Sharing Agreements will be required or that any PIBs will be created or stored in these applications.

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.

PCT is signing with the understanding that reasonable security can be attained with the appropriate security controls. Information Security Branch (ISB) in OCIO has confirmed that Multifactor Authentication if used, meets this. However, other controls may be assessed for adequacy in future but must be first confirmed with ISB. If these findings are to change, this PIA will need to be updated to reflect the change in assessment.

Keleigh Annau	K. Annau	November 19, 2020
Director, Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 7 – Program Area Comments and Signatures

~~Dwayne Robinson~~ Aaron Leskiw		November 30, 2020
a/Executive Director Network, Communications and Collaboration Services OCIO Enterprise Services	Signature	Date
Heather Dunlop		December 03, 2020
Director, Information Privacy and Security and Ministry Privacy Officer Information Management Branch OCIO Enterprise Services	Signature	Date
Garry Mierzuak		November 22, 2020
Ministry Information Security Officer Information Management Branch OCIO Enterprise Services	Signature	Date
Alex MacLennan		December 1, 2020
Assistant Deputy Minister and Chief Technology Officer OCIO Enterprise Services	Signature	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.

ID: 21034, Title: CITZ use MDM Intune

Full Name:

Approval Route: Lam, Keith > Gergel, Michael > Kirsten McCaig > Attwood, Mindy

Assigned To: Attwood, Mindy CITZ:EX Rush: No Other - Other Signature: Executive Director

Branch: ES-NCCS Other Number: CITZ21046

Link: N/A

Due Date: 2/4/2022 Date Completed: N/A Date Initiated: 1/28/2022 N/A

Item History

2/3/2022 05:32 PM

McCaig, Kirsten [Assignee] approved the item and forwarded it to Attwood, Mindy CITZ:EX for action

Approved. I can't add my signature on docs in e-approvals, so I am hoping that this approval services that purpose for tracking. If not, please ask my admin July Lee to download this file and place it in my signing folder. thanks

1/31/2022 02:15 PM

Gergel, Michael CITZ:EX [Assignee] approved the item and forwarded it to McCaig, Kirsten for action

Kirsten - Keith and I approve.

1/28/2022 10:25 AM

Attwood, Mindy CITZ:EX created this item

Intune PIA is ready for final executive signatures.

1/28/2022 10:25 AM

Attwood, Mindy CITZ:EX has created a new eApprovals item and assigned it to Gergel, Michael CITZ:EX

1/28/2022 10:25 AM

Attwood, Mindy CITZ:EX added a document: CITZ21046 -MDM INtune PIA.FINAL V2 - PCT Signed.pdf

Privacy Impact Assessment for

Microsoft Intune

PIA#*CITZ21046*

Part 1 – General

Name of Ministry:	Ministry of Citizen's Services		
PIA Drafter:	Roxanna Dehghan		
Email:	Roxanna.dehghan@gov.bc.ca	Phone:	**250-818-8829**
Program Manager:	**Keith Lam**		
Email:	Keith.Lam@gov.bc.ca	Phone:	**250 387-9252**

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

Microsoft Intune is a cloud service that provides mobile device management, mobile application management and PC management capabilities. Intune will allow the Province to provide employees with access to corporate applications, data, and resource from virtually anywhere on almost any device, while helping to keep corporate information secure. The application itself leverages access controls from Azure Active Directory and Conditional Access to helps secure corporate data, including Exchange Mail, Outlook Mobile, OneDrive and OneNote from Business documents, based on the enrollment status of the device and the compliance policies set by the administrator.

The MDM-Intune Service is not intended to be a repository for critical or personal information. The type of information included is business contact information such as phone number and email address.

2. Scope of this PIA

The scope of this assessment is limited to the use of Microsoft Intune as a Mobile Device Management (MDM) and Mobile Application Management (MAM) service for the BC Government. In scope for this assessment are the following mobile Operating Systems:

- iOS
- Android OS
- MacOS

This PIA's assesses any privacy implications of the information through the use of Microsoft Intune and does not include the assessment of any other Microsoft services that may integrate or be accompanied by the Use of Microsoft Intune. The Intune service itself does not involve any personal or sensitive information.

3. Related Privacy Impact Assessments

MTICS15048, MTIC16024, CITZ17025, CITZ20028, CITZ20038, CITZ20078 discuss elements of Azure Activity Directory and previous versions of Microsoft Intune pertinent to this PIA

CITZ000762 STRA

4. Elements of Information or Data

When using Microsoft's cloud services, the province remains the sole owners 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 data processor.

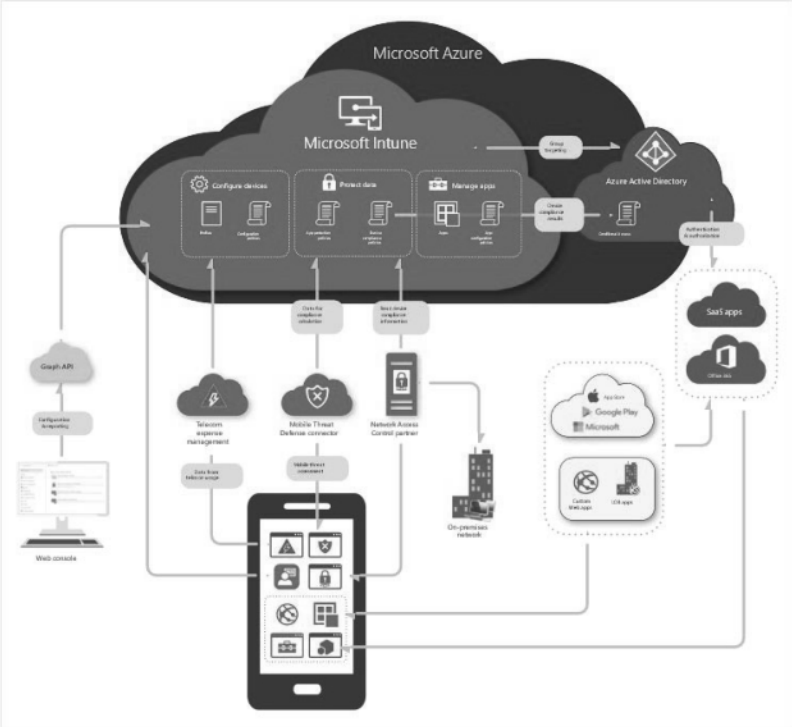
Administrators cannot see personal information when a device is enrolled with Microsoft Intune. Only certain pieces of information on the device, such as:

- Device model
- Device manufacturer
- Operating system and version
- App inventory and app names. On personal devices, admins can only see the managed app inventory and names, no data/content is visible. For corporate-owned fully managed and dedicated devices, admins can see all of the app inventory. For corporate-owned devices with a work profile, only see the app inventory in you're the profile is seen.
- Device owner
- Device name
- Device serial number
- IMEI

What might be viewable:

- Phone number: For corporate-owned devices, the full phone number can be seen. For personal-owned devices, just the last four digits of the phone number are visible.
- Device storage space.
- Location: For corporate-owned devices, admins can see the location of a lost device. For personal-owned devices, admins can never see the device location, unless they're trying to find a lost, supervised iOS device.
- Network Information: if the device is being monitored to stay withing a certain location.

Below is a figure of how information flows from mobile devices into Intune and Azure Active Directory.



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.

Jessica Bouchard		September 3, 2021
Privacy Advisor Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens Services'	Signature	Date

Part 7 – Program Area Comments and Signatures

Program Manager	Signature	Date
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date

N/A		
Assistant Deputy Minister or Designate **(if Personal Information is involved in this initiative)**	Signature	Date
Executive Director or equivalent **(if no Personal Information is involved in this initiative)**	Signature	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.

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.

Privacy Impact Assessment for

Microsoft Cloud Services – Phase II

PIA#*MTICS16024*

Part 1 – General

Name of Ministry:	Ministry of Technology, Innovation and 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:	**250-387-8053**

1. Description of the Initiative

Background

The government of British Columbia (BC) is considering the adoption of Microsoft Cloud Services with an in-Canada data residency option for the delivery of IT services to the BC public service. Microsoft Cloud Services in Canada provide an ideal opportunity for modernization, increased agility and robust information security and privacy practices, all while lowering the overall cost and complexity of the Province's information technology services.

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.

The state-of-the-market information technology offerings will provide government with a strategic opportunity to achieve better outcomes for the province through:

- Industrial Grade Security;
- Greater Agility and Service Modernization; and
- Lower Costs through Shared Infrastructure and Converged Communications Technologies.

Based on the availability of cloud services in Canada, the government's Office of the Chief Information Officer (OCIO) is considering Microsoft Cloud Services, specifically Microsoft's Software-as-a-Service (SaaS) Office 365 as an important IT modernization strategy for the Province. Deployment of Microsoft's Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) may be contemplated in the future.

Microsoft Cloud Services Overview

Prior to the cloud, systems were developed in a highly manual, intensive fashion that saw technology specialists provision servers, cabling and software, then manually install and configure

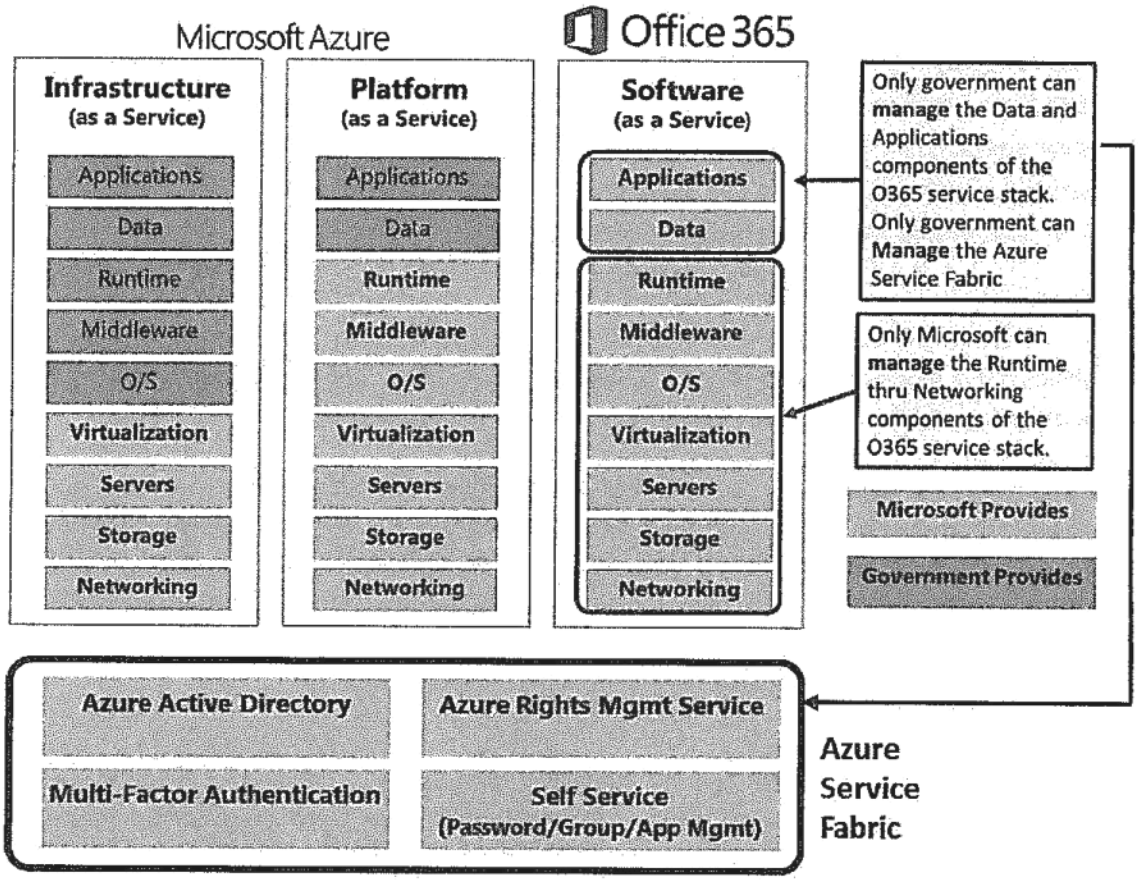
the software and hardware for the purpose of delivering capabilities such as government email services. Following the construction of the system, the same technicians would administer, operate, monitor, patch and evergreen the system.

Microsoft's cloud services are fundamentally different from government's traditional on-premises and out-sourced data centre infrastructure computing models, and represents a profoundly different approach to the delivery of information technology services. Microsoft Cloud Services are highly automated. More importantly though, Microsoft Cloud Services separates the operations, scaling, maintenance and ever-greening of the system from access to end-user content.

