Privacy Impact Assessment for

Microsoft Cloud Services

PIA#*MTICS15048*

Why do I need to do a PIA?

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

What if my initiative does not include personal information?

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

Part 1 – General

Name of Ministry:	Ministry of Technology, Innovation and Citizens' Services		
PIA Drafter:	**Matt Reed**		
Email:	Matt.Reed@gov.bc.ca	Phone:	**250-514-8870**
Program Manager:	**Sharon Plater**		
Email:	Sharon.Plater@gov.bc.ca	Phone:	**250 356-8660**

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

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 to dramatically improve information security and privacy, all while lowering the overall cost and complexity of the Province's information technology services.

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

Microsoft was the first major cloud provider to adopt the new international standard for cloud privacy, **ISO/IEC 27018, which has been endorsed by Chantal Bernier as the highest standard for cloud privacy.** ISO/IEC 27018 assures enterprise customers that their privacy will be protected in several distinct ways:

- **Customers are in control of their data**. Microsoft adherence to the standard ensures that it only processes personally identifiable information according to the explicit instructions provided by customers (i.e. the BC Government);
- **Customers know what's happening with their data**. Adherence to the standard ensures transparency about policies regarding the return, transfer, and deletion of personal information stored in Microsoft data centres. Microsoft lets customers know where their data is, including any subcontractor access to data;
- **Microsoft provides strong security protection for customer data**. Adherence to ISO 27018 provides a number of important security safeguards. It ensures that there are defined restrictions on how Microsoft handles personal information, including restrictions on its transmission over public networks, storage on transportable media, and proper processes for data recovery and restoration efforts. In addition, the standard ensures that all of the people, including Microsoft's employees, who process personal information must be subject to a confidentiality obligation;
- **Immediate breach notification.** In the event of unauthorized access to facilities, processing equipment or personal information resulting in the loss, disclosure or alteration of this information, Microsoft informs customers about it;
- **Customer data won't be used for advertising or secondary purposes**. Enterprise customers are increasingly expressing concerns about cloud service providers using their data for advertising purposes or secondary purposes without consent. The adoption of this standard reaffirms Microsoft's longstanding commitment to not use enterprise customer data for advertising purposes. In fact, Microsoft does not use customer data at all.
- **Microsoft informs customers about government access to data**. The standard requires that law enforcement requests for disclosure of personal information must be disclosed to customers, unless this disclosure is prohibited by law. Microsoft already adhered to this approach and adoption of the standard reinforces this commitment.

All of these commitments are even more important in the consideration of BC's own privacy compliance obligations. For the government, ISO 27018 will serve to ensure strong privacy protection.

Further, evidence of Microsoft's strength in protecting privacy comes from their recognition as meeting the rigorous standards of European Union (EU) privacy law as they are the only cloud service provider to receive such approval from the Article 29 Working Party, which consists of representatives from each of the 28 European Union data protection authorities (DPAs) and the European Commission, and plays a critical role in global privacy law. In addition, Microsoft has been

unaffected by the recent European Court of Justice (ECJ) Safe Harbor Framework ruling, as it conforms with the EU Model Clauses which are of a higher standard than the Safe Harbor approach.

In addition to its adoption of ISO 27018 and Article 29 Working Party approval, Microsoft Cloud Services are constantly innovating and evolving, adding new controls, certifications and security safeguards to protect customer data. Microsoft has privacy controls in place that allows government to configure exactly who has access to data within its organization. Strict controls and design elements prevent mingling of government data with that of other organizations using Office 365 and from Microsoft data centre staff obtaining access to government data.

The Services

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

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

Cloud computing consists of highly standardized, on-demand IT services provided through a network of data centres. Customer demand for cloud services are in turn aggregated across a large number of customers and across multiple industries to achieve economies of scale and maximize utilization of computing capacity. This cloud model has evolved beyond traditional cloud IT outsourcing as the role of the service provider (in this case Microsoft) has changed to a less active role with respect to the data. No longer are cloud vendors required to actively handle or manage data but rather, serve as the physical custodian/technical processor of the data only.

