VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for Non-Ministry Public Bodies

Microsoft Office 365

Part 1 – General

Name of Department/Branch:	Vancouver Island University (VIU)		
PIA Drafter:	Shelly Korobanik, PrivacyWorks Consulting Inc.		
Email:	shelly@privacyworks.ca	Phone:	250-308-5457
Program Manager:	**Paul Lovett**		
Email:	Paul.Lovett@viu.ca	Phone:	

1. Description of the Initiative

Since the early 2000's the Vancouver Island University (VIU) Information Technology (IT) department have been unable to support and respond to the technological requirements of teaching and learning, research and innovation, and administrative functions due to underfunding. Over the past 3 years, the underlying foundational requirements such as the installation of modern digital network and server infrastructure, in addition to department evolution and skill development have been addressed. The Project Nelvana is now underway to introduce a complete technology refresh program, improved IT processes, and further evolution to the IT department. The project includes Microsoft Office 365 (O365) cloud solutions essential to enable the remote learning/work environment necessary during a pandemic.

VIU began implementation of Microsoft Office 365's Exchange Online and Teams in the fall of 2019 due to the COVID-19 pandemic and the necessity to enable a mobile workplace for faculty and staff.

Microsoft Office 365[1] (O365) software-as-a-service (SaaS) offers an in-Canada data residency cloud solution with datacentres located in Quebec City, QC and Toronto, ON. O365 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 provided an opportunity for modernization and improvements to information security and privacy, while lowering the overall cost and complexity of VIU's information technology services. Microsoft provides all 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).

[1] It should be noted that Teams Chat data was initially stored outside of Canada and Microsoft has advised VIU that Teams Chat data migration from US datacentres to Canadian datacentres will be completed by June 30, 2022.

Microsoft's Azure cloud-based computing architecture provides clear separation of roles, duties and controls related to access and management of the O365 SaaS. 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 and Microsoft actively plans changes to help ensure continuous compliance with ever evolving regulations and standards. Microsoft Office365 offers additional controls (such as the Customer Lockbox) on top of Azure's international standards-based security foundation, which are designed to maximize security and ensure privacy of user content. These safeguards coupled with a regular schedule of audits and attestations, results in a suite of in-Canada IT services capable of meeting or exceeding the VIU'S privacy and security requirements.

A key premise of the model is that the customer, VIU, controls and owns their content. Microsoft has no standing access to the service components that VIU 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. As a service provider Microsoft will only interact with VIU data under exceptional circumstances for the purpose of providing support services when a problem cannot be self-remedied by VIU own IT or in-house support teams.

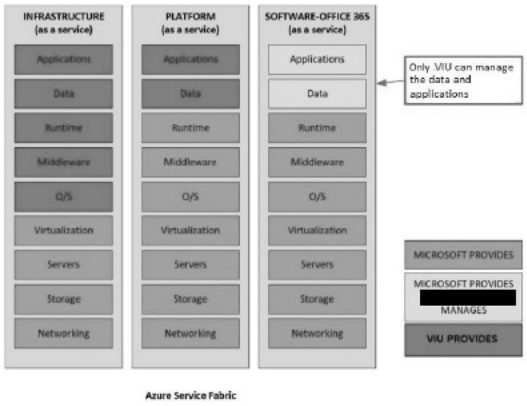
Microsoft Office 365 consists of the following:

1. Office Pro Plus (desktop and cloud-based traditional Microsoft Office suite of software);
2. Exchange email
3. Office 365 SaaS fabric services (security and compliance management tools that overlay all application services);
4. OneDrive (conceptually like Shared File Service today) provides secure cloud storage for users to store, share and sync work files between different devices; and,
5. SharePoint (Web-enabled collaboration services), which will be replaced by Teams.

Commented [MC1]: Wonder if this is still in the works?

Commented [MC2R1]: According to a quick web search, this is a misnomer. Teams relies on Sharepoint – which is where the Teams files are stored.

Figure 1 depicts a visual representation of the Microsoft Cloud Based Service Stacks used to implement O365 for VIU and the party responsible for each.



s. 21(1)

Figure 1: Microsoft Cloud Based Service Stacks IaaS, PaaS, and SaaS

s. 15(1)(l)

Use of [redacted]. Future implementation of these features, as well as any changes or additions to information in this document will be assessed in a PIA Addendum.

[redacted]

s. 13(1)

A training strategy has been developed including the following strategies:

- Implement a technical "Sandbox" environment for staff to work with new tools
- Make extensive use of VIU IT Skill Soft training subscription for relevant courses
- Virtual Instructor led course for all required IT Staffing for MS 365
- VIU employee training plan for all staff (Combination of VIU IT trainer and Free Microsoft Virtual Training)
- Microsoft Fast Track Partners for IT Professionals (free offering Microsoft funded)
- Microsoft 365 Certification Training for 15 staff phase 1

A security, threat risk assessment has been completed and approved.

[redacted]

s. 13(1)

2. Scope of this PIA

The scope of this PIA is for the implementation of MS Office 365 for all VIU employees/faculty including:

- **Exchange Online**– an e-mail messaging system that runs on Windows servers. The server side is Microsoft Exchange Server and the featured client program is Microsoft Outlook, which includes email, calendar, contacts, and tasks. Exchange Online Protection is also included.
- **Teams** – replaced Skype for Business (SfB) Online retired by Microsoft on July 31, 2021 and while similar to SfB, Teams also provides additional functionality that enable users to actively connect and collaborate in real time on documents, files and shared apps.
- **Office Pro Plus** - includes Outlook, Word, Excel and PowerPoint, OneNote, Publisher and Access (client and online versions);
- **OneDrive** – supports collaboration with Word, Excel, PowerPoint, and OneNote from a user's desktop, mobile device, and the web.
- **SharePoint Online** – a Microsoft platform used to create intranets (internal Web sites) for team collaboration, blogs, wikis and news. It is commonly deployed to extend certain information to customers via password-protected Web sites and includes OneDrive.

Out of scope of this PIA are:

- Existing and future use of MS O365 applications by VIU staff beyond what is documented in this assessment;
- MS O365 for students;
- Microsoft Azure;
- Infrastructure-as-a-Service (IaaS);
- Microsoft Azure Platform-as-a-Service (PaaS);
- Microsoft CRM Online (CRM/Case, HR and Financial Management Software as a Service),
- Any other services or applications not specifically noted as being in scope.

3. Assumptions

Currently all O365 data is hosted in Canada, however Teams Chat data was initially stored outside of Canada when VIU implemented its use. It is assumed that Teams Chat data migration from US datacentres to Canadian datacentres will be completed by June 30, 2022 as was indicated by Microsoft. If this migration does not occur and this assumption is incorrect, VIU will be in violation of the Freedom of Information and Protection of Privacy Act (FIPPA) and will need to address the non-compliance with FIPPA with Microsoft. Risk

Commented [MC5]: Need to find out if this migration of Teams chat data has occurred and whether it is now fully on Canadian servers.

Commented [MC6R5]: Have checked with IT, they have assured me that: "all data is stored in **Canada** for Microsoft Teams, Exchange Online, and OneDrive." [redacted] (RE Ticket [redacted]).

s. 13(1)

4. Related Privacy Impact Assessments

- There are no related VIU PIAs.
- Microsoft Office 365 Foundational PIA, February 2016

5. Elements of Information or Data

Microsoft will have custody of 3 basic categories of data, defined as follows:

a) 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, and bandwidth consumption, all of which are examined or used solely for the purpose of providing the cloud service.

i. 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.

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

b) *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 business contact information may be accessed by Microsoft staff providing requested level 2 support if VIU's IT help desk technicians are unable to resolve an access issue. As there are no plans to expand VIU's IT help desk services, only the absolute minimal support will be provided by them for O365 issues, so Microsoft will be heavily relied upon for service support. Microsoft is never provided with a user's password. [redacted] s. 13(1)

c) *Customer Content*

Customer (in this case, VIU) content consists of data, information (including personal information of staff, students, alumni, and faculty), documents, spreadsheets and other artifacts that are authored, edited, communicated, maintained and eventually disposed of by VIU users.

i. 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.

ii. Specific content will range in type, volume and sensitivity according to the VIU users that are making use of Microsoft Cloud Services.

iii. 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 VIU, would be able to investigate and/or fix an ongoing problem with a cloud service.