Microsoft's Azure cloud based computing architecture provides clear separation of roles, duties and controls related to access and management of their O365 SaaS. Microsoft states that proof of this level of separation is verified through their implementation of the most comprehensive set of certifications and attestations of any cloud vendor. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, such as ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1 and SOC 2. Further, because regulations and standards are always evolving, Microsoft's compliance experts are actively planning upcoming changes to help ensure continuous compliance—researching draft regulations, assessing potential new requirements, and developing corresponding controls.

As illustrated below, Microsoft provides all of the infrastructure: from the foundational Azure cloud service fabric, the complete applications stack) down to networking (i.e., all the applications, operating system, cloud management, and network software, including the server and storage hardware elements required to support these software components - see diagram below). A key premise of the model is that the customer controls and owns their content, Microsoft has no standing access to the service components that the government is responsible for (applications configurations, and all application data) in their cloud SaaS solution. Explicitly, this applies to the Office 365 server applications: Exchange, Skype, SharePoint, OneDrive and related services; as well as the Azure Service Fabric including the Azure Active Directory and related services. Microsoft, as the cloud service provider, performs the role of data processor and has zero standing access to customer content. The service provider only interacts with customer data under exceptional circumstances for the purpose of providing support services when a problem cannot be self-remedied by the customer's own IT or in-house support teams.

Microsoft's cloud based service stacks:
IaaS, PaaS, and SaaS



Overview of Microsoft Office 365

Microsoft Office 365 is a cloud computing-based subscription, SaaS that leverages Microsoft Azure. Microsoft Azure supports Office 365 in 4 key ways:

1. Office 365 SaaS Infrastructure (servers, network, disk arrays, and all supporting systems);
2. Azure Active Directory (Global Directory to support authentication, access control and asset management);
3. Azure Digital Rights Management (optional overlay security service for enhanced information protection);
4. Intune Mobile Device Management service; and,
5. Customer Lockbox.

Microsoft Office 365 consists of:

1. Office 2016 (desktop and cloud-based traditional Microsoft Office suite of software);
2. Unified Communications (Exchange email and Skype for Business, which includes audio and video conferencing, Voice over IP, etc.);
3. Office 365 SaaS fabric services (security and compliance management tools that overlay all application services);
4. OneDrive (conceptually similar to Shared File Service today); and,
6. SharePoint (Web-enabled collaboration services).

Key Azure-level Applications

In order to discuss the applications that are a part of this Office 365 implementation, it is necessary to discuss key services provided by Azure that are relied on throughout Office 365.

Supporting Office 365 is a web-based administrative interface that allows users to configure settings delegated to them by client administrators. In this way, both administrators and individual users can enact privacy and security protections and preferences, as has been allotted to them. For example, administrators can restrict the domains that are permitted to interact with a service, and the users can further limit this, as necessary. In practical terms, this means that program areas with particularly sensitive data may add additional safeguards.

Azure Active Directory (AAD)

Azure Active Directory supports Office 365 by providing an identity and access management service. It combines core directory services, identity governance and application access management. Azure Active Directory is a modern identity management solution spanning on-premises and cloud, providing the necessary security capabilities for application access control, federation, identity management, user provisioning, information protection, standard protocols support, comprehensive development libraries, and more.

Azure Rights Management Service

Azure Rights Management Service is another Office 365 support. Microsoft's Rights Management Service is intended to protect information at the data level using encryption, user identity, and authorization policies to help secure files and email in transit across multiple devices—phones, tablets, and PCs. This service allows the province to encrypt shared data and apply policies on data to limit or allow actions by the recipient of the data.

Microsoft Intune

Microsoft Intune is a cloud service that provides mobile device management, mobile application management and PC management capabilities. Intune will allow the Province to provide

employees with access to corporate applications, data and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. The application itself leverages access controls from Azure Active Directory and helps secure corporate data, including Exchange email, Outlook email, and OneDrive for Business documents, based on the enrollment status of the device and the compliance policies set by the administrator.

Key Office 365 Applications

The focus of this PIA will be the key Office 365 applications with which users will interact.

Exchange Online

Microsoft Exchange Online is an email, calendar and contacts solution delivered as a cloud service, hosted by Microsoft, that would be used by all of government. Exchange Online provides end users with a familiar email experience across PCs, the Web and mobile devices, while giving government IT administrators web-based tools for managing their online deployment.

Exchange Online Protection (EOP)

Exchange Online Protection is the enterprise-class spam and malware filtering service offered in conjunction with Exchange Online. EOP can utilize layers of protection features deployed across a global network of datacentres, simplifying the administration of messaging environments; however, for the purposes of the BC Government, EOP will be deployed through only Canadian datacentres.

Skype for Business (SfB)

Skype for Business (formerly Microsoft Lync) is an instant messaging client used with the Skype for Business Server. The real-time communications server software provides the infrastructure for enterprise instant messaging, presence, VoIP, ad hoc and structured conferences (audio, video and web conferencing) and public switched telephone network (PSTN) connectivity through a third-party gateway or SIP trunk.

A feature of SfB is Skype Meeting Broadcast. This component enables Office 365 users to produce and broadcast a meeting on the internet with up to 10,000 attendees, who can attend from a browser on virtually any device. With Skype Meeting Broadcast, users can host large virtual meeting such as webinars, all-hands meetings, and other one-to-many presentations. Scheduling options allow the Province to limit attendance to people within the Government tenant or open it to external users.

SharePoint Online

SharePoint Online, part of the Microsoft Office 365 suite for online productivity solutions, and the successor to Business Productivity Online Services (BPOS), provides a platform for government to

enhance and extend the functionality of existing on-premises SharePoint deployments using a cloud-based service. SharePoint Online provides a single, integrated location where people can:

- Collaborate with team members and external parties;
- Find organizational resources;
- Look up corporate information; and
- Glean business insights for better-informed decisions.

OneDrive for Business is an integral part of Office 365 and is provided by Office 365's SharePoint Service. It provides a secure cloud storage location where employees can store, share, and sync their work files. OneDrive allows employees the ability to easily share files between their different devices.

2. Scope of this PIA

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

This PIA will address the Microsoft service offerings that are deployed corporately. The intention of this PIA is to establish that the foundational infrastructure and platforms that government programs use are compliant with BC's FOIPPA. Some of Microsoft's services, namely Skype (specifically web conferencing) and SharePoint, can be deployed in significantly different capacities from ministry to ministry, making assessment here too broad. SharePoint and Skype will be addressed separately in Corporate Privacy Impact Assessments that will set out fixed parameters within which these services can be used. However, this PIA should establish that these services are able to be consumed in a lawful manner. In essence, this PIA is intended to cover the procurement of the Office 365 services from Microsoft.

"Office 365" refers to the subscription plans that include access to Office applications plus other productivity services that are enabled over the internet (i.e. cloud services). Microsoft can provide these services in a variety of packages. This PIA assumes that the Office 365 Enterprise5 package will be used (and thus all of its services available). However, the PIA excludes (for now) those services that will not be enabled until further review is conducted.

Included in this PIA's analysis are services that are equal in function to the set of services provided and supported by the OCIO today:

- Azure Directory and Rights Management Service;
- Enterprise Mobility Suite, include Intune;
- Office Suite, including Project and Visio;
- Skype for Business;
- Exchange Online and Exchange Online Protection; and
- SharePoint Online (including OneDrive for Business).

Additional Microsoft services that will not be covered by this PIA, either due to the Province not implementing them in the short term, or at all, include:

- Yammer;
- Sway;
- Apps Management; and
- Power BI and Delve Analytics.

Microsoft's security system is also out of scope of this PIA as this has been addressed, at a high level, in the conceptual PIA completed on this initiative (MTICS15048). However, some of the key security measures that support what is otherwise provided in this PIA will be discussed. Further, to ensure that the Microsoft Cloud Services' security is assessed at the appropriate level of granularity, an assessment of Microsoft's security features is addressed in detail in separate Security Threat and Risk Assessments:

- Microsoft Intune Cloud Service (RS3270);
  Azure Rights Management (RS3268);
- Office 365 OneDrive and SharePoint Service (RS3267);
- Azure Active Directory Service (RS3265);
- Common fabric to support O365 SaaS services (RS3264);
- Unified Communications - Office365 (RS3263);
- Office 2016 SAAS Offering (RS3262);
- Microsoft Office 365 SaaS Infrastructure (RS3308).

3. Related Privacy Impact Assessments

This PIA is built on the analysis within the Microsoft Cloud Services PIA (MTICS15048), which conceptually set out the high level parameters of the Microsoft IaaS and PaaS offerings. Although this PIA does not address any government applications to be built on Microsoft's IaaS and PaaS, Microsoft's SaaS, Office 365, suite of services rely on Microsoft Azure, and are thus able to leverage all of the privacy and security protections discussed in PIA# MTICS15048.

Government programs that are built on Microsoft Cloud Services, both IaaS and PaaS, will be required to conduct PIAs that address their specific programs.

4. Elements of Information or Data

Different categories of data are treated differently with respect to storage and access. This PIA relies on the same data categories as the conceptual PIA: system data; employee contact data; and client-generated data, or customer content. To reiterate and summarize the conceptual PIA:

System or Service Data	"System or Service Data" is information about, and generated by, an information system or cloud service, and is non-personal in nature. Examples of service data include: capacity, system health indicators, network traffic volume and bandwidth consumption. All of these are examined or used solely for the purpose of providing the cloud service. System data is distinct from client-created content and is used solely for the purpose of providing, operating and maintaining the service, or diagnosing and/or troubleshooting in the event of problems or system outages. System data is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. Its use is controlled and limited to the provisioning, maintenance, support and ongoing operation of cloud services. All service and maintenance data is accessed and contained within Microsoft's global, private network. System administrators, service technicians and operators access this data. As a rule, technicians are granted just-in-time minimum ("just-in-time"*) privileges necessary to troubleshoot the system on an exceptional basis, and only for a fixed period of time. Upon completion of any maintenance task, administrative privileges and access to service data are revoked, and all associated data around these activities are logged. *"Just-In-Time access and elevation" refers to Microsoft's

Employee Contact Data	"Employee Contact Data" is information to identify and differentiate users of the cloud service. This includes User ID, Organizational ID and basic user contact information (e.g. phone number or email address). This information is used by Microsoft staff in order to troubleshoot service and access issues (e.g. jsmith cannot access file A). The full list of attributes that fall within this category can be found in Appendix A. The vast majority of Employee Contact Data is considered either non-personal information, or [business] Contact Information under FOIPPA. There are however opportunities amongst these open fields for personal information to present, namely and most prominently the "user photo" Attributes that may contain personal information will not be synced from the Active Directory (data resident) to the Azure Active Directory (not stored within Canada). The attributes that will not be synced are noted in gray within Appendix A.
Customer Content	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.

Part 2 – Protection of Personal Information

5. Contractual Protections

This section of the PIA has been completed provisionally given that contract negotiations are underway. This section will be revised as the approach outlined below becomes more concrete (i.e. actual agreed upon contractual provisions).

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, which is: 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 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 compliance with FOIPPA.

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.

Law Enforcement Disclosure
Microsoft will agree not to disclose Customer Data to law enforcement agencies unless required by law. Microsoft will attempt to redirect any law enforcement requests to the customer and, in doing so, may provide basic contact information to the law enforcement agency. If compelled to disclose Customer Data to law enforcement, Microsoft agrees to use commercially reasonable efforts to notify the Province in advance of a disclosure and provide a copy of the demand, unless legally prohibited from doing so.

6. Storage or Access Outside of Canada

Microsoft's Canadian datacentres are located in Quebec City and Toronto. These facilities are designed to run 24x7x365 and employ a variety of measures to minimize the possibility of power failures, physical intrusions and network outages. Data is replicated three times within the primary datacentre with a fourth copy provided from the secondary Canadian datacentre.

Across its business, Microsoft stores Customer Data at rest within certain major geographic areas (a "GEO"). Canada has been defined as a "GEO", meaning that for government's purposes, all customer content will be resident within the Canadian GEO.

All personal information will be held within Microsoft's Canadian datacentres and will not be accessible outside of Canada unless explicitly permitted by the customer using mechanisms such as the Office 365 Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with customer consent, effect temporary movement to another geo-location to ensure customer services and data are not lost.

A decision remains regarding the network connection used between the Province and Microsoft's Canadian datacentres. The Province can choose to use a general internet connection, or to implement a direct connection called ExpressRoute. Given the Province is unable to dictate where the network traffic gets routed across the internet, the preferred solution would be to use Express Route (a dedicated secure channel). It is possible that depending on the provider, there may be a situation where, if the primary link across Canada fails, the secondary link may route traffic through US based facilities. In any case, the traffic is fully encrypted and so exposure potential is minimal.

7. 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
If you have answered "yes" to all three questions, please contact a PCT Privacy Advisor to discuss the requirements of a data-linking initiative.	

