Langara.
THE COLLEGE OF HIGHER LEARNING.

Privacy Impact Assessment for Non-Ministry Public Bodies

Microsoft Office 365

PIA2019-0005

Part 1 – General

Name of Department/Branch:	Langara College		
PIA Drafter:	Shelly Korobanik, PrivacyWorks Consulting Inc.		
Email:	shelly@privacyworks.ca	Phone:	250-308-5457
Program Manager:	David Cresswell, Chief Information Officer		
Email:	dcresswell@langara.ca	Phone:	604-323-5929

1. **Description of the Initiative**

In 2014 Langara College (also referred to as Langara in this document) began migrating staff and faculty email accounts to Global Relay for two technologies, namely, Global Relay Mail Archive (7-year retention of all mail regardless of deletion) and Zimbra Mail, Calendar, Contacts, and Tasks. However, due to ongoing technical hurdles with Zimbra, migrations ceased and eventually Global Relay and Langara mutually agreed to walk away from contractual agreements. This necessitated the need to migrate users to a new platform by the end of September 2016.

Microsoft Office 365 (O365) software-as-a-service (SaaS) was the selected solution as an in-Canada data residency cloud solution had become available with datacentres located in Quebec City, QC and Toronto, ON. "Office 365" refers to the subscription plans that include access to Office applications plus other productivity services that are enabled over the internet (i.e. cloud services). Microsoft can provide these services in a variety of packages. This provided an opportunity for modernization and improvements to information security and privacy, while lowering the overall cost and complexity of Langara College'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).

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 every 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 Langara's privacy and security requirements.

A key premise of the model is that the customer, Langara, controls and owns their content. Microsoft has no standing access to the service components that Langara 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 Langara data under exceptional circumstances for the purpose of providing support services when a problem cannot be self-remedied by Langara College's 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. Unified Communications (Exchange email and Skype for Business, which includes audio and video conferencing, Voice over IP, etc.);
3. Office 365 SaaS fabric services (security and compliance management tools that overlay all application services);
4. OneDrive (conceptually like Shared File Service today); and,
5. SharePoint (Web-enabled collaboration services).

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

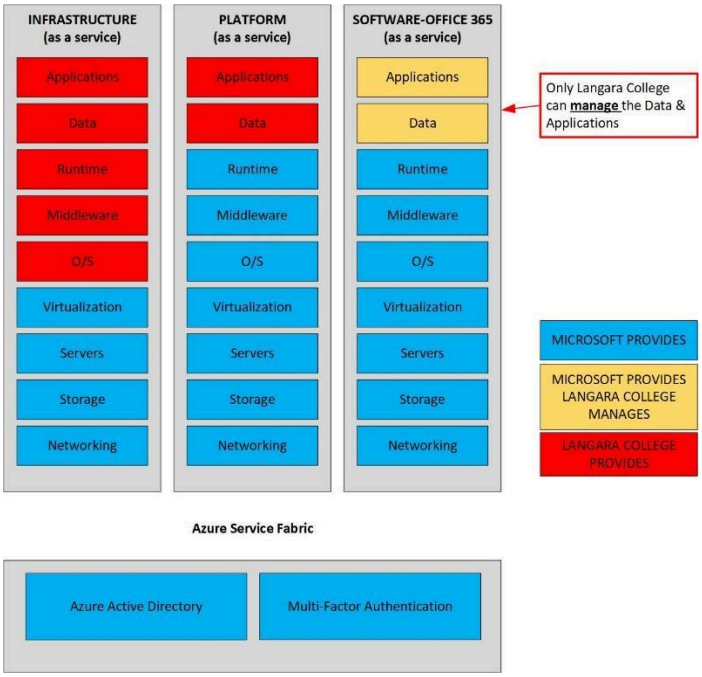


Figure 1: Microsoft Cloud Based Service Stacks IaaS, PaaS, and SaaS

Approximately 1500 staff and faculty email accounts were migrated to O365's Exchange Online service in 2016, with the 7-year retention policy remaining in effect as the same Global Relay Archive system is used by the Microsoft solution. In conjunction with Exchange Online, Exchange Online Protection (EOP), an enterprise-class spam and malware filtering service, was also implemented. No risk assessment was conducted at that time.

The implementation of the O365 solution will now continue as Luminis, which powers the myLangara portal and message servers for students' email accounts, is at end-of-life and no longer supported by the vendor. It is not stable, has not been patched and presents a high security risk as a public facing service. Subsequently Langara will be migrating all active student email accounts to Exchange Online, as well as the staff and faculty portion of the myLangara portal to SharePoint Online. OneDrive for Business, provided by O365's SharePoint Service, will also be implemented to provide a secure cloud storage location where users can store, share, and sync their work files between their different devices. Skype for Business Online (SfB), as well as Teams, will be implemented to enable collaboration in real-time for Langara users. SfB will be retired by Microsoft on July 31, 2021, at which time if Teams have not been implemented, a transition of Langara users will be required.