On June 2nd, 2015, Microsoft announced plans to bring public commercial cloud services to the Canadian marketplace in CY2016. Microsoft's introduction of public cloud services to the Canadian market is a significant opportunity for the BC public sector. These in-Canada services will provide services that meet international security and privacy certifications such as ISO 27001, ISO 27018, PCI, SOC1 and SOC2. This level of compliance coupled with a regular schedule of audits and attestations, results in a suite of in-Canada IT services capable of meeting or exceeding the BC government's privacy and security requirements.

Based on the availability of cloud services in Canada, the government's Office of the Chief Information Officer (OCIO) is considering Microsoft Cloud services (Office 365, Microsoft Azure and CRM) as an important IT modernization strategy for the Province.

2. Scope of this PIA

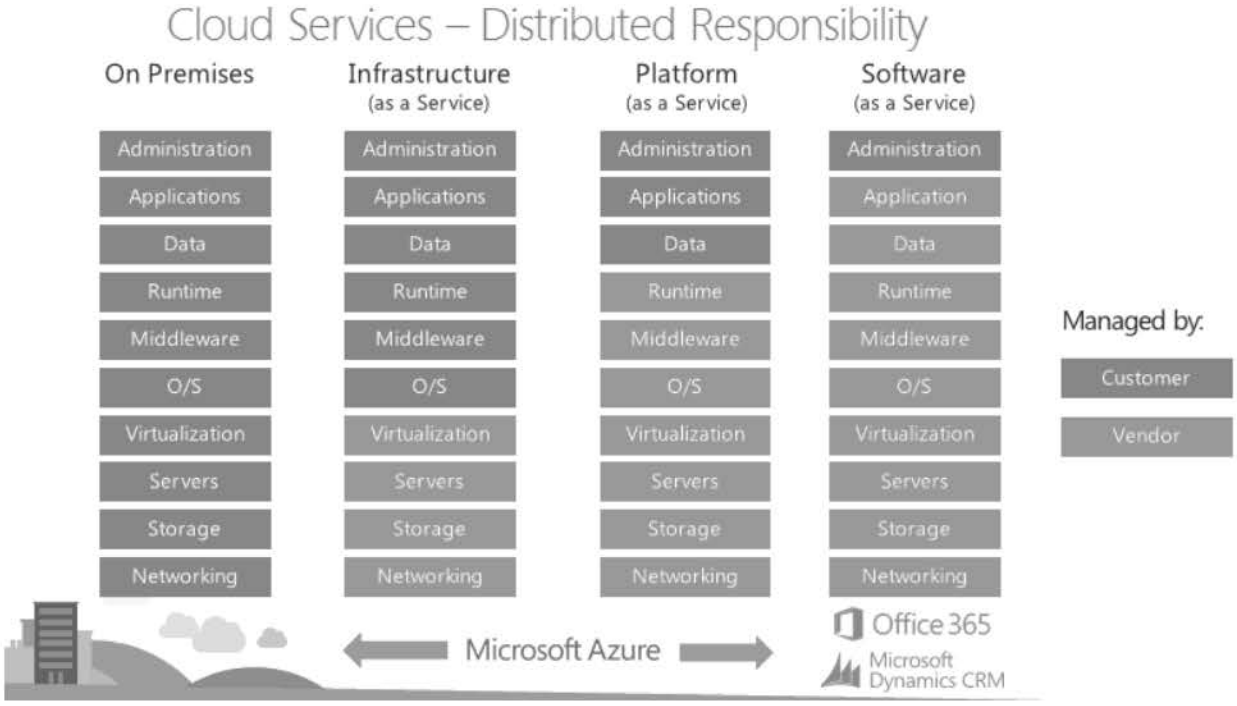
The scope of this conceptual PIA is centred on government's exploration of Microsoft Cloud Services for government use through data resident, Canadian data centres, specifically:

- Microsoft Azure
  - Infrastructure-as-a-Service (IaaS); and
  - Microsoft Azure Platform-as-a-Service (PaaS);
- Microsoft Office 365, a Software-as-a-Service (SaaS) collaboration and productivity suite consisting of:
  - Office Pro Plus, specifically Word, Excel and PowerPoint (client and online versions);
  - Exchange 2016 Online;
  - SharePoint 2016 Online;
  - Skype for Business; and
- Microsoft CRM Online

This PIA does not address government's specific implementations or iterations of Microsoft's service offerings. The intention of this PIA is to establish that the foundational infrastructure and platforms on which government programs will develop are compliant with BC's FOIPPA.

A government program that intends to use Microsoft Cloud Services will still be required to conduct a Privacy Impact Assessment (PIA) in order to ensure that the tools and programs built on Microsoft's foundation are also compliant with BC's FOIPPA.

It should be noted that the Azure portfolio serves as a foundation both for itself and in support of Microsoft's SaaS offerings, such as Office 365 and CRM Online. Therefore, the privacy and security provisions of Azure can be applied to an analysis of Office 365 and CRM Online. At the next level, Microsoft Office365 builds on top of the international standards-based security foundation provided by Azure, with additional controls (like the Customer Lockbox) which are designed to maximize security and ensure privacy of user content. The following diagram is a visual representation of the responsibilities associated with each of Microsoft's services.



3. Related Privacy Impact Assessments

There are no prior BC government privacy impact assessments related to the current PIA.

Government programs that are built on Microsoft Cloud Services, both Infrastructure-as-a-Service and Platform-as-a-Service, will be required to conduct PIAs that address their specific programs, which will reference this PIA.

4. Elements of Information or Data

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

1. Service or System Data

System or Service Data is data about, and generated by, an information system or cloud service. Typical examples of service data include: remaining storage capacity, system health indicators, network traffic volume, bandwidth consumption, all of which are examined or used solely for the purpose of providing the cloud service.

a. System data is not personal information and is distinct from user generated content. System data is used solely for the purpose of providing, operating and maintaining the

service, or diagnosing and/or troubleshooting in the event of problems or system outages.

b. This non-personal data is accessed by authenticated system administrators, service technicians and operators with the appropriate and minimized levels of access. As a rule, technicians are granted just-in-time[1] minimum privileges necessary to troubleshoot the system on an exceptional basis, and only for a fixed period of time. Upon completion of any maintenance task, administrative privileges and access to service data are revoked, and all associated data around these activities are logged.

2. Employee Contact Data

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

3. Customer Content

Customer content consists of data, information, documents, spreadsheets and other artifacts that are authored, edited, communicated, maintained and eventually disposed of by the government.

a. Content is considered sensitive in nature. In Microsoft Cloud Services, customers control their own content data. Microsoft's role is limited to that of data processor, a position that is further reinforced in the Microsoft Online Privacy Statement, and their security audits, third party attestations and certifications such as ISO 27001.

b. Specific content will range in type, volume and sensitivity according to the government programs that are making use of Microsoft Cloud Services. Individual programs using Microsoft Cloud Services will be assessed through individual PIAs specific to their implementation.

c. 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.

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

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

All personal information will be held within Canada, with the exception of personal information that may be accessed (temporarily) for the purposes of technical maintenance.

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

1. System or Service Data comes from the ongoing operation of Office 365 and Microsoft Azure cloud services. System data is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. All service and maintenance data is accessed and contained within Microsoft's global, private network.

2. Employee Contact Data in Microsoft Cloud Services will be entered into Microsoft Azure active directory (AAD). All replication of AAD data around the globe happens within Microsoft's global, private network.

3. For Microsoft's in-Canada Cloud Services, Customer Content is encrypted at rest and stored in Canadian facilities. Data location is dictated by customer choice and remains in country unless initiated by the customer.

