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

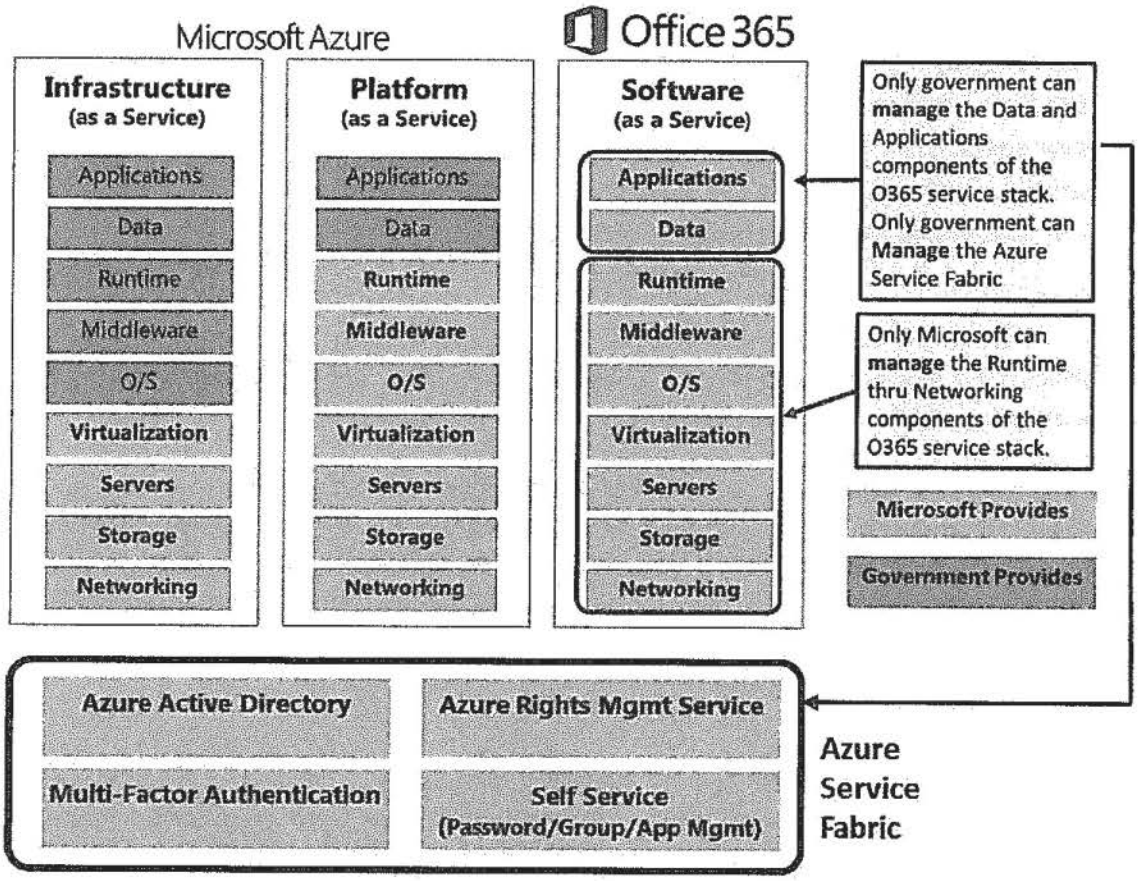
the software and hardware for the purpose of delivering capabilities such as government email services. Following the construction of the system, the same technicians would administer, operate, monitor, patch and evergreen the system.