O365 Test and Production environments exist as depicted in Figure 1 below. The Test environment is configured like the Production environment, has essentially the same user and login ID's, is not accessible to the public, and does not contain any production content. Some test email content may exist from prior email migration testing.

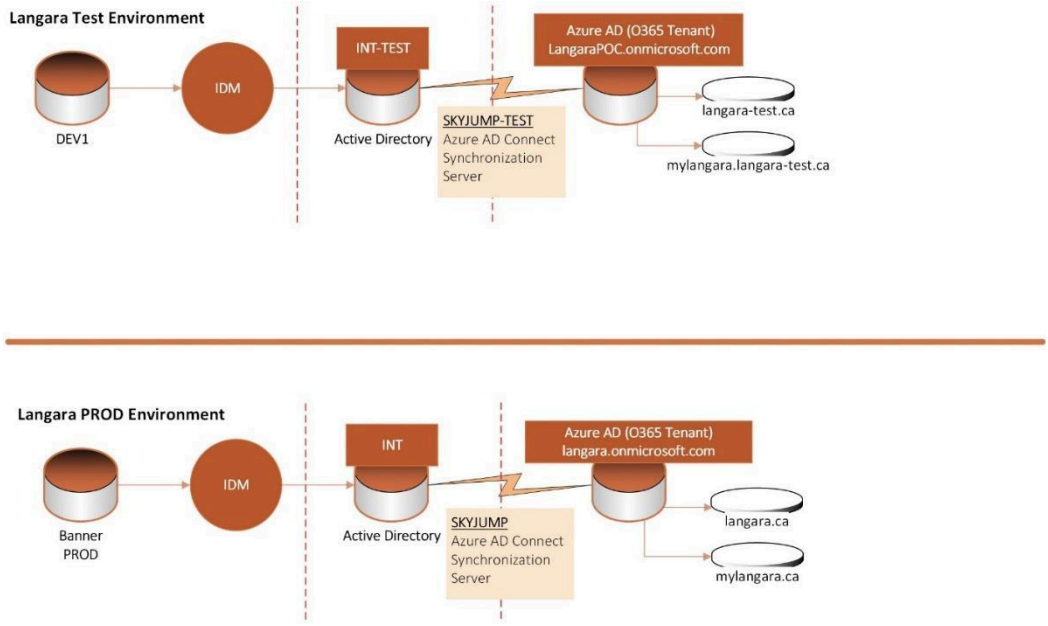


Figure 1: O365 environments for Langara College

O365 services will be accessible directly via the Internet to all authorized users. Microsoft does offer Express Route which provides a dedicated secure route from the customer to Microsoft which could restrict data transmission within Canada, however it is not currently being used by Langara. Go live for these initiatives if planned for December 2019.

2. Scope of this PIA

The scope of this PIA is for Langara College's implementation of the following components of Microsoft Office 365, a SaaS cloud solution hosted in Canadian data centres:

- **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.
- **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 company news. It is also commonly deployed to extend certain information to customers via password-protected Web sites and includes OneDrive for Business.
- **Skype for Business Online (SfB) –** a communication service that includes instant messaging, audio and video calling, online meetings, and Web conferencing capabilities.

- **Teams** – similar to SfB but provides additional functionality that enable users to actively connect and collaborate in real time on documents, files and shared apps.

Out of scope of this PIA are:
- 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), and
- Any other services or applications not specifically noted as being in scope.

3. Related Privacy Impact Assessments

There are no related Langara College PIAs.

4. 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[1] minimum privileges necessary to troubleshoot the system on an exceptional basis, and only for a fixed period of time. Upon completion of any maintenance task, administrative privileges and access to service data are revoked, and all associated data around these activities are logged.

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 information may be accessed by Microsoft staff

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

providing requested level 2 support in the event that Langara's IT help desk are unable to resolve an access issue. Microsoft is never provided with a user's password.

c) *Customer Content*

Customer (in this case, Langara College) 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 Langara College 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 Langara College 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 Langara College, would be able to investigate and/or fix an ongoing problem with a cloud service.

Langara College 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

5. 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.

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 Toronto (primary datacentre for Langara) and Québec City (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 Langara using mechanisms such as the Office 365 Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with Langara's consent, effect temporary movement to another data centre location to ensure customer services and data are not lost.

   Office 365 uses both physical storage and Azure cloud storage. Exchange Online and Skype for Business Online use their own storage for customer (Langara) 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 and Langara email addresses disclosed to Microsoft in the Azure active directory which is replicated around the globe within Microsoft's global private network. Subsequently, consent will be collected from all users every time they sign in to use O365 and

other services offered by Langara. See question 10. Collection Notice for further details regarding consent.

The second relates to the Microsoft Online Services Terms[2] (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 datacenters, the OST is updated. Teams has been the most recent service made available in the Canadian datacentres and the OST soon to 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 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, Langara 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. Langara will be

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

implemented consent process when logging in, but currently has no other administrative safeguards to mitigate this risk. Risk

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative 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.	