8. 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.	

9. 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. Primary connectivity to the Microsoft datacentre will be through Canadian paths. 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, that the flow of personal information between Microsoft and the Province will be conducted under the following authorities for collection and disclosure:

- 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), STRARS3262 and discussed at a high-level in Part 3 of this PIA substantiate that Microsoft can only access customer content through Customer Lockbox.

On-Premises Active Directory and Azure Active Directory

The on-premises, tenanted-Active Directory (AD) is a directory service that controls access to government's domain through authentication. AD is data resident but will sync with Microsoft's Azure Active Directory (AAD) service which controls access to government's data within Microsoft's systems. The elements of the AD that would sync to AAD are limited to data that is considered business contact information. All AAD attributes are listed in Appendix A (with those attributes currently identified to not be synced marked in grey).

Azure Active Directory is a component of the IaaS and PaaS Microsoft Cloud Service. It is included within the scope of this PIA because employee contact data is entered into AAD and is used to provide identity and access management services. It combines core directory services, advanced identity governance, security and application access management. All replication of AAD data around the globe happens within Microsoft's secure global, private network. The information is not disclosed to the public, rather it remains accessible only to the authorized users' community in the same customer tenant.

Personal Information Flow Table #1 – Azure Active Directory			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*BC government imports a limited CHIPs data element into Active Directory attributes.*	*No personal information*	*N/A*
2.	*BC government contractually limits Microsoft to sync limited attributes of non-personal information from the Tenanted-Active Directory (AD) to the global Azure Active Directory (AAD).*	*No personal information*	*N/A*
3.	*BC Government uses AD attributes in order to authenticate users, ensure system security, encourage employee engagement and workplace collaboration*	*Use*	*32(a)*

4.	*By not syncing the AD attributes that may contain personal information, the Province is avoiding any disclosure of this type of personal information to Microsoft, and is also avoiding any potential storage of, or access to this information by Microsoft outside of Canada.*	*Disclosure*	*N/A*

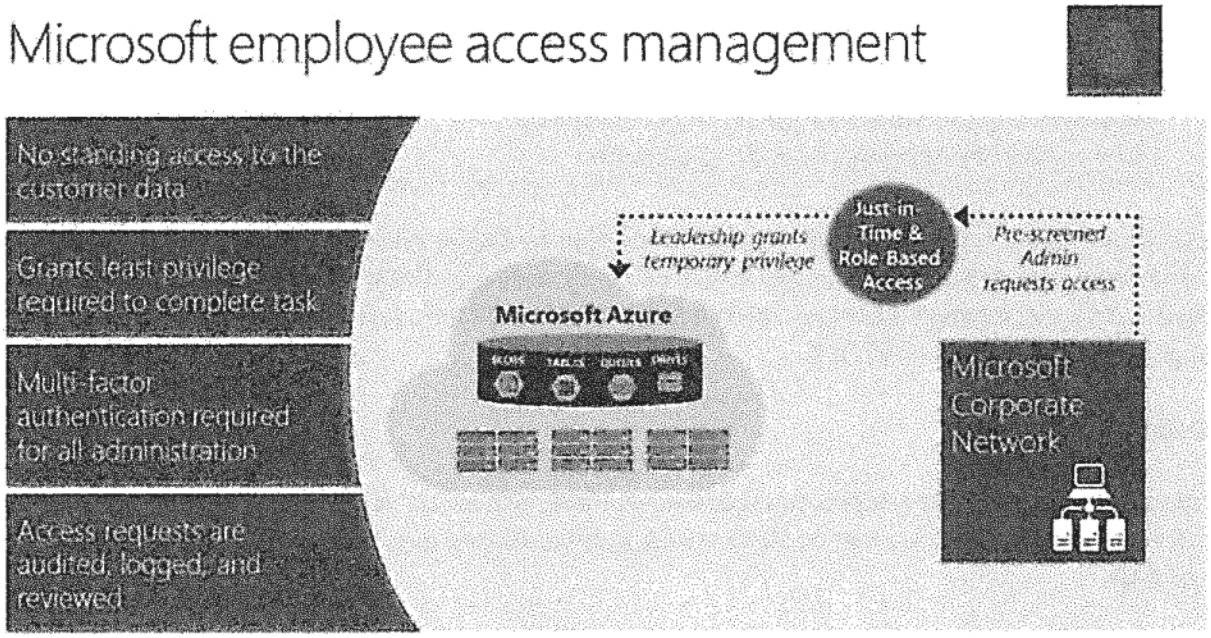
The Province controls the flow of directory information to AAD service. Although there is no personal information present, Microsoft personnel will not have access to this information, except when the Province allows it, through a process referred to in the Azure fabric layer as "Just in Time and Just Enough Access" services, or JIT/JEA.

AAD Support

Microsoft has zero standing access to customer content, and access to customer content by Microsoft personnel is restricted. Customer content is only accessed when necessary to support the Province's use of AAD.

A support case can be requested through the Azure Portal, or the Microsoft Premier Services contract. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of Windows Azure Active Directory (in support of Office 365) and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). As highlighted in the below graphic, Microsoft supervisory approval is required prior to granting elevated credentials and access for resolving the support ticket. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. When granted (requires leadership approval), access is carefully managed and logged. These audit logs are available to the Province for review.

Microsoft Azure Access Control Standard Operating Procedure was reviewed by British Standards Institution in the course of Microsoft Azure ISO 27001 certification. Microsoft Azure relies on Microsoft Corporate Active Directory, managed by Microsoft IT, to control access to key information systems. Multi-factor authentication is required, and access is only granted from secure consoles. All access attempts are monitored and can be displayed via a basic set of reports. The processes mentioned rely on Just in Time (JIT) and Just Enough Access (JEA) as it relates to Azure support actions.



Exchange Online

Microsoft Exchange Online users interact with this service via software email clients (e.g., Outlook, Exchange ActiveSync, and Outlook Web App). In plain terms, Outlook, Exchange ActiveSync and Outlook Web App are the services with which a user would use their Exchange account (i.e. email, calendar) via their computer, their mobile device and their personal computer.

Exchange Online stores customer data within mailboxes that are hosted within Extensible Storage Engine ("ESE") databases called mailbox databases. These mailboxes include user mailboxes, resource mailboxes (e.g. meeting rooms, vehicles), shared mailboxes and public folder mailboxes. User mailboxes may also include saved Skype for Business data, such as conversation histories (functionality currently available today). User mailbox data includes emails and email attachments, calendaring and "free/busy" information, contacts, tasks, notes, groups, voice mails for Unified Messaging enabled mailboxes and inference data.

Each mailbox database within Exchange Online contains mailboxes from multiple tenants. All mailboxes are secured by authorization code, including within a tenancy. As with an on-premises deployment of Exchange, by default, no one but the assigned user has access to a mailbox. The access control list ("ACL") that secures a mailbox contains an identity that is authenticated by Azure Active Directory (AAD) at the tenant level. The mailboxes for Tenant A are limited to identities authenticated against Tenant A's authentication provider. Such identities involve only users from Tenant A. Note:

"Tenant" represents government's space in the Microsoft Cloud; "User" refers to the individual/person.

Personal Information Flow Table #2 - Exchange			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Exchange mailbox is established for an individual user*	*n/a*	*n/a*
2.	*User sends/receives emails from mailbox that may/may not contain personal information*	*n/a*	*n/a*
3.	*Email is analyzed by Exchange Online Protection filters*	*See Personal Information Flow Table #3 below on Exchange Online Protection*	
4.	*Summary of email transport activity is logged by Microsoft in tracking logs (containing fields: sent by; sent to; subject heading; time stamp)*	*Collection*	*26(c)*
5.	*Email is stored on the Province's tenancy within Microsoft's servers.*	*Disclosure (by Province)*	*33.2(c)*
Note: All disclosures by Province and collections by Microsoft are of encrypted data only. The Province retains the only encryption key and is thus the only party able to view personal information.			

Email Records Management: This technology in Office 365 enables Microsoft customers to control how long to keep items in users' mailboxes and define what action to take on items that have reached a certain age.

Exchange eDiscovery, Advanced eDiscovery, and/or Data Loss Prevention: Microsoft provides a tool characterized as an "eDiscovery Center" in Exchange. This tool can be delegated to specialist client users (e.g. compliance officers, human resources personnel) to search for and preserve records for litigation purposes. eDiscovery uses the content indexes created by Exchange Search. Authorized customer users can perform an eDiscovery search by selecting the mailboxes, and then specifying search criteria such as keywords, start and end dates, sender and recipient addresses, and message types. The function can also be used to proactively identify client-defined sensitive information for data loss prevention purposes. After the search is complete, authorized users can then:

- Obtain an estimate of the total size and number of items that will be returned by the search, based on the specified criteria;
- Preview search results (messages returned from each mailbox searched are displayed);
- Copy search results (copy messages to a discovery mailbox); and
- Export search results to a PST file.

Advanced eDiscovery builds on the eDiscovery capabilities by enabling an initial search of all content sources to identify and collect data that may be relevant to a specific legal case. With it, the data set size that is relevant can be reduced before further review by applying text analytics, machine learning and Relevance/predictive coding.

Exchange Online Protection

Exchange Online Protection (EOP) is a SaaS based product from Microsoft that provides enterprise-class reliability and protection against spam and malware within incoming and outgoing messages. The EOP system only scans information that is outbound or inbound: it does not scan internal content. These emails are scanned for malware by an internal/government spam/AV service on Exchange. Emails that are sent from one user to another within the same Office 365 tenant do not flow through EOP.

Microsoft has moved away from many of the traditional techniques employed to detect and intercept malware to focus more on leveraging the significant resources that exist within Office 365 to erect sophisticated barriers against new threat vectors. Known spam/viruses are filtered and not stored and any suspicious incoming emails are quarantined and stored for a specified time, for the end user to read and determine validity. The end user has the ability to release the email to their inbox or delete it. This feature of the service is completely customizable.

Outgoing emails pass through the filter for spam and viruses and are then sent to the recipient. If spam or a virus is suspected an alert is sent to the identified organization administrator to investigate. These emails are not stored on the Microsoft servers at any time.

Emails that cannot be delivered to the specific mailbox server are cached and EOP will continue to attempt delivery of the mail to the recipient/s. Scanning takes place during the transport process as the messages flow through the system.

It should be noted that the spam/malware filtering services provided by EOP are of critical importance to the Province. Given the extraordinarily high volume of attacks posed against the government network (~5-10 million monthly), lack of this type of service would have catastrophic repercussions, particularly given the critical status of the Exchange service to government operations.

Personal Information Flow Table #3 – Exchange Online Protection			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Microsoft filters incoming/outgoing emails through the EOP gateway.*	*Collection*	*26(c)*

2.	*The Province's outgoing emails are filtered through the EOP gateway*	*Disclosure*	*33.1(1)(p) / 33.2(c)*
Note: All disclosures by Province and collections by Microsoft are of encrypted data only. The Province retains the only encryption key and is thus the only party able to view personal information.			

Skype for Business

Skype for Business (SfB) Online users interact with this service through the SfB client and Web browsers. SfB voice and video traffic is transmitted using Secure Realtime Transport Protocol ("SRTP"). SfB does not store customer calls or messages but can be configured (by system or by the user) to store calls and messages in Exchange Online.

SfB stores customer content in a variety of places within the Canadian GEO:

- User and account information, which includes connection endpoints, tenant IDs, dial plans, roaming settings, presence state, contact lists, are stored in the SfB Online Active Directory servers, as well as in various SfB Online database servers. Contact lists are stored in the user's Exchange Online mailbox if the user is enabled for both products, or on SfB Online servers if the user is not. SfB Online database servers are not physically partitioned per tenant, but multi-tenancy is enforced through Role Based Access Control (RBAC). This is assessed in STRA RS3263.
- Meeting content, such as content that users upload during SfB Online meetings, is stored on Distributed File System ("DFS") shares. This content can also be archived in Exchange, provided archiving is enabled by the system or the user (as determined by the Province). The DFS shares are not partitioned "per tenant" but the content is secured with ACLs and multi-tenancy is enforced through RBAC. This is assessed in STRA RS3263.
- Call detail records, which consists of activity history, such as call history, Instant Messaging ("IM") sessions, application sharing and IM history, can also be stored in Exchange Online, but most call detail records are temporarily stored on call detail record ("CDR") servers. Content is not partitioned per tenant, but multi-tenancy is enforced through RBAC.