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

VIU users control their user-created content and the content which they receive from others, including the deletion of such content.

Appendix A provides a detailed list of data elements that may be involved in the O365 implementation, not including users' content.

Part 2 – Protection of Personal Information

6. Storage or Access outside Canada

With respect to storage and access 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 as follows:

1. System or Service Data comes from the ongoing operation of Office 365 and Microsoft Azure cloud services. System data, which does not contain personal information, is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. All service and maintenance data are accessed and contained within Microsoft's global, private network.

2. Employee Contact Data (not considered personal information under the *Freedom of Information and Protection of Privacy Act*) in Microsoft Cloud Services will be entered in Microsoft Azure active directory. All replication of such data around the globe happens within Microsoft's global, private network.

[redacted] s.13(1)

3. For Microsoft's in-Canada Cloud Services, Customer Content, likely to contain personal information, is encrypted at rest and stored in Canadian facilities located in [redacted] (primary datacenter for VIU) and [redacted] (secondary datacentre). 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 retained in the secondary datacentre. Customer content is not accessible outside of Canada by Microsoft unless explicitly permitted by the VIU using mechanisms such as the Office 365 Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with VIU's consent, effect temporary movement to another Datacenter location to ensure customer services and data are not lost. s. 15(1)(l)

   Office 365 uses both physical storage and Azure cloud storage. Exchange Online uses its own storage for customer (VIU) data. SharePoint Online leverages both its SQL Server storage and Azure storage, which necessitates the need for additional isolation of client data at the storage level.

There are three areas of concern regarding the potential disclosure, processing and storage of information outside of Canada with this implementation of O365. The first relates to non-employees' names (i.e., students) and VIU email addresses disclosed to Microsoft in the Azure active directory which is replicated around the globe within Microsoft's global private network. As only VIU staff are in scope for the project, there is no personal information involved, just business contact information so no consent is required for this disclosure. However, when expansion to include non-staff users, VIU will need to reassess the requirement for consent depending upon the data fields being disclosed to Microsoft Azure AD. See question 10. Collection Notice for further details regarding potential consent requirements in future when students' personal information involved.

The second relates to the Microsoft Online Services Terms[3] (OST) which appears to give Microsoft the discretion to transmit, store and process information at other locations beyond the chosen Canadian data centres. The third relates to the use of microservices, such as the spell check and translate functions, which requires information be sent outside of Canada for processing. In both cases the concern is that personal information could be disclosed, processed and retained by Microsoft outside of Canada in contravention of FIPPA. Microsoft was contacted regarding these concerns and provided details on both, summarized below (full response available in Appendix B):

The Online Services Terms states "*Except as described elsewhere in the OST, Customer Data and Personal Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Subprocessors operate*." This applies to other cloud services where Microsoft does not have a contractual commitment to maintain that data in country, such as Sway, Yammer and some of the other non-core Office 365 services. As Microsoft enables more core services in the Canadian datacentres, the OST is updated. Teams has been the most recent service made available in the Canadian datacentres and the OST soon will reflect that contractually. Further in the OST, Microsoft stipulates that they maintain Office 365 core data in Canada and then go on to define exactly what services that entails (Exchange, SharePoint, OneDrive, etc.). Given this response, the discretion given to Microsoft in the OST to transmit, process and retain data outside of Canada does not appear to impact this initiative.

Regarding the concern related to O365 microservices, Microsoft will not allow customers to disable them as it would effectively stop them from writing code for a modern cloud. Microsoft has added the ability for an organization's IT to disable "connected services" features from the Office Pro Plus tools, and while this reduces the use of microservices within Office 365, it does not eliminate them, as other services will continue to use them. See more here: https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls. This complex issue is one that Microsoft's BC Government team continues to work through with

[3] http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=PT&lang=English

the BC Office of the Information and Privacy Commissioner (OIPC), as it has implications for all of BC public sector. ~~Risk~~

Regarding access to personal information from outside of Canada, VIU authorized users can access data via the Internet so it is possible that this could occur. This access would primarily be users accessing their own created content, however, could also involve accessing personal information being used in a collaboration with other authorized users. Currently VIU has no administrative or technical safeguards to mitigate this risk. Risk

It should be noted that due to recent COVID-19 pandemic, the B.C. Minister of Citizens' Services issued a Ministerial Order (See Appendix D) which has been extended multiple times, and currently expires on December 31, 2021[4] (unless rescinded or extended again). A portion of the Order states:

2. *A public body may disclose personal information inside or outside of Canada in accordance with s. 33.2(a) or (c) of Freedom of Information and Protection of Privacy Act through the use of third-party tools and applications on the condition that the disclosure is for the following purposes:*

    a. *the third-party tools or applications are being used to support and maintain the operation of programs or activities of the public body or public bodies,*

    b. *the third-party tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (e.g. social distancing, working from home, etc.), and*

    c. any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer or minister of the public body.

    However, the public body must ensure the deletion of all personal information stored outside of Canada as per item 3 of the order which states:

3. *A public body must not disclose information under sections 1 or 2 unless the head of the public body is satisfied that with respect to the information disclosed:*

    a. the third-party application is reasonably secure in compliance with s. 30 of the Freedom of Information and Protection of Privacy Act; ***and***
    b. the public body makes all reasonable efforts to remove personal information which is collected, used or disclosed using a third-party application from the third-party application as

[4] https://www.cwilson.com/british-columbia-extends-covid-19-related-data-residency-exemptions-for-health-care-and-public-bodies/

soon as is operationally reasonable and the public body retains and manages the information, as required by law.

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 and you must 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;	yes
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 your privacy office(r) 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;	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.	

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

VIU users accessing Microsoft Office 365 services begins at internet-enabled locations and ends at a Microsoft Canadian-based datacenter. Connectivity to the Microsoft datacenter will be via the Internet. Microsoft will only access and use VIU's content to provide VIU with the Microsoft Online Services, including purposes compatible with providing those services (i.e., service support).

As a contracted service provider, the flow of personal information between Microsoft and VIU will be conducted under the following FIPPA authorities for collection and disclosure:

- **S. 26(c)** - Collection - *the information relates directly to and is necessary for a program or activity of the public body,*
- **S. 33.2(c)** - Disclosure - *to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister;*
- **S. 33.1(1)(p)** (where applicable) - Disclosure Inside or outside Canada -
  (i) is necessary for
  (A)installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment that includes an electronic system, or

(B)data recovery that is being undertaken following the failure of an electronic system that is used in Canada, by the public body or by a service provider for the purposes of providing services to a public body, and

(ii)in the case of disclosure outside Canada, results in temporary access and storage that is limited to the minimum period of time necessary to complete the installation, implementation, maintenance, repair, trouble-shooting, upgrading or data recovery referred to in subparagraph (i);

(p.1) if the disclosure

(i)is necessary for the processing of information and if that processing does not

(A)involve the intentional access of the information by an individual, or

(B)result in the storage of personal information, other than personal information that is metadata, outside Canada, and

(ii)in the case of disclosure outside Canada, results in temporary access that is limited to the minimum period of time necessary to complete the processing;

(p.2) if the information is metadata that

(i)is generated by an electronic system, and

(ii)describes an individual's interaction with the electronic system, and if,

(iii)if practicable, personal information in individually identifiable form has been removed from the metadata or destroyed, and

(iv)in the case of disclosure to a service provider, the public body has prohibited any subsequent use or disclosure of personal information in individually identifiable form without the express authorization of the public body;

Although Microsoft has physical/technical custody of client-generated data, the technical Infrastructure, as described at a high level in Part 3 of this document, substantiates that Microsoft may only access personal information when that information relates directly to, and is necessary for, a program or activity of VIU. VIU may disclose, and/or provision access to personal information if the information is necessary for the performance of the duties of a Microsoft employee as a VIU service provider.