7. Common or Integrated Program or Activity*

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

Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

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

Langara College users accessing Microsoft Office 365 services begins at internet-enabled locations and ends at a Microsoft Canadian-based datacentre. Connectivity to the Microsoft datacentre will be via the Internet. Microsoft will only access and use Langara College content to provide Langara College 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 Langara College 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 - the disclosure
  (i) is necessary for
  (A) installing, implementing, maintaining, repairing, troubleshooting or upgrading an electronic system or equipment that includes an electronic system, or
  (B) data recovery that is being undertaken following 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,
  (A) is limited to temporary access and storage for the minimum time necessary for that purpose, and
  (B) in relation to data recovery under subparagraph (i) (B), is limited to access and storage only after the system failure has occurred;

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 Langara College. Langara College 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 Langara College service provider.

On-Premises Active Directory and Azure Active Directory

Data from Langara College's onsite Active Directory (AD) domain synchronizes Azure's Active Directory (AAD) every 30 minutes, and there are also push triggers that may be activated. 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 are limited to data that is considered business contact information. AAD attributes are listed in Appendix A.

Once authenticated, data transactions occur directly between the user and Microsoft. The important differences between how Langara currently manages the services and features it uses that are currently within O365 on campus and MS O365 in the cloud is that user data will be stored (at rest) on Microsoft's servers, as opposed to Langara College servers, and email between Langara College account holders will now cross the internet, whereas previously the data was only processed on Langara College's internal network.

Exchange Online
Outlook Exchange ActiveSync, and Outlook Web App are Microsoft O365 services a Langara College 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 (e.g. 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 Langara College'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 Langara's tenancy within Microsoft's servers.*	*Disclosure*	*33.2(c)*
Note: All disclosures by Langara and collections by Microsoft are of encrypted data only. Langara retains the only encryption key and is the only party able to view the personal information.			

The table below (available on the Microsoft website[3]) 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.

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

Feature & Links	Description
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 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

Exchange Online Protection (EOP)

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

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

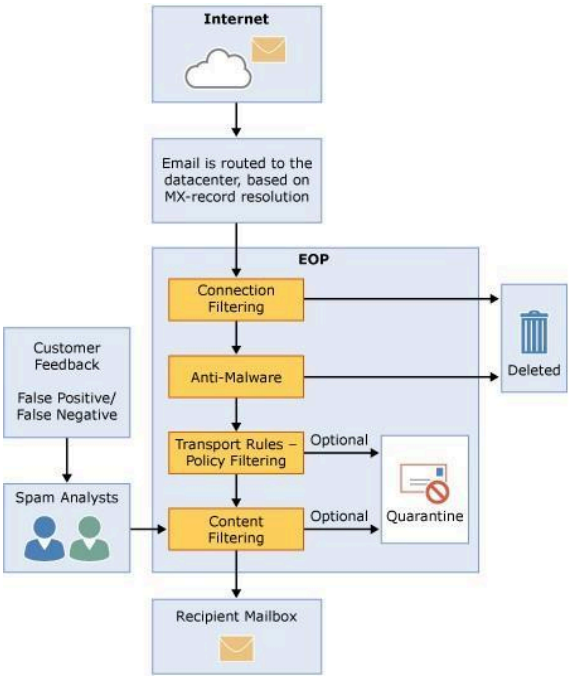


Figure 1: EOP Processes for Incoming email

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

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

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

The table below (available on the Microsoft website[4]) 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

[4] 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
	• 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 • 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

Category	Exchange Online Protection Features
Reporting and logging	• Message tracing • Web-based reports • Detailed reporting via the Excel reporting workbook • Audit logging
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 (e.g. compliance officers, human resources personnel) to search for and preserve records for litigation purposes. eDiscovery uses the content indexes created by SharePoint Search. Authorized client users can perform an eDiscovery search 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.