As customer content is the only category of data likely to contain personal information this information's storage criteria is held to a higher standard. Customer content is stored in Microsoft's in-Canada cloud services and is not accessible outside 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.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	*No*
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	*No*
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	*No*
If you have answered "yes" to all three questions, please contact a PLB Privacy Advisor to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	*No*
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	*No*
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	*No*
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

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

The following three representative use cases are used to describe standard cloud service information flows with corresponding service provider mitigation activities.

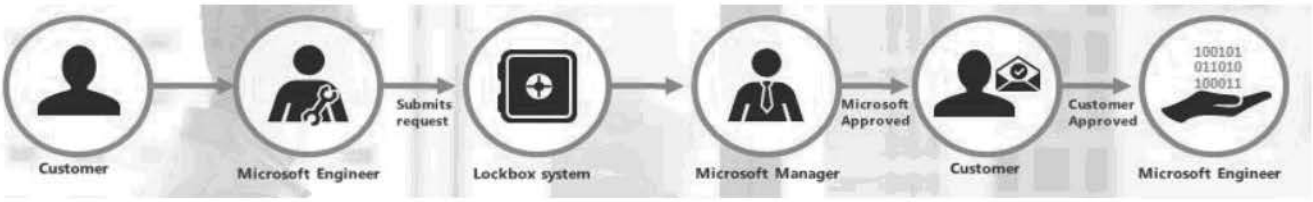
1. A Support Engineer requires elevated privileges for a non-routine maintenance activity

Scenario: A customer finds that one of her documents in Office 365 is either corrupted or unusable. In exceptional and rare instances that a cloud service customer is not able to self-remediate using available resources or with the assistance of a government call centre technician, the user registers a trouble ticket in the service portal to fix the problem. This scenario applies to Microsoft Office 365 (Exchange, SharePoint).

Microsoft Remediation Activity:

Nearly all service operations performed by Microsoft are fully automated and human involvement is highly controlled and abstracted away from customer content. Therefore, Microsoft Engineers do not need and do not have standing access to any service operation.

In the event that automated support and support without access to customer content fails, Microsoft requires explicit consent from government in order to be granted access. This consent is practically managed through a rigorous access control technology called Lockbox. Lockbox enforces access control through multiple levels of approval within Microsoft, providing just-in-time access with limited and time-bound authorization. In addition, all access control activities in the service are logged and audited.



The Customer Lockbox process works 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 and data location for the request;
- Once a Microsoft Engineer's request for access has been approved by a Microsoft Manager, 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.

- 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.

2. ***Standard Notification of Breach***

Scenario: A breach occurs within Office 365 and the government is notified via the standard Microsoft process for notification of a breach, or the government is the victim of a breach within its own implementation. Scenario applies to: Microsoft Cloud Services, Azure and Office 365

Microsoft Remediation Activity:

Microsoft has a global, 24/7 incident response service that works to mitigate the effects of attacks and malicious activity. Breach Incidents and corresponding responses are a shared responsibility of both government and Microsoft.

The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces with internal and external partners alike. If Microsoft becomes aware of any unlawful access to any government 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 government data, Microsoft will promptly:

1. Identify: If an event indicates a privacy or security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft.

2. Notify: Notify government of the incident.

3. Contain: The immediate priority of the escalation team is to ensure the incident is contained and data is safe.

4. Eradicate: After the situation is contained, the escalation team moves toward eradicating any damage caused by the incident and identifies the root cause of the issue.

5. Recover: Software or configuration updates are applied to the system and services are returned to full working capacity.

6. Prevent: Each incident is analyzed to ensure the appropriate mitigations are applied to protect against future recurrence.

3. Microsoft receives a government court order for information contained in the BC tenant of Office 365

Scenario: A US court order is received for email information from government's Office 365 or Microsoft Azure implementation. Scenario applies to: Microsoft Cloud Services

Microsoft Remediation Activity:

Notification of lawful requests for information.

Microsoft believes that customers should control their data whether stored on their premises or in a cloud service. Microsoft will not disclose customer data to law enforcement except as a customer directs or where required by law. When a government makes a lawful demand for customer data from Microsoft, Microsoft strives to be principled, limited in what they disclose, and committed to transparency.