On-Premises Active Directory and Azure Active Directory

Commented [MC8]: There is now an addendum for this.

Currently data from VIU's onsite Active Directory (AD) domain is not synchronized to Azure's Active Directory (AAD) but may be in future. AAD is a component of the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Microsoft Cloud Service and is included here because it is used to provide identity and access management services for O365. It combines core directory services, advanced identity governance, and 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 in the same customer tenant. The elements of the AD

that would sync to AAD can be limited to data that is considered business contact information. Potential AAD attributes are listed in Appendix A.

Once authenticated, data transactions occur directly between the user and Microsoft with [redacted], and [redacted] s.15(1)(l)

Exchange Online
Outlook Exchange ActiveSync, and Outlook Web App are Microsoft O365 services a VIU user would use in order to use their Exchange Online 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 mailbox databases. These mailboxes include user mailboxes, resource mailboxes (i.e., meeting rooms, vehicles), shared mailboxes and public folder mailboxes.

Their user mailbox data includes emails and email attachments, calendaring and "free/busy" information, contacts, tasks, notes, groups, 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, only 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 VIU's space in the Microsoft Cloud; "User" refers to the individual/person.

Personal Information Flow Table #1 - Exchange			
	Description/Purpose	**Type**	**FIPPA 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.*	*Collection* *Use* *Disclosure*	*26(c)* *32* *33.2(c)*

3.	*Email is analyzed by Exchange Online Protection filters.*	*See Personal Information Flow Below for Exchange Online Protection*	
4.	*Summary of email transport activity is logged by Microsoft in tracking logs (containing fields sent by, sent to, subject heading, and time stamp).*	*Collection*	*26(c)*
5.	*Email is stored on VIU's tenancy within Microsoft's servers.*	*Disclosure*	*33.2(c)*
Note: All disclosures by VIU and collections by Microsoft are of encrypted data only. [redacted]			

s. 15(1)(l)

The table below (available on the Microsoft website[5]) provides an overview of the security and compliance features of Exchange Online, and links to additional information on each feature.

Feature & Links	Description
Archive mailboxes in Exchange Online	Archive mailboxes (called *In-Place Archiving*) let people in your Office 365 organization take control of messaging data by providing additional email storage. People can use Outlook or Outlook Web App to view messages in their archive mailbox and move or copy messages between their primary and archive mailboxes.
In-Place Hold and Litigation Hold	In-Place Hold and Litigation Hold allow you to preserve or *archive* mailbox content for compliance and eDiscovery.
In-Place eDiscovery	In-Place eDiscovery allows authorized compliance officers in your organization to search mailbox data across your Exchange organization, preview search results, copy them to a Discovery mailbox or export them to a .pst file.
Inactive mailboxes in Exchange Online	You can preserve the contents of deleted mailboxes indefinitely by using *inactive mailboxes*. You can make an inactive mailbox by placing an In-Place Hold or a Litigation Hold on the mailbox, and then deleting the corresponding Office 365 user account. In addition to preserving mailbox contents, administrators or compliance officers can use In-Place eDiscovery to search the contents of an inactive mailbox.
Data loss prevention (DLP)	Data loss prevention (DLP) helps you identify and monitor sensitive information, such as private identification numbers, credit card numbers, or standard forms used in your organization. You can set up DLP policies to notify users that they

[redacted]

s. 13(1)

[5] Refer to the Microsoft website for more information: https://technet.microsoft.com/en-us/library/jj200706(v=exchg.150).aspx

Feature & Links	Description
	are sending sensitive information or block the transmission of sensitive information.
Exchange auditing reports	You can use the auditing functionality in Exchange Online to track changes made to your Exchange Online configuration by Microsoft and by your organization's administrators, and to audit mailbox access by persons other than the mailbox owner. In Exchange Online, audited actions are recorded and available to view in an online report or export to a file.
Messaging records management (MRM)	Messaging records management (MRM) helps your organization manage email lifecycle to meet business and regulatory requirements and reduce the legal risks associated with email. In Exchange Online, you can use In-Place Hold or Litigation Hold to preserve email and Retention tags and retention policies to archive and delete email.
Information Rights Management in Exchange Online	Information Rights Management (IRM) helps you and your users control who can access, forward, print, or copy sensitive data within an email. IRM can use your on-premises Active Directory Rights Management Services (AD RMS) server or Azure RMS.
Office 365 Message Encryption	Office 365 Message Encryption allows you to send encrypted messages to people inside or outside your organization, regardless of the destination email service—whether it's Outlook.com, Yahoo, Gmail, or another service. Designated recipients can send encrypted replies.
S/MIME for message signing and encryption	Secure/Multipurpose Internet Mail Extensions (S/MIME) allows email users to help protect sensitive information by sending signed and encrypted email within their organization. As an administrator, you can enable S/MIME-based security for your organization if you have mailboxes in either Exchange 2013 SP1 or Exchange Online.
Journaling	Journaling can help you meet legal, regulatory, and organizational compliance requirements by recording inbound and outbound email communications. In Exchange Online, you can create journal rules to deliver journal reports to your on-premises mailbox or archiving system, or to an external archiving service.
Mail flow or transport rules	You can use mail flow rules, also known as Transport rules, to inspect messages sent or received by your users and take actions such as blocking or bouncing a message, holding it for review by a manager or an administrator or delivering a copy to another recipient if the mail flow rule is satisfied.

[redacted] s.15(1)(l)

[redacted]

s.15(1)(l)

Personal Information Flow Table #2 – Exchange Online Protection			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	[redacted]	*Collection*	*26(c)*
2.	[redacted]	*Disclosure*	*33.1(1)(p)(p.1)(p.2) / 33.2(c)*
Note: [redacted]			

s. 15(1)(l)

The table below (available on the Microsoft website[6]) provides an overview of the security and compliance features of Exchange Online, and links to additional information on each feature.

Category	Exchange Online Protection Features
Anti-spam protection	• Inbound spam detection • Outbound spam detection • NDR backscatter protection • Bulk mail filtering • Malicious URL block lists • Anti-phishing protection
Spam Management	• The ability to configure connection filter IP Allow and IP Block lists • The ability to customize content filter policies per user, group, or domain • The ability to configure actions on content-filtered messages • The ability to configure advanced options for aggressive spam filtering • International spam filtering • Manage spam via Outlook or Outlook Web App (OWA) • Spam submissions via the Junk Email Reporting Add-in for Microsoft Office Outlook • Spam and non-spam submissions via an email alias • Spam and non-spam submissions via OWA Junk Email Reporting • End-user spam quarantine notifications • The ability for admins to configure the language of end-user spam quarantine notifications • Access and manage messages in quarantine via a web page

[6] Refer to the Microsoft website for more information: https://technet.microsoft.com/en-us/library/dn762130(v=exchg.150).aspx

Category	Exchange Online Protection Features
	• The ability to search the quarantine • View spam-quarantined message headers from the Exchange admin center
Anti-malware Protection	• Multiple engine anti-malware protection • The option to disable malware filtering • Malware inspection of the message body and attachments • Default or custom malware alert notifications • The option to remove an attachment when malware is detected • Anti-spyware protection • The ability to customize malware filter policies per user, group, or domain
Mail routing and connectors	• Conditional mail routing • Opportunistic or forced TLS • Regional routing (the restriction of mail flow to a specific region) • The SMTP Connectivity Checker tool • Match subdomains
Transport rules	• Policy-based filtering and actions • Filter by text patterns • Custom dictionaries • Per-domain policy rules • Attachment scanning • Send policy rule notifications to the sender • Send messages to fixed addresses (such as redirecting or copying a message to a specific address) • The ability to easily adjust rule priority across multiple rules • The ability to filter messages and then change the routing or attributes of a message • Change the spam confidence level of a message by rule. • Inspect message attachments
Administration	• Web-based administration • Directory synchronization • Directory Based Edge Blocking (DBEB) • Remote Windows PowerShell access
Reporting and logging	• Message tracing • Web-based reports • Detailed reporting via the Excel reporting workbook • Audit logging

Category	Exchange Online Protection Features
Service Level Agreements (SLAs) and support	• Spam effectiveness SLA • False positive ratio SLA • Virus detection and blocking SLA • Monthly uptime SLA • Phone and web technical support 24 hours a day, seven days a week
Other features	• A geo-redundant global network of servers • Message queuing when the on-premises server cannot accept mail • Office 365 Message Encryption available as an add-on service

SharePoint Online
Microsoft SharePoint Online is a collection of cloud- and web-based technologies that makes it easy to store, share and manage digital information within an organization.