Personal Information Flow Table #4 – Skype for Business			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	User information is imported into SfB from Active Directory (AD) Government is disclosing Active Directory (AD) elements to SfB	Collection Disclosure	26(c), 27(1)(b) 33.2(c)

	Free/busy calendar info (point in time only, not stored) User (opts to) upload photo for purposes of employee/workplace engagement and familiarity	Collection Collection and Disclosure	26(c), 27(1)(b) 26(c) 33.2(a)/(c)
2.	SfB collects information from users directly: o when a user is not at their computer for x # of minutes; o when a user does not want to be disturbed; o when a user is adding contact information that is specific; o when a user types in a status note.	Collection Disclosure	26(c) 33.2(a)/(c)
3.	SfB users search the Skype directory and add other users to their contacts list	Use	32(a)
4.	SfB users add external (outside of BC Gov't) contacts to their contacts list	Collection	26(c)
5.	User activity logs are created when users communicate with each other using SfB	Collection	26(c)
6.	SfB users may share information in Skype meetings	Disclosure	Only when authorized to do so under section 33.1 of FOIPPA. This will be assessed via a PIA CIRMO16001
7.	Microsoft Engineer accesses customer content for the purpose of remedying a technical issue.	Disclosure	33.1(1)(p)
8.	*SfB logs and other data are stored on the Province's tenancy within Office365.*	*Disclosure (by Province)*	*33.2(c)*
Note: All disclosures by Province and collections by Microsoft are of encrypted data only. The Province retains the only encryption key and is thus the only party able to view personal information.			

SharePoint Online

SharePoint Online users interact with that service through Web browsers and OneDrive for Business clients.

SharePoint Online stores objects as abstracted code within application databases. When a user uploads a file, that file is disassembled and translated into application code and stored in multiple tables across multiple databases. If a user/hacker was able to gain direct access to the storage containing the data, the content is not interpretable to a human or any system other than SharePoint Online.

All SharePoint Online resources are secured by the authorization code and RBAC policy, including within a tenancy. By default, the resources for Tenant A are limited to identities authenticated against Tenant A's authentication provider. Such identities involve only users from Tenant A. Data belonging to Tenant A cannot in any way be obtained by users in Tenant B, unless explicitly approved and provided by Tenant A.

A tenant level property that specifies the authentication provider (which is the tenant specific Active Directory) is written once and cannot be changed once set. Once an authentication provider tenant property has been set for a tenant, it cannot be changed using any APIs exposed to a tenant.

A unique "SubscriptionId" is also used for each tenant. The SubscriptionId property is written once and cannot be changed. Once a site is assigned to a tenant, it cannot be moved to a different tenant later using the content store API. The SubscriptionId is also the key that is used to create the security scope for the authentication provider and is tied to the tenant.

SharePoint Online uses SQL Server and Azure storage for data storage. At the SQL level, the partition key for the content store is "SiteId". When running a SQL query, SharePoint Online uses a SiteId that has been verified as part of a tenant-level SubscriptionId check.

SharePoint Online stores file binary "blobs" (e.g., the file streams) in Azure. Each SharePoint Online farm has its own Azure account and all of the blobs saved in Azure are encrypted individually using a key that is stored in the SQL content store. The encryption key is not exposed directly to the end user, and is protected in code by the authorization layer.

Finally, SharePoint Online has real-time monitoring in place to detect when an HTTP request reads or writes data for more than one tenant. It does this by tracking the SubscriptionId of the request identity against the SubscriptionId of the resource being accessed.

Document Records Management: This technology in Office 365 enables clients to control how long to keep items in users' SharePoint sites and define what action to take on items that have reached a certain age.

eDiscovery, Advanced eDiscovery and/or Data Loss Prevention: Microsoft provides a tool characterized as an "eDiscovery Center" for SharePoint. This tool can be delegated to specialist client users (e.g. compliance officers, human resources personnel) to search for and preserve records for litigation purposes. eDiscovery uses the content indexes created by SharePoint Search. Authorized client users can perform an eDiscovery search by selecting the mailboxes, and then specifying search criteria such as keywords, start and end dates, sender and recipient addresses, and message types. The function can also be used to proactively identify client-defined sensitive information for data loss prevention purposes. After the search is complete, authorized users can then:

- Obtain an estimate of the total size and number of items that will be returned by the search, based on the specified criteria;
- Preview search results (messages returned from each mailbox searched are displayed);
- Copy search results (copy messages to a discovery mailbox); and
- Export search results to a PST file.

Advanced eDiscovery builds on the eDiscovery capabilities by enabling an initial search of all content sources to identify and collect data that may be relevant to a specific legal case. With it, the data set size that is relevant can be reduced before further review by applying text analytics, machine learning and Relevance/predictive coding.

Personal Information Flow Table #5 - SharePoint			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*SharePoint Online sites are created within Province's tenancy within Microsoft's servers*	*Disclosure (by Province)*	*33.2(c)*
2.	*SharePoint Online sites are used for work units to collaborate. Collaboration could include: conversations, surveys, documents (and revision), and work histories respecting a project.*	*Disclosure*	*33.2(a)/(c)*
3.	*Microsoft stores all data resting on a SharePoint Online site*	*Collection*	*26(c)*
Note: All disclosures by Province and collections by Microsoft are of encrypted data only. The Province retains the only encryption key and is thus the only party able to view personal information.			

Office 365 Compliance Search

Office365 Compliance Search ("Compliance Search") is an enterprise search capability available across an Office365 tenant for use by all users and administrators. Office365 will surface search data based on a user's access permission to content i.e., eDiscovery searches are only available to users allowed to perform eDiscovery processes.

Compliance Search is designed for times when the full-fledged search case management of eDiscovery search isn't required. Compliance Search is ideal for quick searches across content in Office 365. Compliance Search allows the Province to:

- Search all Office 365 data without limits on number of mailboxes or documents;
- Use Keyword Query Language for advanced search;
- Preview search results with hit highlighting;
- Use fine-grained permissions to control what can be searched; and
- Ensure searches include only recent, up-to-date data through Compliance Search functionality.

Office 365 Search uses a tenant separation model that prevents the Search features from:

- Returning query results that contain documents from other tenants;
- Exposing sufficient information in query results that a skilled user could infer information about other tenants;
- Showing schema or settings from another tenant;
- Mixing analytics processing information between tenants or storing results in the wrong tenant; and
- Using dictionary entries from another tenant.

Office 365 Customer Lockbox

In exceptional and rare instances, where a cloud service customer is not able to self-remediate an issue using available resources or with the assistance of a government call centre technician, the user can register a trouble ticket in the service portal to have the problem fixed by Microsoft. The issuance of trouble ticket is the required first step in provisioning access to a Microsoft Engineer through the Customer Lockbox mechanism. The Customer Lockbox process is as follows:

- Automated support and Microsoft support without access have failed to address an issue, thus requiring Microsoft Engineer access. This process is initiated by government;
- The Microsoft Engineer, who has provided multi-factor authentication credentials, submits for dual approvals within Microsoft a request for access which details the purposes, duration (duration is requested by Microsoft Engineer based on scope of work and approved by Province Administrator) and data location for the request;
- Once a Microsoft Engineer's request for access has been approved by Microsoft Managers, government's Office 365 administrators are notified via email that there is a request for

access;

- Government's Office 365 Administrators then have the option of either approving or rejecting the Customer Lockbox request for access. If the Administrators do not respond within 12 hours, the request will expire (by default). Expired requests do not result in access to customer content. If the Administrators approve the request, Microsoft will have access to relevant data for the specified time.
- If the problem is not fixed within the specified time the Microsoft Engineer provided in the original request, the Microsoft Engineer must repeat the approval process outlined above where the fact that they have requested additional time will be carefully scrutinized.
- After a service request has been completed, all access is logged and a detailed record of all activities performed is available to the government.

Use of the Customer Lockbox feature ensures that the Microsoft Engineer does not get access to government's content without government's explicit approval. This process cannot be initiated by Microsoft, and must be initiated through a ticket by government.

Personal Information Flow Table #6 – Customer Lockbox			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Government employee identifies or experiences an issue which cannot be resolved by automated support and requires a Microsoft Engineer to access the employee's mailbox, SharePoint site etc.*	*n/a*	*n/a*
2.	*Government employee initiates a service request with Microsoft. Microsoft Engineer submits a request with both a Microsoft Manager and government Office 365 administrators for access to the Customer Lockbox, which contains only the data required to perform the required troubleshooting.*	*n/a*	*n/a*
3.	*Microsoft Engineer accesses customer content for the purpose of remedying a technical issue. Once the predetermined time limit has expired, the Engineer will be locked out of the Customer Lockbox and cannot access the Customer Lockbox again without receiving approval from both Microsoft and government administrators.*	*Disclosure*	*33.1 (p)(i)(A)*

10. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
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 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*	*Very Low*	*Variable*

		Stored Abroad (LEADS) Act was introduced in February 2015 to a Congressional Committee. This Bill has been put forward by multi-national IT 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 and users of the government systems.* *Microsoft utilizes controls to manage employee access, such as their two-factor authentication and their Customer Lockbox approval process.*	*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-*	*Government will ensure that a contract*	*Low*	*Variable*

	through of privacy requirements from government to service provider.	*with Microsoft supports compliance with FOIPPA.*		
7.	*Sensitive documentation may require additional protection/security provisioning.*	*Azure Rights Management Service (RMS) provides the province the capability of applying easy configuration and enforcement of information protection policies to particularly sensitive data within O365. Government documents are tracked in logs generated by RMS and are accessible by the Province. These logs detail the user who is opening documents and when they are opened (who, when, where, what). This will alert the Province when permissions may need to be altered.* *Azure RMS does not view the Province's content or store the data as part of the information protection process. Azure RMS simply makes the data in a document unreadable to anyone other than authorized users and services:* • *The data is encrypted at the application level and includes a policy that defines the authorized use for that document.* • *When a protected document is used by a legitimate user or it is processed by an authorized service, the data in the document is decrypted and the rights that are defined in the policy are enforced*	*Low*	*Variable*
8.	*Data protection and security is not consistently applied across provincial computers, networks and devices.*	*Intune is an application that will enable provincial device management, application management and content management.* *Intune will allow the province to provide their employees with access to corporate applications, data and resources from virtually anywhere on almost any device,*	*Low*	*Variable*

		while helping to keep corporate information secure. The application itself leverages access control from Azure Active Directory and data protection from Azure Rights Management.		
9.	The policy parameters of "Just in Time and Just Enough Access" services within the Azure fabric are not as explicit as the O365 Customer Lockbox.	*Customer Content (which is where the Province's personal information rests) does not sit in the Azure space.* *Content within the AAD will not include personal information.* *Microsoft is currently working to improve the controls for Azure for enterprise customers.* *The policy parameters of JIT/JEA services are supported by higher level principles and requirements that exist within the IS27001 standards that Microsoft meets, including; Information Security Policy, Human Resources (i.e. training), Asset Management (i.e. asset classification and protection commensurate with sensitivity), Access Control (e.g. least privilege) and logging and monitoring (e.g. use is monitored and audited).*	*Low*	*Variable*

Risk Mitigation Table (risks identified in STRA)				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Part of the Infrastructure service, Azure Active Directory component*	*Only non-personal elements of information will be synced from the Active Directory with the Azure Active Directory.*	*Low*	*Low*

	(AAD) resides in the US.	*Attributes that contain personal information (e.g. home number, personal photo) will not be synced. These are indicated in grey within Appendix A.* *At this time, attributes that are customizable will not contain personal information. If the Province chooses to customize these fields with personal information the attributes will not by synced or will be addressed with government policy (e.g. if an employee may self-populate personal information to synced fields, they will be required to provide consent in compliance with section 30.1 of FOIPPA).*		
2.	*Users will be in control of whether personal information is exposed within their profile.*	*That users can update their profiles themselves is both a risk and a benefit to the individuals. The user will have the ability to not populate fields with personal information, however, OCIO will attempt to ensure that where personal information is likely to appear, that those fields will not be synced with AAD.* *For example, the AD customizable fields do not need to be synced with AAD. However, if the OCIO operationalizes the customizable fields within the AD to be synced with AAD a PIA Initiative Update would be required.* *Individuals will need to be informed of what information is appropriate/expected in open profile fields. The OCIO service owner will develop communications strategy to mitigate this risk.*	*Low*	*Low*