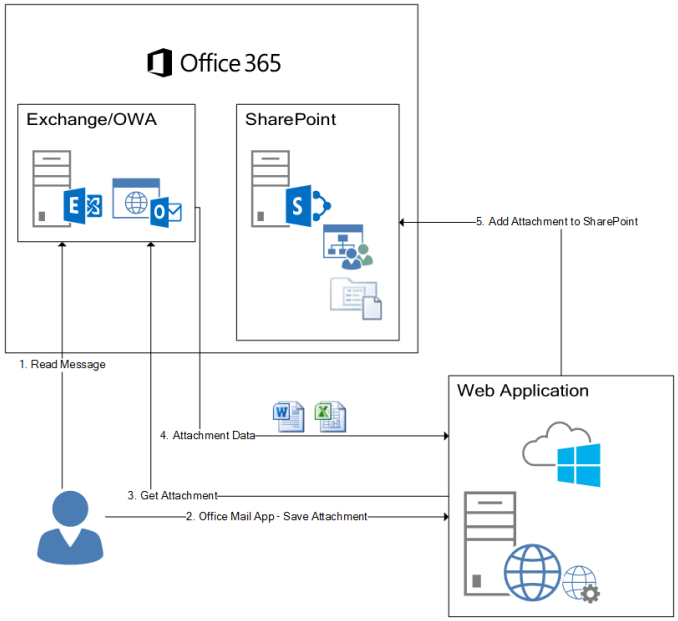


Figure 3: Example Dataflow: User Selecting an Attachment to Save in SharePoint

Personal Information Flow Table #4 - SharePoint			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*SharePoint Online sites are created within Langara's tenancy within Microsoft's servers*	*Disclosure (by Langara)*	*33.2(c)*
2.	*SharePoint Online sites are used for work units to collaborate. Collaboration could include conversations, surveys, documents (and revision), and work histories respecting a project.*	*Disclosure*	*33.2(a)/(c)*
3.	*Microsoft stores all data resting on a SharePoint Online site*	*Collection*	*26(c)*

Note: All disclosures by Langara and collections by Microsoft are of encrypted data only. Langara retains the only encryption key and is thus the only party able to view personal information.

Skype for Business Online (SfB)

Microsoft Skype for Business Online is a hosted communications service that connects people anytime and from virtually anywhere by delivering the collaboration capabilities of Skype as a cloud-based service. It gives users access to presence, instant messaging, audio and video calling, online meetings, and extensive web conferencing capabilities. It is scheduled for retirement by Microsoft on July 31, 2021, with Langara users anticipated to be transition to Teams prior to that date.

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

SfB stores customer content in a variety of places within the Canadian datacentres as follows:

- User and account information, which includes connection endpoints, tenant IDs, dial plans, roaming settings, presence state, contact lists, are stored in the SfB Active Directory servers, as well as in various SfB database servers. Contact lists are stored in the user's Exchange Online mailbox if the user is enabled for both products, or on SfB Online servers if the user is not. SfB database servers are not physically partitioned per tenant, but multi-tenancy is enforced through Role Based Access Control (RBAC).

- Meeting content, such as content that users upload during SfB Online meetings, is stored on Distributed File System ("DFS") shares. This content can also be archived in Exchange, provided archiving is enabled by the system or the user (as determined by Langara). The DFS shares are not partitioned "per tenant" but the content is secured with ACLs and multi-tenancy is enforced through RBAC.

- Call detail records, which consists of activity history, such as call history, Instant Messaging ("IM") sessions, application sharing and IM history, can also be stored in Exchange Online, but most call detail records are temporarily stored on call detail record ("CDR") servers. Content is not partitioned per tenant, but multi-tenancy is enforced through RBAC.

Personal Information Flow Table #5 – Skype for Business			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	• *User information is imported into SfB from Active Directory (AD)* • *Langara discloses the Active Directory (AD) user information to SfB*	*Collection* *Disclosure*	*26(c), 27(1)(b)* *33.2(c)*
2.	• *Free/busy calendar info (point in time only, not stored)* • *User (opts to) upload photo for purposes of employee/workplace engagement and familiarity*	*Collection* *Collection & Disclosure*	*26(c), 27(1)(b)* *26(c)* *33.2(a)/(c)*
3.	*SfB collects information from users directly:* • *when a user is not at their computer for x number of minutes;* • *when a user does not want to be disturbed;* • *when a user adds specific contact information;* • *when a user types in a status note.*	*Collection* *Disclosure*	*26(c)* *33.2(a)/(c)*
4.	*SfB users search the Skype directory and adds other users to their contacts list*	*Use*	*32(a)*
5.	*SfB users add external (outside of Langara) contacts to their contacts list*	*Collection*	*26(c)*
6.	*User activity logs are created when users communicate with each other using SfB*	*Collection*	*26(c)*
7.	*SfB users may share information in Skype meetings*	*Disclosure*	*Only when authorized to do so under section 33.1 of FIPPA.*
8.	*Microsoft Engineer accesses customer content for the purpose of requested service support.*	*Disclosure*	*33.1(1)(p)*

Personal Information Flow Table #5 – Skype for Business			
	Description/Purpose	**Type**	**FIPPA Authority**
9.	*SfB logs and other data are stored on Langara's tenancy within Office 365.*	*Disclosure (by Langara)*	*33.2(c)*
Note: All disclosures by Langara and collections by Microsoft are of encrypted data only. Langara retains the only encryption key and is thus the only party able to view personal information.			

Teams

Microsoft Teams is similar to SfB in regard to 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.
As SfB will be retired by Microsoft on July 31, 2021, Langara has the option to integrate Teams between now and 2021, or transition users from SfB to Teams in 2021. A PIA Addendum will be completed to document that implementation of Teams.

Office 365 Customer Lockbox

In exceptional and rare instances, where a Langara 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.