SharePoint Online is divided into three hubs:

- Newsfeed,
- OneDrive, and
- Sites.

A new microblogging feature allows users to engage in conversations, "like" posts, include pictures, videos and documents and mention other users in the Newsfeed. Sites can be easily customized or configured for mobile devices.

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 "Subscription ID" is also used for each tenant. The Subscription ID 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 Subscription ID 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 "Site ID". When running a SQL query, SharePoint Online uses a Site ID that has been verified as part of a tenant-level Subscription ID 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 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 Subscription ID of the request identity against the Subscription ID 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 (i.e., 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 of mailboxes or SharePoint content by specifying search criteria such as keywords, start and end dates, etc. 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
- Copy search results; and
- Export search results.

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.

An example SharePoint data flow is depicted in Figure 3.

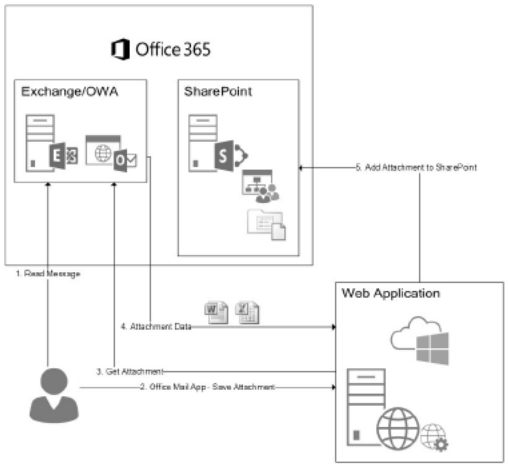


Figure 3: Example Dataflow: User Selecting an Attachment to Save in SharePoint

Personal Information Flow Table #4 - SharePoint			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*SharePoint Online sites are created within VIU's tenancy within Microsoft's servers*	*Disclosure (by VIU)*	*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)*
[redacted]			

s. 15(1)(l)

Teams

Microsoft Teams are like SfB regarding its audio, video, web conferencing, and chat functionality, but it differs in its integration with other O365 applications that enables enhanced collaboration between members of a Team. In contrast to SfB, Teams can integrate with over 140 Microsoft and third-party apps to further improve collaborative work. Teams Chat data, as noted earlier, while now stored on Canadian servers, was initially stored on servers outside of Canada and will be migrated to Canadian servers by June 2022.

As per the Microsoft Office 365 Foundational PIA (2020 Update):

Teams is a "chat-based workspace in Office 365." Teams is a graphical-user interface that integrates many of Microsoft's already existing Office 365 products in to one application. Conceptually, Teams is an interface that lays on top of other Microsoft Services (OneDrive, SharePoint, Exchange/Outlook, etc.). Teams can be accessed either through the Teams client or via web browser.

The basic premise of Teams is to provide users with the capability to communicate privately, as well as publicly in groups or "teams", while being able to facilitate document exchange and collaboration on projects. This can be done for internal, as well as external parties, who also use Office 365, to facilitate secure document exchanges. SharePoint Online provides the back-end document management capabilities available in Teams.

Teams' video conferencing largely encompasses the same capabilities of its predecessor, Skype for Business. The key difference is that users may schedule meetings from within a team, allowing anyone within that team to join the meeting. Video conferences may also leverage Stream to broadcast the meeting/content to other users across the organization or publicly.

Task management is built into MS Teams via Microsoft's Planner application, which allows user to assign tasks and track their progress/completion.
Teams has also implemented its own application store. Here, users are able to access Microsoft-developed, as well as third-party developer's applications that integrate with Teams.

File level encryption is used with Microsoft Teams such that customer data at rest may be stored in the form of files or presentations that have been uploaded by meeting participants. The Web Conferencing server encrypts data content using AES with a 256-bit key. The encrypted data content is stored on a file share. Each piece of content is encrypted using a different randomly generated 256-bit key. The encryption key is stored in a corresponding metadata XML file that is

also encrypted by a per-conference master key. The master key is also randomly generated once per conference.

When a piece of content is shared in a conference, the Web Conferencing server instructs the conferencing clients to download the encrypted content via HTTPS. It sends the corresponding key to clients so that the content can be decrypted. The Web Conferencing server also authenticates conferencing clients before it allows them access to conference content. When joining a Web conference, each conferencing client establishes a SIP dialog with the conferencing focus component running inside the front-end server over TLS first. The conferencing focus passes an authentication cookie generated by the Web Conferencing server to the conference client. The conference client then connects to the Web Conferencing server, presenting the authentication cookie to be authenticated by the server.

All client-facing servers negotiate a secure session using TLS with client machines for data in transit. This applies to various protocols such as HTTP, POP3, etc., that are used by clients such as Outlook, Microsoft Teams, and Outlook Web App.

Microsoft Teams users interact with that service through the Teams client and Web browsers. Teams voice and video traffic is transmitted using Secure Real-time Transport Protocol ("SRTP"). Teams does not store customer calls, but it can be configured to store calls in Exchange Online.

Microsoft Teams the conversations are persistent and, by default, retained as long as the Client maintains their tenant. It is, however, possible for admins can configure retention policies (both preservation and deletion) in the Security & Compliance Center for Teams chat and channel messages. This helps either retain data for compliance (preservation policy) for a specific period or get rid of data (deletion policy) if it is considered a liability after a specific period. Teams retention policies ensure that when an organization delete data, it is removed from all permanent data storage locations on the Teams service

Office 365 Customer Lockbox

In exceptional and rare instances, where VIU is not able to self-remediate an issue using available resources a ticket may be opened in the service portal to have the problem resolved by Microsoft. The issuance of a ticket is the required first step in provisioning access to a Microsoft Engineer through the Customer Lockbox mechanism.

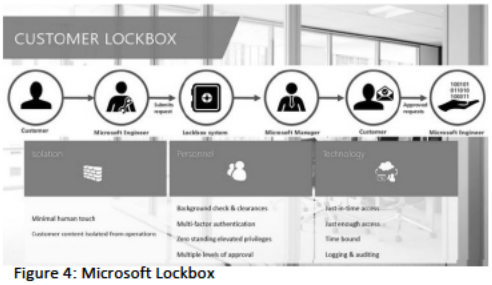


Figure 4: Microsoft Lockbox

Customer Lockbox Process:

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.

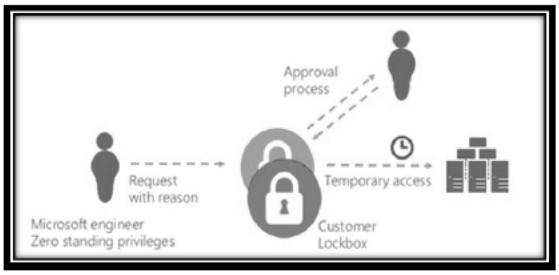


Figure 5: Overview of Access Request Approval Process

- Automated support and Microsoft support without access have failed to address an issue, thus requiring Microsoft Engineer access. This process is initiated by VIU.
- 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, VIU's Office 365 administrators are notified via email that there is a request for access.
- Microsoft can only proceed following approval of a Customer Lockbox request. If VIU rejects a Customer Lockbox request, no access to customer content will occur. If a user was experiencing a service issue that required Microsoft to access customer content in order to resolve (though such circumstances are expected to be extremely rare), then the service issue might simply persist. Microsoft would inform the customer of this outcome.