- *Microsoft does not provide any third party with direct or unfettered access to customer data. Microsoft only releases specific data mandated by the relevant legal demand.*

- *If a government requests access to customer data—including for national security purposes—it needs to follow the applicable legal process. It must serve Microsoft with a warrant or court order for content or subpoena for account information. If compelled to disclose customer data, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.*

- *Microsoft will only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. Every request is explicitly reviewed by Microsoft's legal team, who ensures that the requests are valid, rejects those that are not, and makes sure Microsoft only provides the data specified in the order.*

In its commitment to transparency, Microsoft publishes an online Law Enforcement Requests Report every six months providing a comprehensive view of all the legal demands Microsoft receives from governments around the world. This includes any requests from the FISA court, although it does not specify their origin if they are sealed orders. The latest online report shows results and the number of requests Microsoft received from law enforcement world-wide for the second half of CY2014.

Microsoft received very few law enforcement requests for data associated with the use of commercial services by enterprise customers (e.g. government and corporations). In the second half of 2014, Microsoft only received three requests from law enforcement.

In two of those cases, the requests were rejected or law enforcement was successfully redirected to the customer. In the third case, Microsoft notified the customer of the legal demand and the customer directed Microsoft to provide responsive information to law enforcement.

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*USA Freedom Act permits 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 in the second half of 2014). 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 the Office365, Microsoft would need to write specific code to override the Customer Lockbox system. It is*	*Very Low*	*Variable*

		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 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*	*Low*	*Variable*

		as government employees and users of the government systems. *Government will ensure that Microsoft utilizes controls to manage employee access, such as their two-factor authentication and their Lockbox approval process.*		
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 integrity to ensure compliance with international standards, such as ISO 27018 and ISO 27001 among others.*	*Low*	*Variable*
5.	*Data security*	*All data will be encrypted during transmission between government and Microsoft. Data will also be encrypted while at rest in Microsoft's facilities.*	*Low*	*Variable*
6.	*Proper flow-through of privacy requirements from government to service provider.*	*Government will ensure that a contract with Microsoft is in compliance with FOIPPA.*	*Low*	*Variable*

10. Collection Notice

As Microsoft will not be collecting any personal information directly, they will not be providing any collection notices. All collection of personal information will be done by the government programs opting to use Microsoft's services. It is the responsibility of these government programs to provide collection notices, as appropriate, to the individual from whom they collect personal information. As such, there is no collection notice required here, as per section 27(3)(c) / 27(1)(b) of FOIPPA.

Part 3 – Security of Personal Information

Microsoft's construct for security, compliance, and privacy in cloud services has two equally important dimensions. The first dimension includes service-level capabilities that include technology, operational procedures, and policies that are enabled by default for customers using the service. The second entails customer controls that include features that enable you to customize your Office 365 environment based on the specific needs of your organization.

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

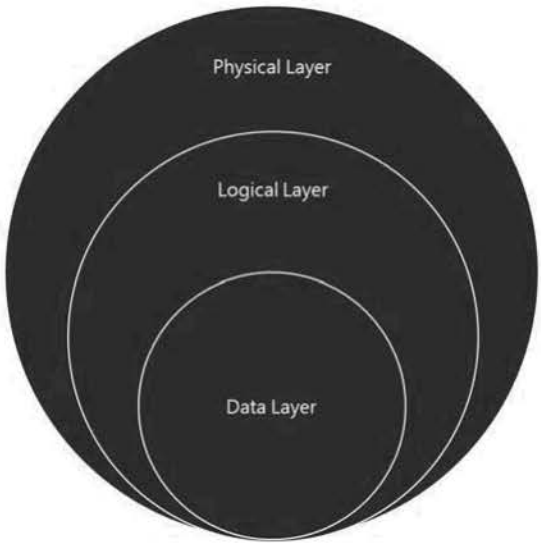


Figure 1 Defense in depth

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

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

- Port scanning and remediation
- Perimeter vulnerability scanning
- Operating system security patching
- Network-level DDOS (distributed denial-of-service) detection and prevention

- Multi-factor authentication for service access
- Regular penetration testing

With regards to people and process, preventing breaches involves:

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

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

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

Microsoft cloud services are manned by Microsoft personnel and all activities are logged and can be audited. Services comply with the common engineering criteria for physical security of Azure assets.