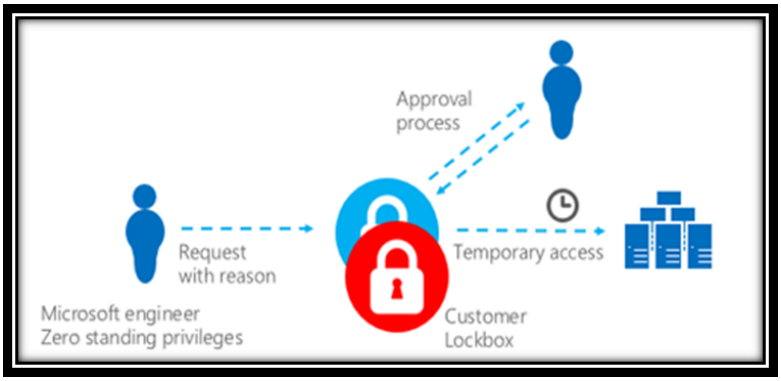


Figure 5: Overview of Access Request Approval Process

- Automated support and Microsoft support without access have failed to address an issue, thus requiring Microsoft Engineer access. This process is initiated by Langara.
- 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, Langara'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 Langara 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.

- Langara'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 Langara.
- Use of the Customer Lockbox feature ensures that the Microsoft Engineer does not get access to Langara's content without their explicit approval.

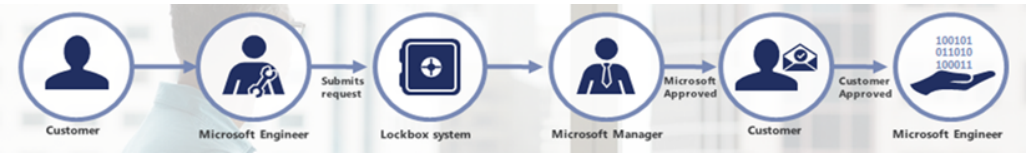


Figure 5: Microsoft Lock Box Dataflow Process

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

Personal Information Flow Scenarios

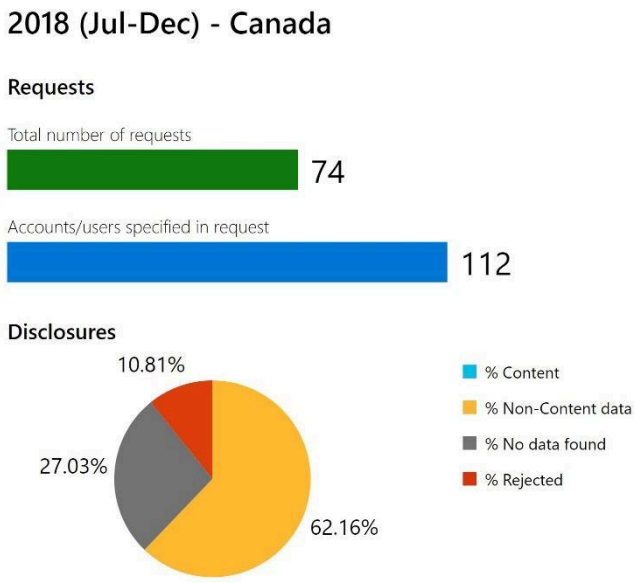
Scenario # 1:	**A Microsoft Support Engineer requires elevated privileges for a non-routine maintenance activity**
Scenario Description	A customer finds that one of their documents in Office 365 is either corrupted or unusable. In exceptional and rare instances that a cloud service customer is not able to self-remediate using available resources or with the assistance of a Langara 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 Langara 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 Langara is notified via the standard Microsoft process for notification of a breach, or Langara 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 Langara 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 Langara data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to

	Scenario #2:	**Standard Notification of Breach**
		such equipment or facilities resulting in loss, disclosure, or alteration of Langara 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 Langara 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 Langara tenant of Office 365**	
Scenario Description	A US court order is received for email information from Langara's Office 365 or Microsoft Azure implementation. Scenario applies to Microsoft Cloud Services	
Microsoft Remediation Activity	Notification of lawful requests for information. Langara 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	

Scenario #3:	**Microsoft receives a government court order for information contained in the Langara tenant of Office 365**
	seize property located outside the U.S. For more information on that case, go to https://digitalconstitution.com. 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

Scenario #3:	**Microsoft receives a government court order for information contained in the Langara tenant of Office 365**
	data to law enforcement except as a customer directs or where required by law. When a government makes a lawful demand for customer data from Microsoft, Microsoft strives to be principled, limited in what they disclose, and committed to transparency. ● Microsoft does not provide any third party with direct or unfettered access to customer data. Microsoft only releases specific data mandated by the relevant legal demand. ● If a government requests access to customer data—including for national security purposes—it needs to follow the applicable legal process. It must serve Microsoft with a warrant or court order for content or subpoena for account information. If compelled to disclose customer data, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so. ● Microsoft will only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. Every request is explicitly reviewed by Microsoft's legal team, who ensures that the requests are valid, rejects those that are not, and makes sure Microsoft only provides the data specified in the order.