- VIU'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 scrutinized.
- After a service request has been completed, all access is logged, and a detailed record of all activities performed is available to VIU.
- Use of the Customer Lockbox feature ensures that the Microsoft Engineer does not get access to VIU's content without their explicit approval.

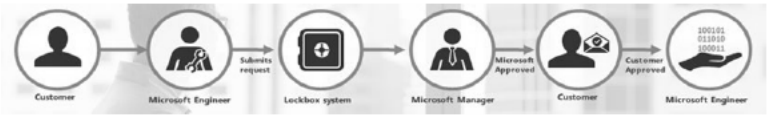


Figure 5: Microsoft Lock Box Dataflow Process

Personal Information Flow Table #5 – Customer Lockbox			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*VIU user identifies or experiences an issue which they are unable to resolve on their own. User would contact the VIU Service Desk for assistance.*	*Use*	*32(a)*
2.	*If unable to resolve the problem, VIU Service Desk initiates a service request with Microsoft. Microsoft Engineer submits a request with both a Microsoft Manager and VIU's 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 VIU administrators.*	*Disclosure*	*33.1 (p)(i)(a)*

Personal Information Flow Scenarios

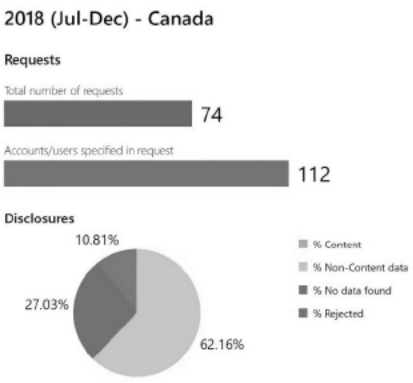
Scenario # 1:	**A Microsoft Support Engineer requires elevated privileges for a non-routine maintenance activity**
Scenario Description	A customer finds that one of their documents in Office 365 is either corrupted or unusable. In exceptional and rare instances that a cloud service customer is not able to self-remediate using available resources or with the assistance of a VIU Service Desk, 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. If automated support and support without access to customer content fails, Microsoft requires explicit consent from VIU in order to be granted access. This consent is practically managed through a rigorous access control technology called Lockbox.

Scenario #2:	**Standard Notification of Breach**
Scenario Description	A breach occurs within Office 365 and VIU is notified via the standard Microsoft process for notification of a breach, or VIU 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 VIU 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 VIU 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 VIU's 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 VIU 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.

Scenario #3:	**Microsoft receives a government court order for information contained in the VIU tenant of Office 365**
Scenario Description	A US court order is received for email information from VIU's Office 365 or Microsoft Azure implementation. Scenario applies to Microsoft Cloud Services
Microsoft Remediation Activity	Notification of lawful requests for information. VIU data will be stored on servers located in Canada. Since early 2013, Microsoft has published a Law Enforcement Requests Report twice yearly detailing the legal demands for customer data they receive from law enforcement agencies around the world. This report is available at https://www.microsoft.com/about/csr/transparencyhub/lerr/. Every year, Microsoft rejects a number of law enforcement requests. In many of these cases, Microsoft informed the requesting government that they were unable to disclose the requested information and explained their reason for rejecting the request. In addition, when appropriate, Microsoft will challenge requests in court. For example, in December 2013, Microsoft formally challenged the geographic reach of a U.S. search warrant, arguing that email should receive the same treatment as physical documents or other property, where the U.S. Government cannot obtain a search warrant to search and seize property located outside the U.S. For more information on that case, go to https://digitalconstitution.com.

Scenario #3:	Microsoft receives a government court order for information contained in the VIU tenant of Office 365
	In July 2016, a US federal appeals court stated that the US government cannot force Microsoft, and other companies, to turn over customer emails stored on servers outside the U.S. Judge Susan Carney said communications held by U.S. service providers on servers outside the United States are beyond the reach of domestic search warrants issued under the Stored Communications Act, a 1986 federal law. If a non-governmental party requests customer data, it must serve Microsoft with a valid subpoena or court order for content, or subscriber information, or other non-content data. For content requests, Microsoft requires specific lawful consent of the account owner, and for all requests they provide notice to the account owner unless prohibited by law from doing so. Microsoft requires that any requests be targeted at specific accounts and identifiers. Their compliance team reviews civil proceeding legal requests for user data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order. 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

Scenario #3:	Microsoft receives a government court order for information contained in the VIU tenant of Office 365
	not, and makes sure Microsoft only provides the data specified in the order.
Law Enforcement Request Report 2018	**Canadian Law Enforcement Requests received for all Microsoft Services from July – December 2018:**  For additional information on the Law Enforcement Request Report, reference: https://www.microsoft.com/about/csr/transparencyhub/lerr/

10. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	[redacted] If the migration of chat records from US to	[redacted] -Ensure follow up is conducted with Microsoft	[redacted] Low	[redacted] Low

s. 13(1)

	Canadian-based MS servers does not occur as planned by June 2022, VIU will be in violation of the Freedom of Information and Protection of Privacy Act (FIPPA).	to confirm the data migration to Canadian Servers.		
2.	Current use of O365 applications beyond the scope of this PIA could put VIU at risk of non-compliance with FIPPA.	Ensure risk assessments are conducted for any planned changes or additions to what is documented in this assessment.	Med	High
3.	O365 utilizes microservices which may result in contravention of FIPPA.	Recent changes to FIPPA permit some limited storage and processing of personal information outside of Canada, however, may be other microservices that still result in unauthorized disclosure or use of personal information (i.e., translation services). Collection notice and/or consent models should be implemented as appropriate to ensure compliance with FIPPA when using O365 applications. See Appendix B for communication with Microsoft on this matter.	Medium	Low

~~43~~.	Access to personal information from outside of Canada by VIU users may occur in contravention to FIPPA.	Administrative safeguards as noted in #6 should be implemented prior to go live across VIU. Project Nelvana planned staff training should include Privacy and security training for all VIU users should and highlight details regarding users' FIPPA obligations related to access to personal information from outside of Canada.	Low	Low
~~54~~.	Lack of administrative safeguards such as privacy and security training, Terms of Use, Data Access & Acceptable Use Agreement, policies, Teams request form, etc., for staff, students and faculty which could result in privacy breaches due to lack of understanding of users' responsibilities.	Recommend that VIU develops the following administrative safeguards be implemented asap for existing users of O365 and prior to expanded use across VIU: • **In Progress -** Terms of Use or Data Access & Acceptable Use agreements • Confidentiality Agreement • **In Progress -** Development and or updating of policies and procedures related to information collection, use, disclosure, retention and disposal to reflect the use of O365, including but not limited to: ○ Records Management	High	High

		○ Records retention and disposal schedule ○ Use of Personal Information for Secondary Purposes ○ User Access management ○ Breach Management ○ Audit **In Progress -** Privacy and security training be developed and made mandatory for all staff, faculty and students with a regular refresh (i.e., annual).		
65.	[redacted]	[redacted]	[redacted]	High
76.	VIU currently has no notice of collection for staff or students putting them in contravention of FIPPA.	Collection notice should be developed compliant to FIPPA requirements and mechanism for staff/students to be informed (i.e., new hire/student process; online at login screen, existing email to new users of network, etc.) implemented prior to VIU	High	High

s. 15(1)(l)

		collecting any personal information from individuals.		
~~87~~.	VIU currently has no consent model for personal information that may be stored/accessed from outside of Canada (i.e., microservices) putting VIU at risk of non-compliance with FIPPA.	Administrative safeguards such as mandatory user training. A consent model should be developed and implemented to address potential storage and access of personal information storage outside of Canada.	Medium	Medium
~~98~~.	A directory of Personal information banks (PIB) is not maintained at VIU as required under FIPPA.	PIB directory should be created at VIU and assigned to appropriate individual(s) to maintain in accordance to FIPPA requirements.	High	Low
~~109~~.	[redacted]	[redacted]	High	High

s. 15(1)(l)

11. Collection Notice

As Microsoft will not be collecting any personal information directly, they will not be providing any collection notices. Any direct collection of personal information is conducted by VIU who would be responsible for ensuring appropriate notice (and/or consent) is given compliant with FIPPA S. 27(2). Currently there is no collection notice in place at VIU for collection of information from employees or students.[redacted]

s. 13(1)

Part 3 – Security of Personal Information

12. Please describe the privacy and security safeguards related to the initiative (if applicable).
Please refer to the STRA.