Microsoft Cloud Services are built on an internationally certified global infrastructure foundation. Additional Information on Microsoft security, audits and certifications can be found *here*.

At the global infrastructure level, a long list of physical security measures is provided through Microsoft Azure.

Azure Physical Security Measures

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

The Canadian Microsoft facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These data centres, including Canadian facilities, comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel and include:

- Perimeter Defences include: on-premise security staff around the clock; facility setback requirements; barriers; and fencing.
- Buildings are equipped with: alarms; security operations centre; seismic bracing; security cameras; and security breach alarms.
- Computer rooms are equipped with: two-factor access control; biometric and card readers; cameras; and days of backup power.
- 24-hour monitoring of data centres.
- Multi-factor authentication, including biometric scanning, badges and smart cards for data centre access.
- Internal data centre network is segregated from the external network.
- Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
- Faulty drives and hardware are demagnetized and destroyed.
- In case of a natural disaster, security also includes automated fire prevention and extinguishing systems and seismically braced racks where necessary.

Physical controls are rounded out with monitoring and logging. Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Azure meets a broad set of international as well as regional and industry-specific compliance standards addressing physical security, such as ISO 27001, FedRAMP, SOC 1 and SOC 2. Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

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

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

For Microsoft Azure

- Security Update management.
- Antivirus and antimalware protection.
- Penetration testing.
- DDoS Protection.
- Network Protection.
- Network isolation.
- Virtual networks.
- VPN and Express Route.
- Encrypting communications.
- Data Protection.
- Data Isolation (within multi-tenant environment).
- Encrypting data at rest.
- Encrypting data in transit.
- Encryption.
- Data redundancy.
- Data destruction.

For Microsoft Office 365

Along with the encryption technologies that are addressed at the service-level in Office 365 and managed by Microsoft, Microsoft also offers various technologies that government can implement and configure. These technologies offer a variety of ways to encrypt data in different workloads and offer ways to encrypt data at rest or in transit. These technologies include:

- Rights Management Service

- With RMS, government can not only encrypt data but also apply policies on the data to limit or allow the actions by the recipient of the data.

- Secure Multipurpose Internet Mail Extension (S/MIME)
  - S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and digital signing of MIME data. S/MIME allows a user to (1) encrypt an email (2) digitally sign an email.

- Office 365 Message Encryption
  - Allows users to send and receive encrypted email as easily as regular email directly from their desktops. Email can be encrypted without complex hardware and software to purchase, configure, or maintain.

- Transport Layer Security (TLS) for SMTP messages to partners
  - Government may setup an SMTP connection to their trusted partners that is secured using Transport Layer Security negotiation. Sending email via an encrypted SMTP channel can prevent data in emails from being stolen in man-in-the-middle attacks where one corporation is sending emails to their business partner.

- Anti-malware/anti-spam controls
  - Office 365 uses multi-engine anti-malware scanning to protect incoming, outgoing, and internal messages from malicious software transferred through email.

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

Microsoft Cloud Services are designed for security from the ground up. For instance, Azure code development adheres to Microsoft's Security Development Lifecycle (SDL). The SDL is a software development process that helps developers build more secure software and address security compliance requirements. It embeds security requirements into systems and software through the planning, design, development, and deployment phases.

Enhancing operational security. Azure adheres to a rigorous set of security controls that govern operations and support. Microsoft deploys combinations of preventive, defensive, and reactive controls including mechanisms to help protect against unauthorized developer and/or administrative activity.

Assume breach. One key operational best practice that Microsoft uses to harden its cloud services is known as the "assume breach" strategy. A dedicated "red team" of software security experts simulates real-world attacks at the network, platform, and application layers, testing Azure's ability to detect, protect against, and recover from breaches.