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*

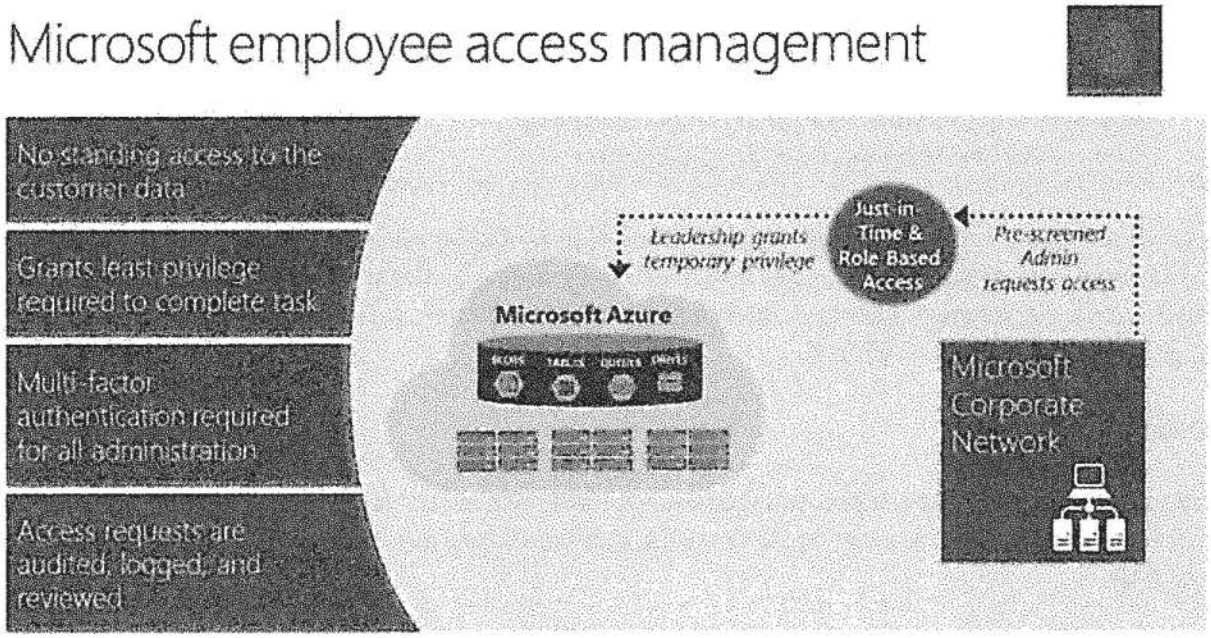
The Province controls the flow of directory information to AAD service. Although there is no personal information present, Microsoft personnel will not have access to this information, except when the Province allows it, through a process referred to in the Azure fabric layer as "Just in Time and Just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

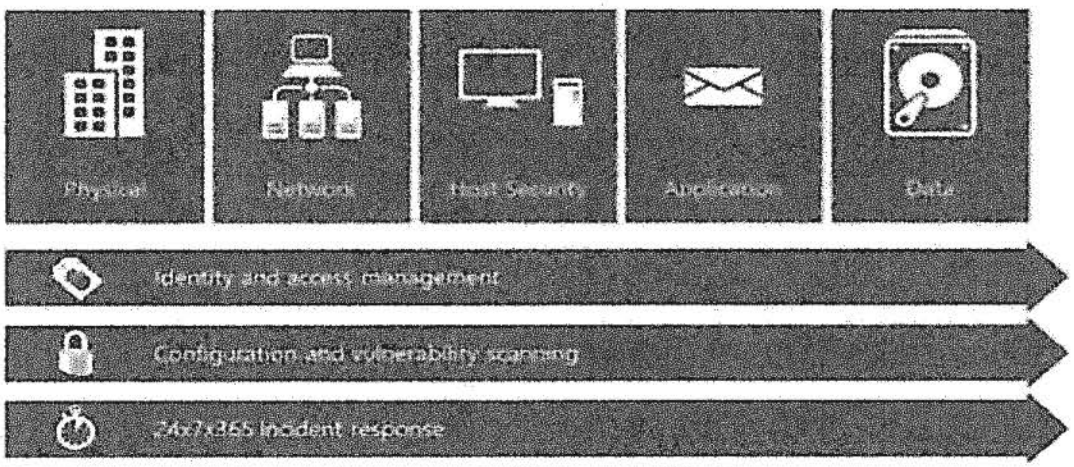
3.	*If user management is not appropriately standardized by the OCIO, especially around transfers, user content and access may not be appropriately managed.*	*Microsoft Cloud Services provides the controls to meet this requirement, however, it does not remove the need for the service owner to operationalize 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:

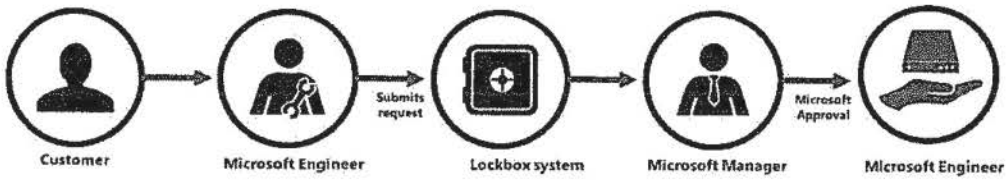
- Auditing all operator/administrator access and actions;
- Zero standing permission for administrators in the service;
- "Just-In-Time (JIT) access and elevation", which enforces access control through multiple levels of approval with limited and time-bound authorization; Segregation of the employee 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 080 to/à Page 099

Withheld pursuant to/removed as

s.3