Scenario #3:	**Microsoft receives a government court order for information contained in the Langara tenant of Office 365**
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/

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Personal information is compromised when transferred between Langara and Microsoft.	• Data is encrypted in transmission. • Microsoft's Express Route could provide a dedicated secure route restricted to within Canada from Langara to Microsoft however it is not currently in use. Investigation is being conducted to see if BCNet has a peering relationship which may enable Langara to implement Express Route sooner than otherwise may be possible.	Low	High
2.	Lack of administrative safeguards such as privacy and security training, Terms of Use, Data Access & Acceptable Use Agreement, policies, etc., for staff, students and faculty which could result in privacy breaches due to lack of understanding of users' responsibilities.	Recommend that the following administrative safeguards be implemented asap for existing users of O365 and prior to go live with additional users: • Terms of Use or Data Access & Acceptable Use agreement • Updating of any existing policies (i.e. B5010 – Records and Information Management, B4002 – Electronic Communication and B5002 – Computer & Computer System Use) to reflect the use of O365. • Security policies be developed. (Note: Langara is currently developing a Cyber Security practice which will	High	High

		include a Security policy which is expected to be completed mid-late 2020.) ● Privacy and security training be created and provided for all staff, faculty and students with a regular refresh (i.e. annual).		
3.	Langara currently does not audit security and access privileges on a regular basis resulting in the potential for unknown privacy breaches to go undetected.	Both proactive and reactive user access auditing should be developed and assigned for regular review to ensure no inappropriate access, use or disclosure of personal information.	High	High

10. 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 Langara College using existing collection notices compliant with FIPPA S. 27(2). As noted in question 5. Storage or Access outside Canada, there is storage of limited personal information when using O365. As obtaining "written" consent from all users is not practicable, and a past finding (F07-10[5]) by the Office of the Information Privacy Commissioner of BC has found electronic consent acceptable, consent for use of O365 (as well as other online services offered by Langara) will be obtained at point of sign in by all users, including employees who may log into O365 via microsoftonline.com. The following will be displayed to users prior to their logging in.

> *Use of this service may result in limited personal information (i.e. name, Langara email address) being transmitted through or stored in jurisdictions outside of Canada. Your use of this service is your consent and acknowledgement that you have read and understood this statement.*

Login of users is auditable so if needed, confirmation that a user saw the consent is available.

Part 3 – Security of Personal Information

11. Please describe the privacy and security safeguards related to the initiative (if applicable).

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.

[5] Available online at: https://www.oipc.bc.ca/orders/912

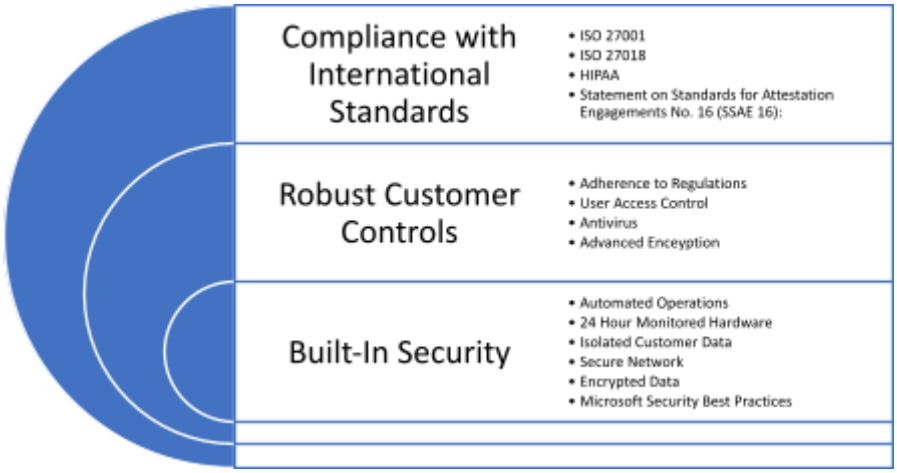


Figure 6: Examples of Microsoft's safeguards

Compliance with International Standards

Many international, industry, and regional organizations independently certify that Microsoft cloud services and platforms meet rigorous security standards[6] and are trusted. Although not all the standards apply to the Langara's implementation of Office 365, they are a good indicator of the depth and breadth of Microsoft's compliance.

The standards most applicable to Langara'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 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

[6] 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

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 that Langara controls including:

- adhering to compliance requirements through Office 365's range of compliance features, including data loss prevention (DLP), eDiscovery, and auditing and reporting functionality.
- providing access to services and content to individuals in a customer's organization,
- configuring antimalware/antispam controls, and
- encrypting data where a customer holds the keys.

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 Langara 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, Langara 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
    - Langara 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.

For this O365 implementation the Transport Layer Security (TLS) will be implemented. The remaining technologies may be considered for implementation in future and would be documented in a PIA Addendum.

Microsoft does offer ExpressRoute which provides a dedicated secure channel between the customer to the Microsoft datacentres which could restrict data transmission within Canada, it is not currently being used by Langara. Although the preferred solution would be to use ExpressRoute, the traffic is fully encrypted and so exposure potential is minimal.