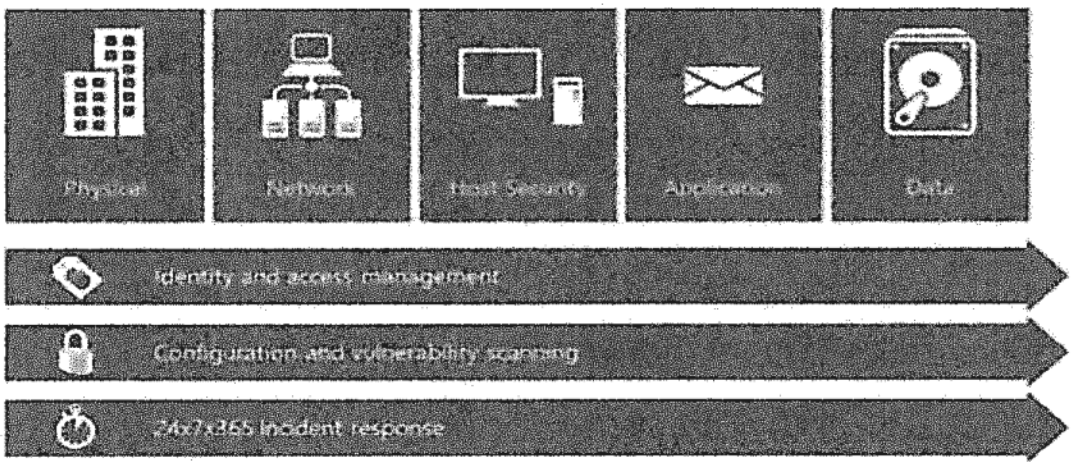
3.	*If user management is not appropriately standardized by the OCIO, especially around transfers, user content and access may not be appropriately managed.*	*Microsoft Cloud Services provides the controls to meet this requirement, however, it does not remove the need for the service owner to operationalize the necessary solution.* *The OCIO service owner will be responsible for implementing the standardized business process and will coordinate with the Privacy, Compliance and Training Branch to ensure the solution meets privacy requirements.*	*Low*	*Variable*
4.	*Appropriate records management may not occur when users transfer or leave govt, or contractors/partners are given access if standards and policy are not reviewed. This is a particular concern regarding shared drives.*	*Individual program areas are responsible for managing their local access permissions, and will continue to do so. Individual program areas are also reminded of this requirement during the completion of program specific PIAs.* *The PSA has provided a guidance document for off-boarding employees/access contractors, which includes removing access permissions. It is a Ministry's responsibility to ensure adherence to this policy. The Corporate Information and Records Management Office may examine adherence to off-boarding policy as part of an audit or compliance review activity.*	*Low*	*Variable*
5.	*There is a global setting that allows sites (global or per site) to be shareable without authentication. This could open the door for unauthorized sharing of personal information, if not managed properly.*	*Currently, unauthenticated access is not permitted and this practice will continue barring further evaluation.*	*Low*	*Low*

6.	*Users could store documents on home desktops when using the service.*	*This is a current risk that exists and is managed through corporate guidance (i.e. the Appropriate Use Policy) directing employees to store all records on shared drives or within approved government information systems.*	*Low*	*Variable*
7.	*Content and location of Azure Rights Management Service (RMS) logs* *Azure RMS reports and logs may be stored outside of Canada. There is a possibility that these reports could contain personal information (e.g. the document file name may contain personal information)*	*The practice of naming records such that they contain personal information is a practice that is generally not encouraged across government. Where at all possible personal information should be left out of document names, or otherwise obscured or de-identified.* *This is a standard message that is provided as a part of government's privacy training, delivered by regularly, or by request.*	*Low*	*Low*
8.	*The current service iteration of Intune is not sufficiently mature/developed to support all of Government's needs*	*Decision to implement this service, which rests with the OCIO, will not be invoked until the OCIO is satisfied that the service will meet its operational needs, and will meet privacy and security needs.*	*Low*	*Low*

11. 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



An example of Defense-in-Depth

Microsoft's defense-in-depth security strategy ensures that controls are layered in order to detect, prevent and mitigate security risks in the physical, logical and data layers of the service. This is intended to ensure, in the event of the failure of one security measure, that compensating controls maintain data security. How these safeguards are operationalized within the O365 context have been assessed in multiple Security Threat Risk Assessments (STRA).

At a conceptual level, the Microsoft Cloud Services PIA (#MTICS14058) discussed in detail 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 default technology and operational procedures and policies as well as customer controls available for customization to the specific needs of the organization.

At a high level, privacy-enhanced security controls include:

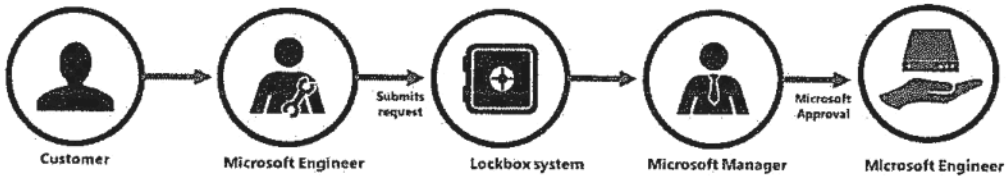
- Auditing all operator/administrator access and actions;
- Zero standing permission for administrators in the service;
- "Just-In-Time (JIT) access and elevation", which enforces access control through multiple levels of approval with limited and time-bound authorization; Segregation of the employee email environment from the production access environment (i.e. secured, segregated multi-tenancy);
- Mandatory background checks for high privilege access. These checks are a highly scrutinized, manual-approval process. Additionally, Microsoft conducts background verification checks of certain operations personnel and limits access to applications,

systems, and network infrastructure in proportion to the level of background verification;

- Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services;
- Tenant isolation based on the Azure Active Directory authorization and role-based access controls to prevent data leakage or unauthorized access across tenants and prevents the actions of one tenant from adversely affecting the service for another tenant;
- SharePoint Online provides data isolation mechanisms at the storage level; and
- Microsoft will promptly notify customers of a security incident (unlawful access to any customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure or alteration of client data), will investigate the incident and provide the client with detailed information and will take reasonable steps to mitigate the effects and to minimize damage.

Microsoft Customer Lockbox

Lockbox



Scoped, least privileged access
Just-in-time access for limited duration
Audit logs for all access

The Customer Lockbox is one aspect of the O365 suite of security and privacy controls that ensures robust access control and thus, privacy protection. Though this is discussed in the Microsoft Cloud Services PIA, it has been highlighted here given its significance.

Microsoft personnel do not have standing access to any service operation. All access is obtained through an access control technology called Customer Lockbox. Customer Lockbox enforces access control through multiple levels of approval in order to provide "just-in-time" access with limited and time-bound authorization. No Microsoft personnel hold standing access to customer content.

If Microsoft requires access to Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content (including the files stored within that site), or OneDrive for Business content in order to perform a troubleshooting operation at the request of the customer, then Customer Lockbox will require Microsoft to request and obtain Customer's approval before Microsoft is able to obtain this access. If Customer does not reject or approve the request within 12 hours, then the request will expire automatically without Microsoft obtaining access to this Customer Data. If Customer approves the request, then Microsoft's access to this Customer Data will be logged and auditable and revoked automatically after the time assigned to complete the troubleshooting operation expires.

Law Enforcement Disclosures

In addition to measures described above in order to avoid compliance with a foreign demand for disclosure, Microsoft also has a stated policy with respect to all its software and services (including Office 365), which is as follows:

- Microsoft does not provide any government with direct and unfettered access to client data. A relevant legal demand is required.
- If a government wants client data, including for national security purposes, it must follow applicable legal process (i.e. serve a court order or subpoena for content or account information).
- Microsoft only responds to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to client data. Aggregate data published by Microsoft indicates that only a small fraction —fractions of a percent— of clients have ever been subject to a government demand related to criminal law or national security.
- A Microsoft compliance team reviews each request and is tasked to ensure that such requests are valid and that any data released is limited to that specified in the order.

Part 4 – Accuracy/Correction/Retention of Personal Information

12. 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.

13. 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.

14. If you answered "yes" to question 13, 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.

15. If you answered "yes" to question 13, 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

16. 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.

17. 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.

18. 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 – Next Steps

The process of assessing a program of the size and scope as Microsoft Office 365 requires multiple levels of review and assessment. The conceptual PIA (MTICS 15048) assessed whether or not there were any major barriers that would preclude continuing negotiations and business case development with Microsoft. This PIA sets out in more detail the measures required in order to ensure that Office 365 could be procured and offered to government in a lawful manner. The next

steps require government to finalize the policy and procedural obligations as set out in this PIA. Furthermore, government must engage in assessment that reviews the operational, or implementation parameters of some of the Office 365 services (e.g. SharePoint Online and Skype for Business).

This PIA has demonstrated that Microsoft can offer their services in a lawful manner. The remaining work to be done will demonstrate that Microsoft services can be *consumed* in a lawful manner – this means that government will ensure that the customer-activated controls are appropriately invoked; that any required policies, procedures training or guidelines are developed; and that any further PIAs that may be required are also completed.

Part 7 – External Review

As a part of the due diligence for assessment of the Microsoft Office 365 services, government submitted this PIA for review and comment to the Office of the Information and Privacy Commissioner (OIPC), along with an in-person briefing.

On July 14th, 2016, government received the first round of comments on this initiative. Attached as Appendix B, is the review of this PIA conducted on behalf of the OIPC by Travis Martin, Ph.D. It provides an overview of the PIA, comment on the cloud services system, access protocols, data storage, and finally, an analysis of any remaining issues across the Microsoft services discussed.

On July 22nd, 2016, government provided the OIPC a response to the received comments. Attached as Appendix C is the government response. This appendix responds to each of the issues raised in the review of the PIA in turn.

Finally, on August 18th, 2016, the OIPC issued a letter to government providing their final remarks on this phase of review of the Microsoft Office 365 initiative and its PIA. This letter is attached as Appendix D.

Part 8 – PLB Comments and Signatures

This PIA is based on a review of the material provided to PLB 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 PLB.

Matt Reed		Jan. 12, 2018
A/Executive Director Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date

Part 9 – Program Area Comments and Signatures

Derek Rutherford Program Owner Executive Director Architecture, Standards and Planning Ministry of Citizens' Services	Signature	June 8, 2018 Date
Ken Prosser Contact Responsible for Security Director, Cybersecurity Intelligence and Investigations Office of the Chief Information Officer Ministry of Technology, Innovation and Citizens' Services	Signature	March 27, 2018. Date
Ian Donaldson Assistant Deputy Minister Ministry of Technology, Innovation and Citizens' Services	Signature	July 30/18 Date

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

PLB 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 PLB or call the Privacy and Access Helpline at 250 356-1851.

Appendix A - All Azure Active Directory Attributes

Service Name	Attribute Name	Comment
3rd Party Applications	givenName	Contains the given name (first name) of the user.
3rd Party Applications	mail	The list of email addresses for a contact.
3rd Party Applications	mailNickName	Alias of the users mailbox.
3rd Party Applications	managedBy	The distinguished name of the user that is assigned to manage this object.
3rd Party Applications	member	The list of users that belong to the group.
3rd Party Applications	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
3rd Party Applications	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
3rd Party Applications	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
3rd Party Applications	sn	This attribute contains the family or last name for a user.
3rd Party Applications	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
3rd Party Applications	accountEnabled	Defines if an account is enabled.
3rd Party Applications	cn	Common name or alias. Most often the prefix of [mail] value.
3rd Party Applications	displayName	A string that represents the name often shown as the friendly name (first name last name).
3rd Party Applications	usageLocation	mechanical property. The user's country. Used for license assignment.
3rd Party Applications	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Azure RMS	mail	The list of email addresses for a contact.
Azure RMS	member	The list of users that belong to the group.
Azure RMS	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Azure RMS	proxyAddresses	mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
Azure RMS	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens.
Azure RMS	securityEnabled	Derived from groupType.
Azure RMS	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Azure RMS	accountEnabled	Defines if an account is enabled.
Azure RMS	cn	Common name or alias. Most often the prefix of [mail] value.

Azure RMS	displayName	A string that represents the name often shown as the friendly name (first name last name).
Azure RMS	usageLocation	mechanical property. The user's country. Used for license assignment.
Azure RMS	userPrincipalName	This UPN is the login ID for the user. Most often the same as [mail] value.
Dynamics CRM	facsimiletelephonenumb	Contains telephone number of the user's business fax machine.
Dynamics CRM	givenName	Contains the given name (first name) of the user.
Dynamics CRM	l	City
Dynamics CRM	managedBy	The distinguished name of the user that is assigned to manage this object.
Dynamics CRM	manager	Contains the distinguished name of the user who is the user's manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager properties set to this distinguished name.
Dynamics CRM	member	The list of users that belong to the group.
Dynamics CRM	mobile	The primary mobile phone number.
Dynamics CRM	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Dynamics CRM	physicalDeliveryOfficeNa	Contains the office location in the user's place of business.
Dynamics CRM	postalCode	The postal or zip code for mail delivery.
Dynamics CRM	preferredLanguage	The preferred written or spoken language for a person.
Dynamics CRM	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
Dynamics CRM	securityEnabled	Derived from groupType
Dynamics CRM	sn	Last Name
Dynamics CRM	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Dynamics CRM	st	State/Province
Dynamics CRM	streetAddress	Street Address
Dynamics CRM	accountEnabled	Defines if an account is enabled.
Dynamics CRM	c	Country abbreviation
Dynamics CRM	cn	Common name or alias. Most often the prefix of [mail] value.
Dynamics CRM	co	Country
Dynamics CRM	company	The user's company name.
Dynamics CRM	countryCode	Specifies the country/region code for the user's language of choice.
Dynamics CRM	description	Contains the description to display for an object.
Dynamics CRM	displayName	A string that represents the name often shown as the friendly name (first name last name).
Dynamics CRM	telephoneNumber	The primary telephone number.