Microsoft provides a broad range of security and privacy safeguards including contractual assurances through their data processing terms that define how Microsoft will handle and safeguard customer data (Figure 6). By agreeing to these terms, Microsoft commits to over 40 specific security commitments collected from regulations worldwide.

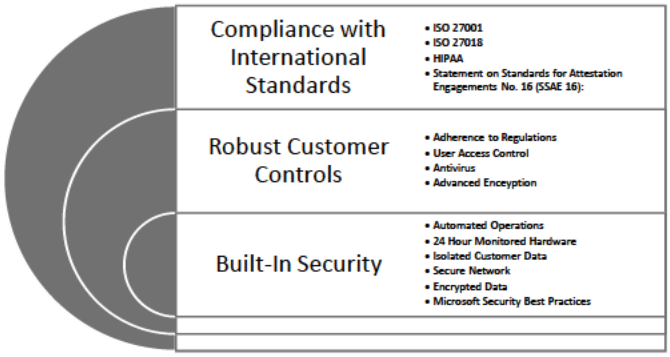


Figure 6: Examples of Microsoft's safeguards

Compliance with International Standards

Many international, industry, and regional organizations independently certify that Microsoft cloud services and platforms meet rigorous security standards[7] and are trusted. [redacted] s. 15(1)(l)
depth and breadth of Microsoft's compliance.

The standards most applicable to VIU's implementation are as follows:

- ISO27001 - ISO27001 is one of the best security benchmarks available in the world. Many products in Office 365 have been verified to meet the rigorous set of physical, logical, process and management controls defined by ISO 27001:2013. This also includes ISO 27018 Privacy controls in the most recent audit. Inclusion of these new ISO 27018 controls in the ISO assessment will further help Office 365 validate to customers the level of protection Office 365 provides to protect the privacy of customer data
- ISO27018 - Microsoft is the first major cloud service provider to be independently verified as complying with ISO 27018, which establishes a uniform, international approach to protecting the privacy of personal information stored in the cloud. Microsoft's compliance

[7] Additional information is available on-line at: Microsoft Trust Center http://www.microsoft.com/trustcenter and https://www.microsoft.com/en-us/TrustCenter/Compliance/complianceofferings

with ISO27018 means that they only process personal information in accordance with customer instructions, are transparent about what happens to customer data, provide strong security protections for personal information in the Microsoft cloud, do not use customer data for advertising, and they inform customers about government access to their data

- Statement on Standards for Attestation Engagements No. 16 (SSAE 16) - Office 365 has been audited by independent third parties and can provide SSAE16 SOC 1 Type I and Type II and SOC 2 Type II reports on how the service implements controls

Robust Customer Controls

Office 365 combines the Microsoft Office suite with cloud-based versions of their next-generation communications (Exchange Online) and collaboration services (SharePoint Online and One Drive). Each of these services offers individualized security features [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

s. 15(1)(l)

Office 365 Built-in Security

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 VIU can implement and configure. The available technologies listed below offer a variety of ways to encrypt data in different workloads and offer ways to encrypt data at rest or in transit.

- Rights Management Service (RMS)
  - With RMS, VIU 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
  - VIU 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.

[redacted]

s. 15(1)(l)

The tables below provide descriptions of the comprehensive controls and security safeguards available in Office 365[8].

Data Privacy		
Safeguard	**Description**	**Additional Information**
Auditing	By using Office 365 auditing policies, customers can log events, including viewing, editing, and deleting content such as email messages, documents, task lists, issues lists, discussion groups, and calendars. When auditing is enabled as part of an information management policy, administrators can view the audit data and summarize current usage.	Administrators can use these reports to determine how information is being used within the organization, manage compliance, and investigate areas of concern.
Data access	The customer is in control of their data including where data is stored and how it is securely accessed and deleted. Depending on the service, the customer can choose where their data is stored geographically.	**Transparency:** • Clear Data Maps and Geographic boundary information provided • The "Ship To" address determines Datacenter Location

[8] Information from the document: MSFT Cloud Architecture Security for Enterprise Architects - http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjf7L2r5-7OAhUJ4GMKHWooALcQFghFMAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F6%2Fd%2Ff%2F6dfd7614-bbcf-4572-a871-e446b8cf5d79%2Fmsft_cloud_architecture_security.pdf&usg=AFQjCNH76W5uCisHLVw7DVyShgLTfC6Kiw

Data Privacy		
Safeguard	**Description**	**Additional Information**
		• Microsoft notifies customers of changes in datacenter locations.
Data Ownership	Microsoft defines customer data as all the data (including all text, sound, software, or image files) that a customer provides, or that is provided on a customer's behalf, to Microsoft through use of the Online Services.	
Data portability	If a customer decides to cancel their service with Microsoft, they can take their data and have it deleted permanently from the Microsoft servers	**Privacy – Office 365**: • Office 365 Customer Data belongs to the customer. • Customers can export their data at any time.
Data Use	Microsoft does not use customer data for purposes unrelated to providing the service, such as advertising. They have a No Standing Access policy — access to customer data by Microsoft personnel is restricted, granted only when necessary for support or operations, and then revoked when no longer needed.	**Transparency:** • Core Customer Data accessed only for troubleshooting and malware prevention purposes • Core Customer Data access limited to key personnel on an exception basis. **Privacy – Office 365:** • No advertising products out of Customer Data. • No scanning of email or documents to build analytics or mine data.
Disclosure of Government Request for Data	If a government approaches Microsoft for access to customer data, they redirect the inquiry to the customer, whenever possible. Microsoft has and will challenge in court any invalid legal demand that prohibits disclosure of a government request for customer data.	

Data Privacy		
Safeguard	**Description**	**Additional Information**
Isolated Customer Data	Office 365 is both scalable and low cost through use of a multi-tenant service (that is, data from different customers shares the same hardware resources). Office 365 is designed to host multiple tenants in a highly secure way through data isolation.	**Built-In Security:** Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by co-tenants. For additional cost, a version of Office 365 that stores data on dedicated hardware is available.
Privacy reviews	As part of the Microsoft development process, privacy reviews are performed to verify that privacy requirements are adequately addressed. This includes verifying the presence of privacy-related features that allow customers to control who can access their data and configure the service to meet the customer's regulatory privacy requirements.	
SPAM	Office 365 evaluates received messages and assigns a spam confidence level (SCL) value. Messages with high SCL values are deleted at the gateway, and messages with low SCL values are delivered to users' inboxes.	Administrators can use the Office 365 Administration Center to manage antimalware/antispam controls, including advanced junk mail options and organization-wide safe and blocked sender lists. Individual

Data Privacy		
Safeguard	**Description**	**Additional Information**
	Messages with borderline SCL values are placed in users' Junk Mail folders, where they are automatically removed after 30 days. Administrators can use the Office 365 Administration Center to manage antimalware/antispam controls, including advanced junk mail options and organization-wide safe and blocked sender lists. Individual users can manage their safe and blocked senders from within their inboxes in Microsoft Outlook or Microsoft Outlook Web App.	users can manage their safe and blocked senders from within their inboxes in Microsoft Outlook or Microsoft Outlook Web App.