The tables below provide descriptions of the comprehensive controls and security safeguards available in Office 365[7].

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 Datacentre Location

[7] 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 datacentre 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

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.	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.

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 data centre 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
Data at Rest	Office 365 and other SaaS services use encryption at rest to protect customer data on Microsoft servers.	

Data Encryption and Rights Management		
		file OS system disk tracing/ message tracking logs.

Identity and Access		
Safeguard	**Description**	**Additional Information**
Langara 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 datacentre, 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 compliance requirements. The SDL includes: ● Risk assessments ● Attack surface analysis and ● reduction ● Threat modeling ● Incident response ● Release review and certification	**Service Security:** Secure engineering (SDL), access control and monitoring, anti-malware
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	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

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
	• Centralized security logging and monitoring • Practice security incident response	(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 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

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
		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 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.	

Datacentre 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

Datacentre Infrastructure & Networking Security		
Safeguard	**Description**	**Additional Information**
		• Dual-factor authentication, intrusion detection, vulnerability scanning • Access control and monitoring, anti-malware, patch and configuration management • Access control and monitoring, file/data integrity
Secure Network	Networks within the Office 365 datacentres 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 datacentre. 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 datacentre. Customers can configure TLS between Office 365 and external servers for both inbound and outbound email. This feature is enabled by default

Physical Datacentre 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. Datacentre 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 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.	**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.

Physical Datacentre Security		
Safeguard	**Description**	**Additional Information**
	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. Datacentre access to the systems that store customer data is strictly controlled via 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. 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

BCNET has entered into an Online Services Terms (OST) for Education Solutions (Appendix C) with Microsoft, and it is through this agreement that Langara has obtained licensing for O365. BCNET did not include the standard Provincial Privacy Schedule as part of their agreement, however the contents of the OST does serve as one means of ensuring an appropriate level of protection for personal information to enable compliance with the *Freedom of Information and Protection of Privacy Act* section 30, to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

The OST reinforces that:

- Microsoft will provide the physical storage of, and processing power for, any personal information that Langara stores within the Office 365 system;
- Langara will retain the only encryption key and is therefore the only party that can view the information; and
- Microsoft will not disclose Langara data to law enforcement agencies unless required by law. Microsoft will attempt to redirect any law enforcement requests to Langara and, in doing so, may provide basic contact information to the law enforcement agency. If compelled to disclose Langara data to law enforcement, Microsoft agrees to use commercially reasonable efforts to notify Langara in advance of a disclosure and provide a copy of the demand, unless legally prohibited from doing so.

With Langara's information located in Canada, under the control of Langara, and being encrypted with the encryption keys also under Langara's control, the risk that personal information could be disclosed in response to a foreign demand without Langara being aware and able to challenge such a request, would be low.

Langara Privacy Controls

Langara has the following policies on the proper use of computing resources, security, privacy and access to information, which will apply to this initiative, however reviews and updates are required to ensure accuracy with the use of the new cloud environment:

- Electronic Communications[8]
- Access to Information policy[9]
- Computer and Computing System Use policy[10]

[8] https://langara.ca/about-langara/administration/pdf/B4002.pdf
[9] https://langara.ca/about-langara/administration/pdf/B5001.pdf
[10] https://langara.ca/registration-and-records/pdf/B5002.pdf

Langara is currently developing a Cyber Security practice which will include security policies, however currently there are no specific cyber security policies in effect. There are existing Acceptable Use of Technology policies. Risk

Langara currently does not require users of their network to complete any type of agreement (i.e. Data Access, Confidentiality or Terms of Use). All users are directed to, and expected to abide by Langara College Policies, including the Acceptable Use of Technology Policy. Risk

Langara currently does not audit security and access privileges on a regular basis. This will be addressed with the implementation of the new Cyber Security program and framework. Risk

12. 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.

Langara has an Identity and Access Management (IAM) project underway which will implement role-based access structure for non-ERP (enterprise resource planning) connected systems. The project is currently in the RFP (request for proposal) vendor selection stage. Go live date anticipated in late 2020.

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. Langara 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.

13. **Please describe how you track who has access to the personal information.**
Langara currently does not audit security and access privileges on a regular basis. Risk

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[11] 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 Langara.

Access to Langara 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 Langara's content, such as Exchange Online email body data and SharePoint Online team site content. If someone - Microsoft personnel, partners, or Langara administrators—accesses Langara content on the service, Langara 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

14. **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?**
Langara College Policy *B5001 – Access to Information* includes processes for individuals to request corrections to their personal information. Authorized users of the O365 applications and services are responsible for their own content, which would include updates and corrections. 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.

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.

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

Microsoft will take all necessary, reasonable steps to aid Langara in complying with its accuracy and completeness requirements.

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

Langara College's policy B5010 – Records and Information Management does exist, however was last updated in 2009 so a review and update to ensure appropriate retention and disposal of personal information in the cloud environment is required. Currently email is being archived and retained for 7-year period as noted earlier. Risk

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. Langara data would not be destroyed by Microsoft without a specific request from them to do so. Microsoft will take all necessary, reasonable steps to aid Langara in complying with its retention and disposition requirements.