Incident management and response. Microsoft has a global, 24/7 incident response service that works to mitigate the effects of attacks and malicious activity.

Office 365 Security monitoring and response. Many threats target software vulnerabilities, but others attack operational weaknesses, which is why Microsoft uses the Operational Security Assurance (OSA) framework. OSA supports continuous monitoring, helps to identify operational risks, provides operational security guidelines, and validates that those guidelines are followed. OSA helps make Microsoft cloud infrastructure more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to security threats.

Independent verification. Office 365 has operationalized security into a scalable process that can quickly adapt to security trends and industry-specific needs. Microsoft engages in regular risk management reviews, and it develops and maintains a security control framework that meets the latest standards. Internal reviews and external audits by trusted organizations are incorporated into the Office 365 service life cycle.

Office 365 has obtained independent verification, including ISO 27001 and SSAE16 SOC 1 (Type II) audits, is able to transfer data outside of the European Union through the U.S.-EU Safe Harbor Framework and the EU Model Clauses, is willing to sign a HIPAA Business Associate Agreement (BAA) with all customers, has received authority to operate from a U.S. federal agency under FISMA, and has disclosed security measures through the Cloud Security Alliance's public registry. Office 365 extends the controls implemented to meet these standards to customers who are not necessarily subject to the respective laws or controls. For a listing of the various certifications with which Microsoft ensures continued compliance, please see Appendix A.

Privacy Customer Controls. In addition to service-level capabilities, Office 365 enables customers to collaborate through the use of transparent policies and strong tools while providing the distinct ability to control information sharing.

- Rights Management in Office 365
- Privacy controls for sites, libraries and folders
- Privacy controls for communications

Data loss prevention (DLP). DLP proactively identifies sensitive information in an email message, such as social security or credit card numbers, and alerts users via "Policy Tips" before they send that message.

Document Fingerprinting. Government may encounter scenarios in which individuals in the organization handle many kinds of sensitive information during a typical day. Document Fingerprinting makes it easier to protect this information by identifying standard forms that are used throughout the organization.

Auditing and Retention Policies. By using Office 365 auditing policies, users can log events, including viewing, editing, and deleting content such as email messages, documents, task lists, issues lists, discussion groups, and calendars. Administrators can use these reports to determine how information is being used within the organization, manage compliance, and investigate areas of concern.

For business, legal, or regulatory reasons, the government may have to retain e-mail messages sent to and from users in the organization, or the government may want to remove e-mail that you aren't required to retain. Messaging records management (MRM), the records management technology in Office 365, enables you to control how long to keep items in users' mailboxes and define what action to take on items that have reached a certain age.

eDiscovery. The new, easy-to-use eDiscovery Center can be delegated to specialist users—such as a compliance officer or human resources personnel—to conduct eDiscovery tasks without having to generate additional overhead for the IT department. Customers can be specific about what to search for and preserve resulting in only locating the desired records and nothing more.

Data Spillage Management. Office 365 has compliance features to support customer organizations in the event of a need to manage data "spillage." For example, if government were to transmit classified data into Office 365, there are ways for government to remove the data by themselves.

Data Deletion. Customer data privacy is one of Microsoft's key commitments for the cloud. With Office 365, at contract termination or expiration, we will provide at least 90 days for customer administrators to confirm all data migration have been completed, at which point the data will be destroyed to make it unrecoverable. Further, we provide guidelines to customer administrators to personally destroy data if that is preferred.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

A list of access controls in Microsoft cloud services follows:

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

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

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

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

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

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

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

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

Microsoft recognizes the importance of the government's content, such as Exchange Online email body data and SharePoint Online team site content. If someone—Microsoft personnel, partners, or government administrators—accesses government content on the service, government can obtain reports regarding that access by either running a Non-owner mailbox access report[2] or an external admin audit log[3]. These two reports enable government to know to monitor access to our data.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

The updating and correction of personal information will be the responsibility of the government programs that are using Microsoft's services. There are no barriers within the Microsoft system that would preclude government from being able to correct, update, or annotate personal information.