Data Encryption and Rights Management		
Safeguard	**Description**	**Additional Information**
Data in Transit	Best-in-class encryption is used to help secure data in transit between datacentres and Microsoft customer, as well as at Microsoft datacentres. Additionally, customers can enable Perfect Forward Secrecy (PFS). PFS uses a different encryption key for every connection, making it more difficult for attackers to decrypt connections.	**Encrypted data:** Customer data in Office 365 exists in two states: at rest on storage media or in transit from a datacenter over a network to a customer device. All email content is encrypted on disk using BitLocker 256-bit Advanced Encryption Standard (AES) encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/ message tracking logs.
Data at Rest	Office 365 and other SaaS services use encryption at rest to protect customer data on Microsoft servers.	

Identity and Access		
Safeguard	**Description**	**Additional Information**
VIU controls access to their data and applications	Microsoft offers comprehensive identity and access management solutions for customers to use across Azure and other services such as Office 365, helping them simplify the management of multiple environments and control user access across applications.	**Service Security:** Office 365 data and services are secured at the datacenter, network, logical, storage, and transit levels. Customers can control who can access data and how they can use data.
Two-Factor Authentication	Two-factor authentication enhances security in a multi-device and cloud-centric world. Although Office 365 is by default configured to use single-factor-authentication for users, Microsoft can provide an in-house solution for two-factor authentication with the phone option and supports third-party two-factor authentication solutions. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.	

Software and Services		
Safeguard	**Description**	**Additional Information**
Secure Development Lifecycle (SDL)	Privacy and security considerations are embedded through the SDL, a software development process that helps developers build more secure software and address security and privacy	**Service Security:** Secure engineering (SDL), access control and monitoring, anti-malware

Software and Services		
Safeguard	**Description**	**Additional Information**
	compliance requirements. The SDL includes: • Risk assessments • Attack surface analysis and • reduction • Threat modeling • Incident response • Release review and certification	
Secure development across the Microsoft cloud	Microsoft Azure, Office 365, Dynamics CRM Online, and all other enterprise cloud services use the processes documented in the Secure Development Lifecycle.	

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
Microsoft Digital Crimes Unit	Microsoft's Digital Crimes Unit (DCU) seeks to provide a safer digital experience for every person and organization on the planet by protecting vulnerable populations, fighting malware, and reducing digital risk.	
Prevent Breach, Assume Breach	In addition to the Prevent Breach Practices of threat modeling, code reviews, and security testing, Microsoft takes an "assume breach" approach to protecting services and data: • Simulate real-world breaches • Live site penetration testing • Centralized security logging and monitoring • Practice security incident response	From a people and process standpoint, preventing breach involves auditing all operator/ administrator access and actions, zero standing permission for administrators in the service, "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and segregation of the

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
		employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Office 365 continues to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. Office 365 conducts penetration tests to enable

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
		continuous improvement of incident response procedures. These internal tests help Office 365 security experts create a methodical, repeatable, and optimized stepwise response process and automation.
Microsoft Cyber Defense Operations Center	The Microsoft Cyber Defense Operations Center is a 24x7 cybersecurity and defense facility that unites their security experts and data scientists in a centralized location. Advanced software tools and real-time analytics help them to protect, detect, and respond to threats to Microsoft's cloud infrastructure, products and devices, and internal resources.	

Datacenter Infrastructure & Networking Security		
Safeguard	**Description**	**Additional Information**
Operational Security for Online Services (OSA)	OSA is a framework that focuses on infrastructure issues to help ensure secure operations throughout the lifecycle of cloud-based services	**Built-In Security:** • Threat and vulnerability management, monitoring, and response • Edge routers, intrusion detection, vulnerability scanning • Dual-factor authentication, intrusion detection, vulnerability scanning • Access control and monitoring, anti-malware, patch and configuration management • Access control and monitoring, file/data integrity

Datacenter Infrastructure & Networking Security		
Safeguard	**Description**	**Additional Information**
Secure Network	Networks within the Office 365 data centres are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Client connections to Office 365 use secure sockets layer (SSL) for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP.	**Built-in-In Security:** Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft datacenter. These connections are encrypted using industry-standard transport layer security (TLS)/ SSL. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the datacenter. Customers can configure TLS between Office 365 and external servers for both inbound and outbound email. This feature is enabled by default

Physical Datacenter Security		
Safeguard	**Description**	**Additional Information**
24-hour Monitored Physical Security	Datacentres are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.	**Built-In Security:** Physical controls, video surveillance, access control. Datacenter access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and

Physical Datacenter Security		
Safeguard	**Description**	**Additional Information**
		security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. The datacentres are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes seismically braced racks where required and automated fire prevention and extinguishing systems.
Zero Standing Privileges	Microsoft maintains a No Standing Access policy on customer data. They have engineered their products so that a majority of service operations are fully automated and only a small set of activities require human involvement. Access by Microsoft personnel is granted only when necessary for support or operations; access is carefully managed and logged, then revoked when no longer needed. Datacenter access to the systems that store customer data is strictly controlled via lock box processes.	**Built-In Security:** Within Microsoft datacentres, access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, fingerprinting, required security training, and access approvals.

Physical Datacenter Security		
Safeguard	**Description**	**Additional Information**
		Engineers request access for particular tasks into a lock box process. The lock box process determines the duration and level of access independently of determining whether another engineer needs to be involved in a monitoring capacity.
Data Destruction	When customers delete data or leave a service, they can take their data with them and have it deleted permanently from Microsoft servers. Microsoft follows strict standards for overwriting storage resources before reuse, as well as for the physical destruction of decommissioned hardware. Faulty drives and hardware are demagnetized and destroyed.	

Contractual Protections

[redacted]

s. 21(1);
s. 15(1)(l)

[redacted]

With VIU's information located in Canada, under the control of VIU, and being encrypted [redacted] the risk that personal information could be disclosed in response to a foreign demand without VIU being aware and able to challenge such a request, would be low. For Teams information currently stored outside of Canada, it is not anticipated that personal information is stored, however it has not been audited so there is a risk that personal information could be disclosed but this risk is mitigated [redacted]

s. 15(1)(l)

VIU Privacy Controls

[redacted]

- [redacted]
- [redacted]
- [redacted]

s. 15(1)(l)

VIU has developed and implemented a Teams request form and processes for management of Teams, and to ensure Teams owners are aware of their responsibilities and accountability, [redacted]

- [redacted]
- [redacted]

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

Microsoft Cloud Services offers the following access controls:

- **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.
- **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. VIU 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 human involvement is highly controlled and abstracted away from customer content. All access control activities in the service are logged and audited.

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

[redacted]

s. 15(1)(l); s. 13(1)

As noted above, Microsoft Cloud Services include access monitoring and logging which can identify access patterns and 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. Activity reports[9] specific to the in-scope O365 applications are also available to authorized administrators. Additional access monitoring functionality in Azure and third-party monitoring tools to detect additional threats may also be used by VIU.

Access to VIU 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 VIU's content, such as Exchange Online email body data and SharePoint Online team site content. If someone - Microsoft personnel, partners, or VIU administrators—accesses VIU content on the service, VIU can obtain reports regarding that access by either running a non-owner mailbox access report or an external admin audit log.

Part 4 – Accuracy/Correction/Retention of Personal Information

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

Authorized users of the O365 applications and services are responsible for their own content, which would include updates and corrections. There are currently no policies or procedures to guide how other individual's personal information should be updated or corrected in VIU records.

[9] https://docs.microsoft.com/en-us/office365/admin/activity-reports/activity-reports?view=o365-worldwide

Personal information disclosed to Microsoft for service support purposes would be the most current information, thus presumed to be correct, so no notifications would be done. [redacted]

s. 13(1)

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 VIU in complying with its accuracy and completeness requirements.

16. Is there a records retention and/or disposition schedule for personal information being retained?

[redacted]

s. 13(1); s. 15(1)(l)

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. [redacted] Microsoft will take all necessary, reasonable steps to aid VIU in complying with its retention and disposition requirements.