Dynamics CRM	title	Contains the user's job title.
Dynamics CRM	usageLocation	mechanical property. The user's country. Used for license assignment.
Dynamics CRM	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Exchange Hybrid Writeback	msDS-ExternalDirectoryObjectI	Derived from cloudAnchor in Azure AD. This is new in Exchange 2016.
Exchange Hybrid Writeback	msExchArchiveStatus	Online Archive: Enables customers to archive mail.
Exchange Hybrid Writeback	msExchBlockedSendersHash	Filtering: Writes back on-premises filtering and online safe and blocked sender data from clients.
Exchange Hybrid Writeback	msExchSafeRecipientsHash	Filtering: Writes back on-premises filtering and online safe and blocked sender data from clients.
Exchange Hybrid Writeback	msExchSafeSendersHash	Filtering: Writes back on-premises filtering and online safe and blocked sender data from clients.
Exchange Hybrid Writeback	msExchUCVoiceMailSettings	Enable Unified Messaging (UM) - Online voice mail: Used by Microsoft Lync Server integration to indicate to Lync Server on-premises that the user has voice mail in online services.
Exchange Hybrid Writeback	msExchUserHoldPolicies	Litigation Hold: Enables cloud services to determine which users are under Litigation Hold.
Exchange Hybrid Writeback	proxyAddresses	Only the x500 address from Exchange Online is inserted.
Exchange Online	accountEnabled	Defines if an account is enabled.
Exchange Online	assistant	The name of the assistant for an account.
Exchange Online	authOrig	Relationship that indicates that the mailbox for the target object is authorized to send mail to the source object.
Exchange Online	c	Country abbreviation
Exchange Online	cn	Common name or alias. Most often the prefix of [mail] value.
Exchange Online	co	Country
Exchange Online	company	The user's company name.
Exchange Online	countryCode	Specifies the country/region code for the user's language of choice.
Exchange Online	department	The name of the person's (user or contact) department.
Exchange Online	description	Contains the description to display for an object.
Exchange Online	displayName	A string that represents the name often shown as the friendly name (first name last name).
Exchange Online	dLMemRejectPerms	Distribution reject permission list.
Exchange Online	dLMemSubmitPerms	Distribution submit permission list.
Exchange Online	extensionAttribute1	Custom attribute that is defined in the customer on-premises directory.

Exchange Online	extensionAttribute10	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute11	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute13	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute14	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute15	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute2	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute3	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute4	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute5	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute6	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute7	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute8	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute9	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	facsimiletelephonenumb	Contains telephone number of the user's business fax machine.
Exchange Online	givenName	Contains the given name (first name) of the user.
Exchange Online	homePhone	The person's (user or contact) main home telephone number.
Exchange Online	info	This attribute is currently not consumed for groups.
Exchange Online	Initials	Strings of initials of some or all of an individual's names, except the surname(s).
Exchange Online	l	City
Exchange Online	legacyExchangeDN	Distinguished Name from Legacy system
Exchange Online	mailNickname	Alias of the users mailbox.
Exchange Online	manager	Contains the distinguished name of the user who is the user's manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager properties set to this distinguished name.
Exchange Online	managedBy	The distinguished name of the user that is assigned to manage this object.
Exchange Online	member	The list of users that belong to the group.
Exchange Online	mobile	The primary mobile phone number.
Exchange Online	msDS-HABSeniorityIndex	Hierarchical address book
Exchange Online	msDS-PhoneticDisplayName	Phonetic display name of an object. In the absence of a phonetic display name, the existing display name is used.
Exchange Online	msExchArchiveGUID	The GUID of the user's archived mailbox.
Exchange Online	msExchArchiveName	Archive Name
Exchange Online	msExchAssistantName	GUID
Exchange Online	msExchAuditAdmin	Audit Admin Flags
Exchange Online	msExchAuditDelegate	Audit Delegate Flags

Exchange Online	msExchAuditDelegateAd	Audit Delegate Admin Flags
Exchange Online	msExchAuditOwner	Audit Owner Flags
Exchange Online	msExchBlockedSendersH ash	Populated through an upgrade from Business Productivity Online Standard Suite. Not synced from on-premises.
Exchange Online	msExchBypassAudit	True/False
Exchange Online	msExchCoManagedByLin	Group only attribute
Exchange Online	msExchDelegateListLink	Delegates list. User only atrribute
Exchange Online	msExchELCExpirySuspens	Litigation Hold End Date
Exchange Online	msExchELCExpirySuspens	Litigation Hold Start Date
Exchange Online	msExchELCMailboxFlags	Contains Litigation Hold
Exchange Online	msExchEnableModeratio	True/False - Related to O365 Group Moderation
Exchange Online	msExchExtensionCustom	This attribute is currently not consumed by Exchange Online.
Exchange Online	msExchExtensionCustom	This attribute is currently not consumed by Exchange Online.
Exchange Online	msExchExtensionCustom	This attribute is currently not consumed by Exchange Online.
Exchange Online	msExchExtensionCustom	This attribute is currently not consumed by Exchange Online.
Exchange Online	msExchExtensionCustom	This attribute is currently not consumed by Exchange Online.
Exchange Online	msExchHideFromAddress	Indicator to control the visibility of a mail recipient for name resolution.
Exchange Online	msExchImmutableID	GUID
Exchange Online	msExchLitigationHoldDat	Litigation Hold Date
Exchange Online	msExchLitigationHoldOw	Owner of Litigation Hold
Exchange Online	msExchMailboxAuditEna	True/False
Exchange Online	msExchMailboxAuditLog	Numeric
Exchange Online	msExchMailboxGuid	The GUID of the user's mailbox.
Exchange Online	telephoneAssistant	Assistant Phone Number
Exchange Online	telephoneNumber	The primary telephone number.
Exchange Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
Exchange Online	title	Contains the user's job title.
Exchange Online	unauthOrig	Email addresses that cannot send messages to this email address
Exchange Online	usageLocation	mechanical property. The user's country. Used for license assignment.
Exchange Online	msExchModeratedByLink	Set in conjunction with msExchEnableModeration tells you who is the group moderator
Exchange Online	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Exchange Online	msExchModerationFlags	The attribute on the Distribution Group indicates if the auto DL approval feature has been enabled.
Exchange Online	wWWHomePage	Web site
Exchange Online	msExchRecipientDisplayT	Numerical value that signifies the type of recipient
Exchange Online	msExchRecipientTypeDet	Numerical value that signifies the type of recipient

Exchange Online	msExchRemoteRecipientT	Numerical.
Exchange Online	msExchRequireAuthToSe	True/False - When enabled for a distribution list (DL), unauthenticated users are rejected.
Exchange Online	msExchResourceCapacity	Room Capacity
Exchange Online	msExchResourceDisplay	Room Display
Exchange Online	msExchResourceMetaDat	Meta Data associated with the room
Exchange Online	msExchResourceSearchPr	Search properties associated with a room.
Exchange Online	msExchRetentionComme	Retention Comment
Exchange Online	msExchRetentionURL	Retention URL
Exchange Online	msExchSafeRecipientsHash	Populated through an upgrade from Business Productivity Online Standard Suite. Not synced from on-premises.
Exchange Online	msExchSafeSendersHash	Populated through an upgrade from Business Productivity Online Standard Suite. Not synced from on premises.
Exchange Online	msExchSenderHintTransl	Mailtips
Exchange Online	msExchTeamMailboxExpi	Date attribute
Exchange Online	msExchTeamMailboxOwn	GUID List
Exchange Online	msExchTeamMailboxShar	Team mailbox SharePoint URL
Exchange Online	msExchUserHoldPolicies	Litigation Hold allows cloud services to determine which users are under Litigation Hold
Exchange Online	msOrg-IsOrganizational	True/False. Constructed attribute (NOT PART OF IDIR SCHEMA)
Exchange Online	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Exchange Online	oOFReplyToOriginator	True/False. Only applies to distribution lists
Exchange Online	otherFacsimileTelephone	A list of alternative facsimile numbers.
Exchange Online	otherHomePhone	A list of alternative home numbers.
Exchange Online	otherTelephone	A list of alternative office telephone numbers.
Exchange Online	pager	The primary pager number.
Exchange Online	physicalDeliveryOfficeNa	Contains the office location in the user's place of business.
Exchange Online	postalCode	The postal or zip code for mail delivery.
Exchange Online	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
Exchange Online	publicDelegates	This attribute stores the user that was configured as a delegate
Exchange Online	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
Exchange Online	reportToOriginator	True/False. The return path to a primary email address.
Exchange Online	reportToOwner	True/False. The return path to a primary email address.
Exchange Online	securityEnabled	Derived from groupType
Exchange Online	sn	Last Name

Exchange Online	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Exchange Online	st	State/Province
Exchange Online	streetAddress	Street Address
Exchange Online	targetAddress	The TargetAddress property specifies the delivery address to which e-mail for this recipient should be sent. This property is read-only.
Exchange Online	userCertificate	Public key certificate.
Exchange Online	userSMIMECertificates	S/MIME Public Key Certificate
Intune	mail	The list of email addresses for a contact.
Intune	mailnickname	Alias of the users mailbox.
Intune	member	The list of users that belong to the group.
Intune	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Intune	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
Intune	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
Intune	securityEnabled	Derived from groupType
Intune	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Intune	accountEnabled	Defines if an account is enabled.
Intune	c	Country abbreviation
Intune	cn	Common name or alias. Most often the prefix of [mail] value.
Intune	description	Contains the description to display for an object.
Intune	displayName	A string that represents the name often shown as the friendly name (first name last name).
Intune	usageLocation	mechanical property. The user's country. Used for license assignment.
Intune	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Lync Online	facsimiletelephonenumb	Contains telephone number of the user's business fax machine.
Lync Online	accountEnabled	Defines if an account is enabled.
Lync Online	c	Country abbreviation
Lync Online	cn	Common name or alias. Most often the prefix of [mail] value.
Lync Online	co	Country
Lync Online	company	The user's company name.
Lync Online	department	The name of the person's (user or contact) department.
Lync Online	description	Contains the description to display for an object.

Lync Online	displayName	A string that represents the name often shown as the friendly name (first name last name).
Lync Online	givenName	Contains the given name (first name) of the user.
Lync Online	homephone	The person's (user or contact) main home telephone number.
Lync Online	ipPhone	TCP/IP Address of common area phone
Lync Online	l	City
Lync Online	mail	The list of email addresses for a contact.
Lync Online	mailNickname	Alias of the users mailbox.
Lync Online	managedBy	The distinguished name of the user that is assigned to manage this object.
Lync Online	manager	Contains the distinguished name of the user who is the user's manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager properties set to this distinguished name.
Lync Online	member	The list of users that belong to the group.
Lync Online	mobile	The primary mobile phone number.
Lync Online	msExchHideFromAddress	Indicator to control the visibility of a mail recipient for name resolution.
Lync Online	msRTCSIP-	Lync/SfB. Option for the application contact.
Lync Online	msRTCSIP-DeploymentLocator	Lync/SfB - Fully qualified DNS name of the Microsoft Lync Server 2010 deployment, as specified in the authoritative (customer, on-premises) directory.
Lync Online	msRTCSIP-Line	Lync/SfB - The device ID (either the Session Initiation Protocol (SIP) uniform resource identifier (URI) or the TEL URI) of the telephone that the user controls.
Lync Online	msRTCSIP-OptionFlags	Lync/SfB
Lync Online	msRTCSIP-OwnerUrn	Lync/SfB
Lync Online	msRTCSIP-PrimaryUserAddress	Lync/SfB - SIP URI for instant messaging, as specified in the authoritative (customer, on-premise) directory.
Lync Online	msRTCSIP-UserEnabled	Lync/SfB - True/False - Indicates whether the user is currently enabled for SIP instant messaging, as specified in the authoritative (customer, on-premises) directory.
Lync Online	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Lync Online	otherTelephone	A list of alternative office telephone numbers.
Lync Online	physicalDeliveryOfficeNa	Contains the office location in the user's place of business.
Lync Online	postalCode	The postal or zip code for mail delivery.
Lync Online	preferredLanguage	The preferred written or spoken language for a person.
Lync Online	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
Lync Online	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.