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

---

[2] *The Non-owner mailbox access report lists the mailboxes that have been accessed by someone other than the person who owns the mailbox. When such access occurs, Microsoft Exchange logs information in a hidden folder in the mailbox being audited for 90 days*

[3] *The administrator audit logging records specific actions performed by administrators and users who have been assigned administrative privileges. The government can search for and view entries from the administrator audit log for actions performed by Microsoft administrators and delegated administrators.*

Government programs using Microsoft's services may use the personal information resting on this system in order to make decisions that directly affect an individual. Given the scope and range of this initiative, it is likely that this would be the case.

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

Government programs will be responsible for ensuring that the personal information stored on Microsoft's systems is accurate and complete. Microsoft can provide assurances that the accuracy and completeness of the data resting on their systems is not affected by data integrity issues, for which they would have responsibility. Microsoft will take all necessary, reasonable steps to aid the government in complying with its accuracy and completeness requirements.

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

Government programs will be responsible for ensuring that the personal information stored on Microsoft's systems is appropriately retained and destroyed.

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

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

Part 5 – Further Information

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

Any government program using the data resting on Microsoft's services will be responsible for the required Information Sharing Agreements in the event that personal information is disclosed routinely or systematically.

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

Any government program using the data resting on Microsoft's services will be responsible for the required Research Agreements in the event that personal information is disclosed for research or statistical purposes.

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

Any government program using the data resting on Microsoft's services will be responsible for providing the OCIO 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 – 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.

Privacy Advisor Privacy and Legislation Branch Office of the Chief Information Officer Ministry of Technology, Innovation and Citizens' Services	Signature	Date
Director or Manager Privacy and Legislation Branch Office of the Chief Information Officer Ministry of Technology, Innovation and Citizens' Services **(if Personal Information is involved in this initiative)**	Signature	Date

Part 7 – Program Area Comments and Signatures

Program Manager	Signature	Date
Ministry Contact Responsible for Security (Signature not required unless MISO has been involved.)	Signature	Date
Assistant Deputy Minister or Designate **(if Personal Information is involved in this initiative)**	Signature	Date
Executive Director or equivalent **(if no Personal Information is involved in this initiative)**	Signature	Date

A final copy of this PIA (with all applicable signatures and attachments) must be provided to 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-

Comprehensive, independently verified compliance

Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services.

- **CDSA.** The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media. Azure passed the CDSA audit, enabling secure workflows for content development and distribution.

- **CJIS.** Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhere to the same requirements that US law enforcement and public safety entities must meet.

- **CSA CCM.** The Cloud Security Alliance (CSA) is a non-profit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

- **EU Model Clauses.** Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through our cloud from Europe to the rest of the world.

- **FDA 21 CFR Part 11.** The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States. The compliance reports produced by Azure's independent third party SSAE and ISO auditors identify the procedural and technical controls established at Microsoft and can be used to satisfy the requirements of CFR Title 21 Part 11. Microsoft is able to show how relevant controls within these reports have an impact on compliance with the FDA 21 CFR 11 regulations.

- **FedRAMP.** Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. FedRAMP is a US government program that provides a standard approach to security assessment, authorization, and monitoring for cloud services used by federal agencies and thereby saves the taxpayer and individual organizations the time and cost of conducting their own independent reviews.
- **FERPA.** The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to use and disclosure restrictions imposed by FERPA.
- **FIPS 140-2.** Azure complies with the Federal Information Processing Standard (FIPS) Publication 140-2, a US government standard that defines a minimum set of security requirements for products and systems that implement cryptography.
- **HIPAA.** The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.
- **IRAP.** Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP), which provides assurance for public sector customers that Microsoft has appropriate and effective security controls.
- **ISO/IEC 27018.** Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.
- **ISO/IEC 27001/27002:2013.** Azure complies with this standard, which defines the security controls required of an information security management system.