Part 5 – Further Information

17. Does the initiative involve systematic disclosures of personal information? If yes, please explain.
There is no anticipated systematic disclosure of personal information. Disclosure to Microsoft will only occur as necessary to enable services (i.e. Azure active directory) and for support purposes.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	

18. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.
There is currently no anticipated research or statistics involving personally identifiable information from this initiative. As VIU does not have any policies or procedures in place relating to use of personal information for research of statistical purposes, should access to personally identifiable information be requested for these purposes, VIU's Privacy officer should ensure compliance with FIPPA prior to such data being released. [redacted]

s. 13(1)

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	

19. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FIPPA. Under this same section, this information is required to be published in a public directory.

Yes, a PIB will result from this initiative [redacted]

s. 13(1);
s. 15(1)(l)

Personal Information Bank Name:
Microsoft Office 365 Solution

Personal Information Location:
Microsoft Datacenter– [redacted]

s. 15(1)(l)

Purpose for the Collection, Use and Disclosure of Personal Information:
To support:

- Initially to conduct a pilot project on O365 solution with intentions to expand use for:
  - Day-to-day operations and collaborations
  - Student academic career administration
  - Student, faculty, staff, and alumni communications

Authority for Collection of Personal Information:

- FIPPA, s. 26 (c) - information relates directly to and is necessary for a program or activity of the public body
- *College and Institute Act,* RSBC 1996, c. 52, s. 41.1(2)(a) – Board may require a student to provide the institution with the personal information that relates directly to and is necessary for an operating program or activity of the institution

Collected Personal Information is About:
Initially just staff, but anticipate expansion to prospective, current, former students and faculty.

Type(s) of Personal Information Collected will include:
Demographic information (i.e. name, email, address, phone)
User content (i.e. content put in emails, documents, etc.)

In accordance with FIPPA and other applicable laws and policies, personal information may be used by and/or disclosed to:

- Initially just VIU staff, but anticipate expansion ton faculty, and students for communication, day-to-day operations and collaborations
- Microsoft for service support purposes

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

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Bill Boyte, General Counsel, University Secretary, and Privacy Officer	Signature	Date

Part 7 – Program Area Signatures

Darren Eveleigh, IT Chief Information Officer	Signature	Date
Karl Childress, IT Infrastructure Manager	Signature	Date
Marlene Kowalski, VP Administration & Finance	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

APPENDIX A - Data Elements

For Exchange Online for staff the following data elements may be used in future to synchronize the Azure AD from VIU's onsite AD:

- [redacted]

[redacted]

The following table of data elements provides an overview of the data that may be collected, used, and disclosed with the O365 applications being implemented. Greyed-out entries will not be used.

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

s. 15(1)(l)

APPENDIX B – Communication with Microsoft

6, 2019, 1:02 PM (3 days ago)

Greg Milligan
to David, me, David

Hi Shelly – I'd be happy to help. As you can imagine, this is something Microsoft is working on with the BC Government and the OIPC, as it has implications in healthcare, municipal governments, core BC government ministries, as well as education. I'll do my best to explain it from an EDU perspective.

The details of how Microsoft stores and processes your data, including what we will and won't do with it are described in the Online Services Terms. It's in the second section on this page: https://www.microsoft.com/en-sg/licensing/product-licensing/products
The current English version of the OST is at the top of the second column.

I'll address the second question first, as it's the most straightforward: On page 11, we stipulate that "Except as described elsewhere in the OST, Customer Data and Personal Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Subprocessors operate." This has caused some anxiety to a few [redacted] because they didn't understand the implications of the first phrase. In the OST (later on page 11), we stipulate that we maintain Office 365 core data in Canada and then go on to define exactly what services that entails (Exchange, SharePoint, OneDrive, etc.).

s. 21(1)

The first paragraph that describes transfers allows us to provide other cloud services where don't have a contractual commitment to maintain that data in country. Examples of this would include Sway, Yammer and some of the other non-core Office 365 workloads. As we enable more core workloads in the Canadian datacentres, we update the OST to reflect that. Teams has been the most recent workload to come into the Canadian datacentres and we will update the OST soon to reflect that contractually. This resource can be useful for determining which services run where: https://products.office.com/en-us/where-is-your-data-located, under "See data storage locations."

The other question about Microservices is more complex.

When the BC-FIPPA legislation was drafted 20 years ago, it was in a world of outsourced datacentres, where a hosting company would run effectively the same workloads as a customer would in their own datacenter. Microsoft Exchange was a good example of this. BC-FIPPA has concerns about data residency and data access, which were really about where the data was written to a disk, and who could access that data. Microsoft's contractual obligations are focused on data residency, meaning data at rest, as this is a common requirement in lots of geographies. As such, we point to the OST and assert that we meet the data residency (or data at rest) requirements of BC-FIPPA.

Recently, the OIPC started to look into where electronic processing of data takes place. In our world, we categorize that as "processing" and differentiate it from "data residency", because we don't persist that data to disk or other form of persistent storage. The challenge is that the world of cloud computing has changed drastically in the last 20 years and workloads are no longer run on a set of VMs running in one single datacenter. Microsoft Azure, Amazon AWS and Google Cloud Platform all provide "Microservice" or "cloud fabric" APIs to complete a task, without requiring the overhead of an entire virtual machine to process the task. Modern SaaS apps like Office 365, D2L Brightspace, Salesforce, etc. use these microservice APIs to scale out their applications. In our world, Azure microservices run in any datacenter, but because it's a machine-to-machine API call with no data persisted to disk, we don't view that as a data residency violation (nor do our European customers, by the way). The OIPC, however, looked at these microservices as an opportunity for data access, even though our understanding of the data access concerns of BC-FIPPA were about humans having access.

Some of the examples of where Office 365 uses microservices are in the Office apps like Word and PowerPoint. Design Ideas takes content from a set of slides and makes an Azure Machine Learning microservice call to determine appropriate fonts, photos, layouts, etc. that might enhance a user's presentation. Similarly, Excel has an Insights feature that takes data, makes an Azure Machine Learning microservices call and then enhances the data's visibility with suggested charts, etc. See https://techcommunity.microsoft.com/t5/Excel-Blog/Get-rich-insights-from-your-data-with-intelligence-in-Excel/ba-p/138261 for more details.

I think that the OIPC wanted Microsoft to find every place where any of our tools use microservices and allow institutions to disable them. Microsoft won't do that, as it effectively stops us from writing code for a modern cloud. Note that this isn't a Microsoft only issue – all SaaS apps under consideration or use by [redacted] will need to be examined to understand how the vendors used the underlying microservices capabilities of the cloud they run on.

s. 21(1)

In the consumer world, we ask the user to opt-in before we enable these features. In a corporate world, IT does that effectively on behalf of their users, so one thing we've added is the ability for IT to disable these "connected services" features from the Office ProPlus tools. This reduces the use of microservices within Office 365, but doesn't eliminate them, as other services will continue to use them. See more here: https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls.

As you can see, this is a complex topic and one that I generally turn to the BC Government team within Microsoft to work through with the OIPC, as it has implications for all of BC public sector.

Hope that helps.
Cheers,
Greg

APPENDIX C – Online Service Terms

Microsoft Online Services Terms for Ed

APPENDIX D – Ministerial Order and Amendments

M085-2020.pdf

m0192_2021.pdf

m0192_2021.pdf

REFERENCES

- Security in Office 365 Whitepaper, January 2016
- Microsoft Office 365 Foundational PIA, February 2016
- Microsoft Office 365 Foundational PIA, Updated January 2020
- PIA MTICS15048[10] - Microsoft Cloud Services – Phase I, December 2015
- PIA MTICS16024 - Microsoft Cloud Services – Phase II September 2016
- Microsoft Cloud Security for Enterprise Architects, December 2018
- Microsoft Online Services Terms, March 2019

[10] MTICS (Ministry of Technology, Innovation and Citizen's Services) PIAs – unknown if content has changed

- END -