Lync Online	securityEnabled	Derived from groupType
Lync Online	sn	Last Name
Lync Online	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Lync Online	st	State/Province
Lync Online	streetAddress	Street Address
Lync Online	telephoneNumber	The primary telephone number.
Lync Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
Lync Online	title	Contains the user's job title.
Lync Online	usageLocation	mechanical property. The user's country. Used for license assignment.
Lync Online	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Lync Online	wWWHomePage	Web site
Office 365 ProPlus	accountEnabled	Defines if an account is enabled.
Office 365 ProPlus	cn	Common name or alias. Most often the prefix of [mail] value.
Office 365 ProPlus	displayName	A string that represents the name often shown as the friendly name (first name last name).
Office 365 ProPlus	usageLocation	mechanical property. The user's country. Used for license assignment.
Office 365 ProPlus	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Office 365 ProPlus	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Office 365 ProPlus	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
Office 365 ProPlus	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
SharePoint Online	accountEnabled	Defines if an account is enabled.
SharePoint Online	authOrig	Relationship that indicates that the mailbox for the target object is authorized to send mail to the source object.
SharePoint Online	c	Country abbreviation
SharePoint Online	cn	Common name or alias. Most often the prefix of [mail] value.
SharePoint Online	co	Country
SharePoint Online	company	The user's company name.
SharePoint Online	countryCode	Specifies the country/region code for the user's language of choice.
SharePoint Online	department	The name of the person's (user or contact) department.
SharePoint Online	description	Contains the description to display for an object.
SharePoint Online	displayName	A string that represents the name often shown as the friendly name (first name last name).

SharePoint Online	dLMemRejectPerms	Distribution reject permission list.
SharePoint Online	dLMemSubmitPerms	Distribution submit permission list.
SharePoint Online	extensionAttribute1	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute10	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute11	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute13	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute14	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute15	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute2	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute3	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute4	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	telephoneAssistant	Assistant Phone Number
SharePoint Online	telephoneNumber	The primary telephone number.
SharePoint Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
SharePoint Online	title	Contains the user's job title.
SharePoint Online	unauthOrig	Email addresses that cannot send messages to this email address
SharePoint Online	usageLocation	mechanical property. The user's country. Used for license assignment.
SharePoint Online	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
SharePoint Online	wWWHomePage	Web site
SharePoint Online	extensionAttribute5	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute6	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute7	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute8	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute9	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	facsimiletelephonenumb	Contains telephone number of the user's business fax machine.
SharePoint Online	givenName	Contains the given name (first name) of the user.
SharePoint Online	hideDLMembership	True/False. Hide distribution list.
SharePoint Online	homephone	The person's (user or contact) main home telephone number.
SharePoint Online	info	"Notes" field on "Telephone" tab of ADUC.
SharePoint Online	initials	Strings of initials of some or all of an individual's names, except the surname(s).
SharePoint Online	ipPhone	TCP/IP Address of common area phone
SharePoint Online	l	City
SharePoint Online	mail	The list of email addresses for a contact.
SharePoint Online	mailnickname	Alias of the users mailbox.
SharePoint Online	managedBy	The distinguished name of the user that is assigned to manage this object.

SharePoint Online	manager	Contains the distinguished name of the user who is the user's manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager properties set to this distinguished name.
SharePoint Online	member	The list of users that belong to the group.
SharePoint Online	middleName	Additional names for a person (user or contact), for example, middle name, patronymic, matronymic, or other names.
SharePoint Online	mobile	The primary mobile phone number.
SharePoint Online	msExchTeamMailboxExpi	Date attribute
SharePoint Online	msExchTeamMailboxOwn	GUID List
SharePoint Online	msExchTeamMailboxShar	GUID. Who linked the mailbox to a SharePoint URL
SharePoint Online	msExchTeamMailboxShar	Team mailbox SharePoint URL
SharePoint Online	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
SharePoint Online	oOFReplyToOriginator	True/False. Only applies to distribution lists
SharePoint Online	otherFacsimileTelephone	A list of alternative facsimile numbers.
SharePoint Online	otherHomePhone	A list of alternative home numbers.
SharePoint Online	otherIpPhone	A list of alternative TCP/IP addresses for the telephone.
SharePoint Online	otherMobile	A list of alternative mobile numbers.
SharePoint Online	otherPager	A list of alternative pager numbers.
SharePoint Online	otherTelephone	A list of alternative office telephone numbers.
SharePoint Online	pager	The primary pager number.
SharePoint Online	physicalDeliveryOfficeNa	Contains the office location in the user's place of business.
SharePoint Online	postalCode	The postal or zip code for mail delivery.
SharePoint Online	postOfficeBox	Postal box identifiers that a postal service uses when a customer arranges to receive mail at a box on the premises of the postal service.
SharePoint Online	preferredLanguage	The preferred written or spoken language for a person.
SharePoint Online	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
SharePoint Online	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
SharePoint Online	reportToOriginator	True/False. The return path to a primary email address.
SharePoint Online	reportToOwner	True/False. The return path to a primary email address.
SharePoint Online	securityEnabled	Derived from groupType
SharePoint Online	sn	Last Name
SharePoint Online	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.

SharePoint Online	st	State/Province
SharePoint Online	streetAddress	Street Address
SharePoint Online	targetAddress	The TargetAddress property specifies the delivery address to which e-mail for this recipient should be sent. This property is read-only.
SharePoint Online	url	The list of alternative web pages.

Page 152 of 183 to/à Page 162 of 183

Withheld pursuant to/removed as

s.3

Privacy Impact Assessment for
Exchange Online Protection (EOP)
PIA#*MTICS16056*

Why do I need to do a PIA?
Section 69 (5) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a ministry to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Section 69 (5.1) requires the head to submit the PIA to the minister responsible for FOIPPA for review, during the development of any new system, project, program or activity, or proposed enactment, or when making changes to an existing one. The Privacy, Compliance and Training Branch (PCT) is the representative of the Minister for these purposes. Ministries must submit PIAs to PCT at pia.intake@gov.bc.ca for review and comment prior to implementation of any initiative. If you have any questions, please call the Privacy and Access Helpline (250 356-1851) for a privacy advisor. Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?
Ministries still need to complete Part 1 of the PIA and submit it, along with the signatures pages, to PCT even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Ministry:	Technology, Innovation and Citizens' Services		
PIA Drafter:	Sonya Miles		
Email:	Sonya.Miles@gov.bc.ca	Phone:	**250-953-6202**
Program Manager:	**KaYee Miwa**		
Email:	KaYee.Miwa@gov.b.ca	Phone:	**250-952-7726**

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

The government of British Columbia (BC) is considering the adoption of Microsoft Cloud Services with an in-Canada data residency option for the delivery of IT services to the BC public service. Microsoft Cloud Services in Canada provides an ideal opportunity for modernization, increased agility and to dramatically improve information security and privacy, all while lowering the overall cost and complexity of the Province's information technology services.

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.

The state-of-the-market information technology offerings will provide government with a strategic opportunity to achieve better outcomes for the province through:

- Industrial Grade Security;

- Greater Agility and Service Modernization; and
- Lower Costs through Shared Infrastructure and Converged Communications Technologies.

s.13

As part of the Microsoft Cloud Services they are offering Exchange Online Protection (EOP). This service would allow government to replace the existing custom email filtering service.

Exchange Online Protection (EOP)

Exchange Online Protection is the enterprise-class spam and malware filtering service offered in conjunction with Exchange Online. EOP can utilize layers of protection features deployed across a global network of datacentres, simplifying the administration of messaging environments; however, for the purposes of the BC Government, EOP will be deployed through only Canadian datacentres.

2. Scope of this PIA

The scope of this PIA is centred on government's purchase of EOP from the Microsoft Cloud Services for government use through data resident, Canadian datacentres. EOP is included with government's E3 licenses agreement for Exchange Service.

EOP is a Software as a Service (SaaS) based product from Microsoft that provides enterprise-class reliability and protection against spam and malware. Microsoft has made big strides building out the service in order to reach feature parity with other market leaders.

EOP utilizes layers of protection features that can be deployed across a global network of datacentres, simplifying the administration of messaging environments.

Microsoft have moved away from many of the traditional techniques employed to detect and intercept malware to focus more on leveraging the huge resources that exist within Office 365 to erect even-more sophisticated barriers against new threat vectors.

EOP is positioned within the Leaders Quadrant of Gartner's 2015 Magic Quadrant for Secure Email.

3. Related Privacy Impact Assessments

Microsoft Cloud Services – Phase II, PIA #MTICS16024

Exchange Online Protection – STRA #RS3355

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

4. Elements of Information or Data

Email information collected, used and disclosed by the Microsoft Exchange Online Protection (EOP) filtering Solution includes:

- Quarantined Information [1](this is only kept while in quarantine state, once message is released the information is deleted from system):
    - Message status:
        - Type
        - Expires
    - Message details:
        - Sender
        - Subject
        - Received
        - Size
    - Message Header

  Note: quarantined information is encrypted and does not at any time include the content within the body of a message

- Routing Information (metadata captured in logs for 90 days and then deleted from server. The content of the email is not kept on the server. These logs are used for troubleshooting purposes only.):
    - Message ID
    - Received Date
    - Sender Address
    - Recipient Address
    - To IP (destination address)
    - From IP (source address)

[1] Quarantined information refers to an Email that has been classified as spam and routed to a hosted quarantine area within Office 365 for evaluation by an Administrator or the end user.

- Subject
- Status
- Size

Note: Security Investigations will have the ability to export the logs to be kept on their On-Premise if required.

If personal information **is** involved in your initiative, please continue to the next page to complete your PIA.

If **no** personal information is involved, please submit Parts 1, 6, and 7 unsigned to PLB at pia.intake@gov.bc.ca. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

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, which is: 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 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 compliance with FOIPPA.

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.

Law Enforcement Disclosure

Microsoft will agree not to disclose Customer Data to law enforcement agencies unless required by law. Microsoft will attempt to redirect any law enforcement requests to the customer and, in doing so, may provide basic contact information to the law enforcement agency. If compelled to disclose

Customer Data to law enforcement, Microsoft agrees to use commercially reasonable efforts to notify the Province in advance of a disclosure and provide a copy of the demand, unless legally prohibited from doing so.

Storage or Access Outside of Canada

Microsoft's Canadian datacentres are located in Quebec City and Toronto. These facilities are designed to run 24x7x365 and employ a variety of measures to minimize the possibility of power failures, physical intrusions and network outages. Data is replicated three times within the primary datacentre with a fourth copy provided from the secondary Canadian datacentre.

Across its business, Microsoft stores Customer Data at rest within certain major geographic areas (a "GEO"). Canada has been defined as a "GEO", meaning that for government's purposes, all customer content will be resident within the Canadian GEO.

All personal information will be held within Microsoft's Canadian datacentres and will not be accessible outside of Canada unless explicitly permitted by the customer using mechanisms such as the Office 365 Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with customer consent, effect temporary movement to another geo-location to ensure customer services and data are not lost.

A decision remains regarding the network connection used between the Province and Microsoft's Canadian datacentres. The Province can choose to use a general internet connection, or to implement a direct connection called ExpressRoute. Given the Province is unable to dictate where the network traffic gets routed across the internet, the preferred solution would be to use ExpressRoute (a dedicated secure channel). It is possible that depending on the provider, there may be a situation where, if the primary link across Canada fails, the secondary link may route traffic through US based facilities. In any case, the traffic is fully encrypted and so exposure potential is minimal.

The ExpressRoute service is provided by Bell and while this service may subsequently be available through other vendors, in each case they are required by Microsoft to meet specific criteria for the operational delivery of the service.

The Province will impose terms on the connectivity contract with such primary contractors that are in compliance with privacy, security and confidentiality requirements and furthermore obligate the contractor to obligate sub-contractors, such as Equinix, to also comply with those terms. The primary contractor with which the Province holds a legal relationship, will be fully responsible for compliance.

In this instance the sub-contracted company named (Equinix) has affirmed they have no access to customer data (at rest or in transit) and have indicated that this is made clear in their legal terms to all customers in their standard MCA (Master Country Agreements) and GTC (Global Terms and Conditions).

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
If you have answered "yes" to all three questions, please contact a PLB Privacy Advisor to discuss the requirements of a data-linking initiative.	

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. Primary connectivity to the Microsoft datacentre will be through Canadian paths. 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, that the flow of personal information between Microsoft and the Province will be conducted under the following authorities for collection and disclosure:

- 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), STRARS3262 and discussed at a high-level in Part 3 of this PIA substantiate that Microsoft can only access customer content through Customer Lockbox.

Exchange Online Protection

Exchange Online Protection (EOP) is a SaaS based product from Microsoft that provides enterprise-class reliability and protection against spam and malware within incoming and outgoing messages. The EOP system only scans information that is outbound or inbound: it does not scan internal content. These emails are scanned for malware by an internal/government spam/AV service on Exchange. Emails that are sent from one user to another within the same Office 365 tenant do not flow through EOP. All data within Office 365, when at rest, is encrypted at all times. The Province retains the encryption key and is thus the only party able to view the personal information. All messages being routed through EOP is protected by Transport Layer Security (TLS) encryption. [2]

Microsoft has moved away from many of the traditional techniques employed to detect and intercept malware to focus more on leveraging the significant resources that exist within Office 365 to erect sophisticated barriers against new threat vectors. Known spam/viruses are filtered and not stored and any suspicious incoming emails are quarantined and stored for a specified time, for the end user to read and determine validity. The end user has the ability to release the email to their inbox or delete it. This feature of the service is completely customizable.

Scanning of an incoming email from the internet is done within the Exchange Online Protection (EOP) infrastructure. An incoming message will initially pass through connection filtering, which checks the sender's reputation and inspects the message for malware. The majority of spam is stopped at this point and deleted by EOP. Messages that pass the connection filtering rules will continue through policy filtering, where messages are evaluated against custom transport rules that BC Government administrators create or enforce from a template. Messages that have successfully passed this step continue on to content filtering (SPAM protection layer), where content is checked for terminology or properties common to spam. A message determined to be spam by the content filter can be sent to a user's Junk Email folder or to the quarantine, among other options, which are determined by BC Government administrators. After a message has successfully passed all of these protection layers, it is delivered to the recipient.

The EOP system comes with pre-set rules at the connection filtering and spam filtering layers. BC Government administrators and end users provide input to the scan engines at both layers so that the system 'learns' to distinguish what email message is acceptable to BC Government and what is not.

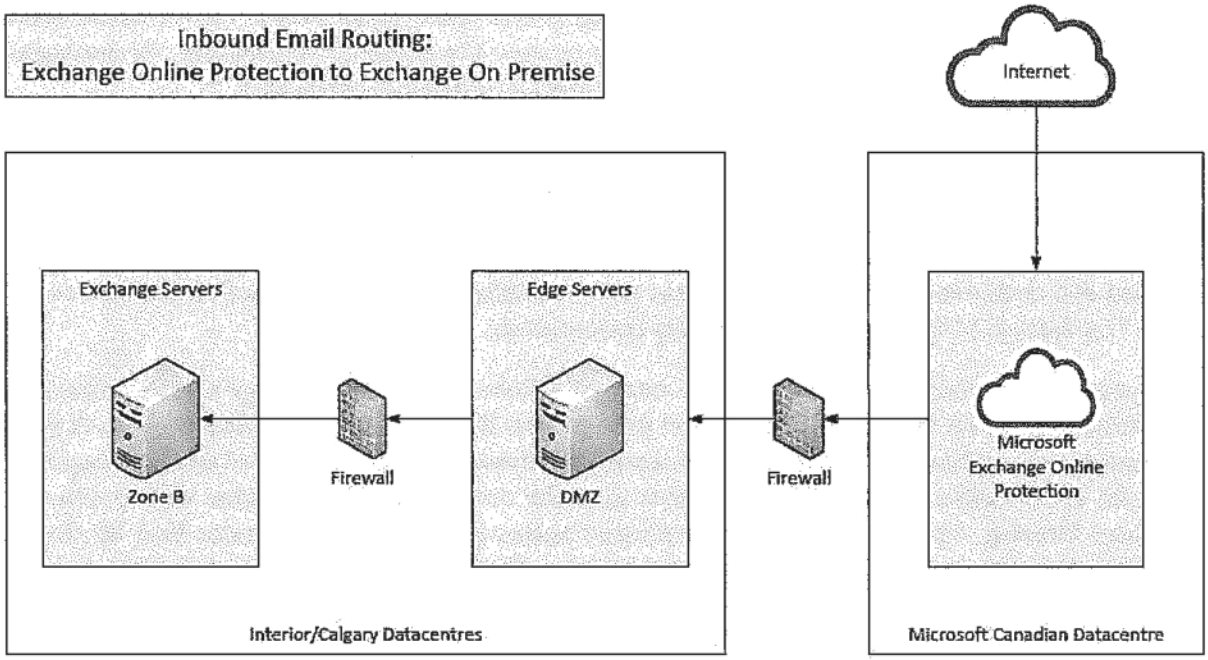
[2] Transport Layer Security (TLS) - service that provides automatic encryption for email messages that are transmitted between source (sender) and destination (receiver).

Outgoing emails pass through the filter for spam and viruses and are then sent to the recipient. If spam or a virus is suspected an alert is sent to the identified organization administrator to investigate. These emails are not stored on the Microsoft servers at any time.

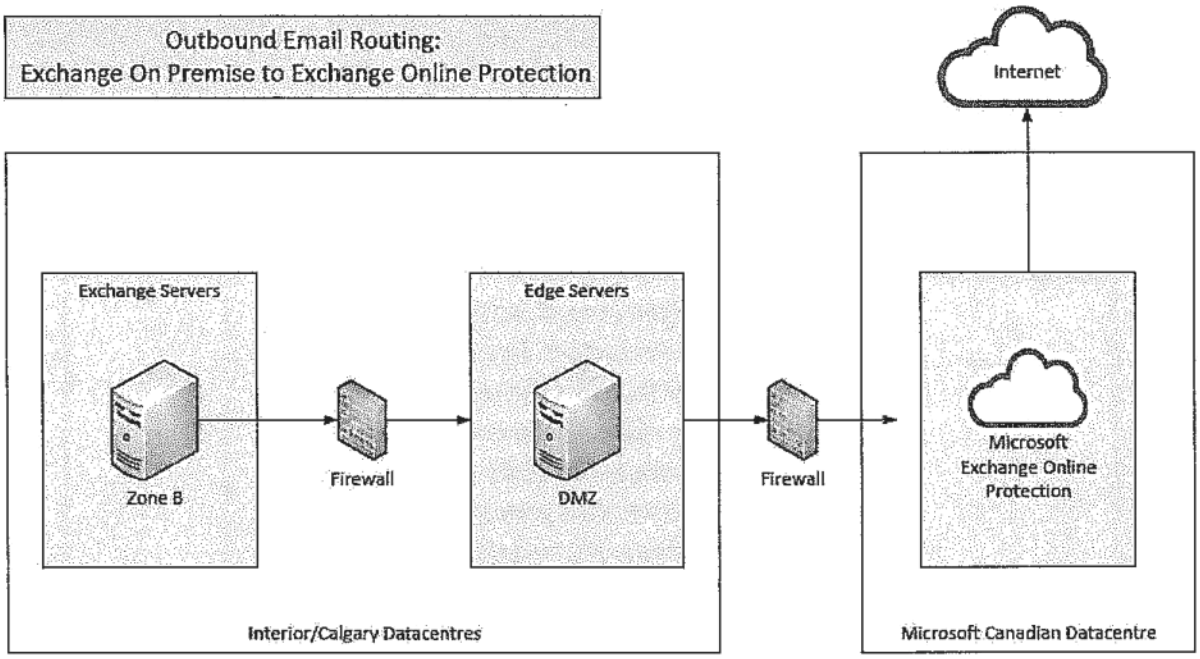
Emails that cannot be delivered to the specific mailbox server are cached and EOP will continue to attempt delivery of the mail to the recipient/s. Scanning takes place during the transport process as the messages flow through the system.

The spam/malware filtering services provided by EOP are of critical importance to the Province. Given the extraordinarily high volume of attacks posed against the government network (~5-10 million monthly), lack of this type of service would have catastrophic repercussions, particularly given the critical status of the Exchange service to government operations.

Inbound



Outbound



Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Microsoft filters incoming/outgoing emails through the EOP gateway.*	*Collection*	*26(c)*
2.	*The Province's outgoing emails are filtered through the EOP gateway*	*Disclosure*	*33.1(1)(p) / 33.2(c)*
Note: All disclosures by Province and collections by Microsoft are of encrypted data only. The Province retains the only encryption key and is thus the only party able to view personal information.			

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
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 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*	*Very Low*	*Variable*

		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 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 and users of the government systems.* *Microsoft utilizes controls to manage employee access, such as their two-factor authentication and their Customer Lockbox approval process.*	*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*	*Low*	*Variable*

		27018 and ISO 27001 among others.		
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. Microsoft's defense-in-depth security strategy ensures that controls are layered in order to detect, prevent and mitigate security risks in the physical, logical and data layers of the service. This is intended to ensure, in the event of the failure of one security measure, that compensating controls maintain data security. How these safeguards are operationalized within the O365 context have been assessed in multiple Security Threat Risk Assessments (STRA).

All of Microsoft's relevant physical security measures and all of Azure and O365 technical security measures are addressed in PIA #MTICS15048. As discussed in detail 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 default technology and operational procedures and policies as well as customer controls available for customization to the specific needs of the organization.

At a high level, privacy-enhanced security controls include:

- Auditing all operator/administrator access and actions;
- Zero standing permission for administrators in the service;
- "Just-In-Time (JIT) access and elevation", which enforces access control through multiple levels of approval with limited and time-bound authorization; Segregation of the employee email environment from the production access environment (i.e. secured, segregated multi-tenancy);
- Mandatory background checks for high privilege access. These checks are a highly scrutinized, manual-approval process. Additionally, Microsoft conducts background verification checks of certain operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification;
- Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services;
- Tenant isolation based on the Azure Active Directory authorization and role-based access controls to prevent data leakage or unauthorized access across tenants and prevents the actions of one tenant from adversely affecting the service for another tenant;
- SharePoint Online provides data isolation mechanisms at the storage level; and
- Microsoft will promptly notify customers of a security incident (unlawful access to any customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure or alteration of client data), will investigate the incident and provide the client with detailed information and will take reasonable steps to mitigate the effects and to minimize damage.

Microsoft personnel do not have standing access to any service operation. All access is obtained through an access control technology called Customer Lockbox. Customer Lockbox enforces access control through multiple levels of approval in order to provide "just-in-time" access with limited and time-bound authorization. No Microsoft personnel hold standing access to customer content.

If Microsoft requires access to Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content (including the files stored within that site), or OneDrive for Business content in order to perform a troubleshooting operation at the request of the customer, then Customer Lockbox will require Microsoft to request and obtain Customer's approval before Microsoft is able to obtain this access. If Customer does not reject or approve the request within 12 hours, then the request will expire automatically without Microsoft obtaining access to this Customer Data. If Customer approves the request, then Microsoft's access to

this Customer Data will be logged and auditable and revoked automatically after the time assigned to complete the troubleshooting operation expires.

Law Enforcement Disclosures

In addition to measures described above in order to avoid compliance with a foreign demand for disclosure, Microsoft also has a stated policy with respect to all its software and services (including Office 365), which is as follows:

- Microsoft does not provide any government with direct and unfettered access to client data. A relevant legal demand is required.
- If a government wants client data, including for national security purposes, it must follow applicable legal process (i.e. serve a court order or subpoena for content or account information).
- Microsoft only responds to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to client data. Aggregate data published by Microsoft indicates that only a small fraction —fractions of a percent— of clients have ever been subject to a government demand related to criminal law or national security.
- A Microsoft compliance team reviews each request and is tasked to ensure that such requests are valid and that any data released is limited to that specified in the order.

12. Please describe the physical security measures related to the initiative (if applicable).

See #11 above

13. Please describe the technical security measures related to the initiative (if applicable).

See #11 above

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

See #11 above

15. 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

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

See #11 above

Part 4 – Accuracy/Correction/Retention of Personal Information

17. 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.

18. 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.

19. 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.

20. 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

21. 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.

Please check this box if the related Information Sharing Agreement (ISA) has been prepared. If you have general questions about preparing an ISA, please contact the Privacy and Access Helpline.	

22. 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.

23. 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.

If yes, please complete the fields in the table below by deleting the descriptive text in the right-hand column and replacing it with your own.

Please ensure Parts 6 and 7 are attached unsigned to your submitted PIA.

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.

Rhianna Begley		Sept. 26, 2016
Senior Privacy Advisor Privacy, Compliance and Training Branch Ministry of Finance	Signature	Date
Matt Reed		Sept. 26, 2016
Senior Director Privacy, Compliance and Training Branch Ministry of Finance	Signature	Date

Part 7 – Program Area Comments and Signatures

Ha Yee Nuda Program Manager Director, Communication and Collaboration Services	Haiyee Nuda Signature	Oct 3 | 2016 Date
Ken Prosser Ministry Contact Responsible for Security Director, Cybersecurity Intelligence & Investigations,	 Signature	Oct. 3, 2016. Date
Chris Haugh Executive Director or equivalent Executive Director Network Communication and Collaboration Services	 Signature	Oct 3, 2016 Date
Ian Bailey Assistant Deputy Minister or Designate	 Signature	Oct 3, 2016 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.