Part 5 – Further Information

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

No there is no systematic disclosure of personal information. Disclosure to Microsoft will only occur when 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).	

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

There is currently no planned research or statistics involving personally identifiable information from this initiative. In future it is possible that data may be used internally for statistical purposes, however this would be only in aggregate form, and in compliance with existing Langara policies and procedures. Should access to personally identifiable information be requested for research purposes in future, Langara has a Research Ethics Board that reviews research proposals by faculty and others. When research involves human subjects, it must conform to the provisions of *Policy-B5007 Ethical Conduct for Research Involving Humans*. This policy applies to all research involving human participants and covers all the following situations:

- Research conducted by members of the College acting in their College capacity (this includes faculty, staff, administrators, students, paid or unpaid associates and any other person associated with the College and identifying their association with the College in connection with the research or engaging in the research as part of their non-instructional duty.);
- Where the research is conducted on any College premise or participants are recruited on College premises or using College facilities (e.g. by sending Emails to College students.);
- Where the research is administered by the College;
- Where ethics approval is required pursuant to any agreement the College might have with any other institution or agency.

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).	

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

Yes, a PIB will result from this initiative and as per Langara College policy *B5001 – Access to Information*. The College maintains a Directory of Personal Information Banks which is accessible to the public.

Personal Information Bank Name:
Microsoft Office 365 Solution

Personal Information Location:
Microsoft Datacentre – Primary datacentre in Toronto; secondary datacentre in Quèbec City

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

- 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:
Prospective, current and former students, faculty and staff

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

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

- Langara College staff, faculty, and students for communication, day-to-day operations and collaborations
- Microsoft for service support purposes

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the consultant by Information Technology and the vendor as of the date below. If in future any substantive changes are made to the scope of this PIA, a department Administrator will contact the Manager, Records Management and Privacy who will complete a PIA Update.

Joanne Rajotte, Manager, Records Management and Privacy	Signature	Date

Part 7 – Program Area Signatures

David Cresswell, Chief Information Officer	Signature	Date
Chris Arnold-Forster, Director, Risk & Internal Controls	Signature	Date
Viktor Sokha, Vice-President, Administration and Finance	Signature	Date

APPENDIX A - Data Elements

For the already implemented Exchange online for staff and faculty the following data elements are being used to synchronize the Azure AD from Langara's onsite AD:

- User login ID
- password hash
- Account status (disabled/enabled/deleted)
- Last password reset time
- User first and last names
- Department
- Job Position
- Office phone
- Office room number
- Work Email Address

For the student implementation of Exchange Online, the following data elements will be synchronized with AAD:

Attribute Name	Type	Value
cn	string	bmejia00
countryCode	number	0
displayName	string	Bianca Mejia
givenName	string	Bianca
lang-utype	string	STUD
mail	string	bmejia00@mylangara.bc.ca
objectGUID	binary	A8 5D D5 8F 18 B5 4B 45 92 5E 99 06 FA 69 93 22
objectSid	binary	01 05 00 00 00 00 00 05 15 00 00 00 C8 2B C9 5B 74 D2 1A ED 4B FE 68 D7 40 67 03 ...
pwdLastSet	number	132121965805550938
sAMAccountName	string	bmejia00
sn	string	Mejia
userAccountControl	number	512
userPrincipalName	string	bmejia00@langara.ca

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.

Service Name	Attribute Name	Comment
Exchange Online	accountEnabled	Defines if an on the table entry account is enabled.
Exchange Online	assistant	The name of the assistant for an account.
Exchange Online	authOrig	Relationship that indicates that the mailbox for the target object is authorized to send mail to the source object.
Exchange Online	c	Country abbreviation

Service Name	Attribute Name	Comment
Exchange Online	cn	Common name or alias. Most often the prefix of [mail] value.
Exchange Online	co	Country
Exchange Online	company	The user's company name.
Exchange Online	Contains the distinguished name of the user who is the user's manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager manager properties set to this distinguished name.	
Exchange Online	countryCode	Specifies the country/region code for the user's language of choice.
Exchange Online	department	The name of the person's (user or contact) department.
Exchange Online	description	Contains the description to display for an object.
Exchange Online	displayName	A string that represents the name often shown as the friendly name (first name last name).
Exchange Online	dLMemRejectPerms	Distribution reject permission list.
Exchange Online	dLMemSubmitPerms	Distribution submit permission list.
Exchange Online	extensionAttribute1	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute10	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute11	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute13	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute14	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute15	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute2	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute3	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute4	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute5	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute6	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute7	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	extensionAttribute8	Custom attribute that is defined in the customer on-premises directory.

Service Name	Attribute Name	Comment
Exchange Online	extensionAttribute9	Custom attribute that is defined in the customer on-premises directory.
Exchange Online	facsimiletelephonenumb Contains telephone number of the user's business fax machine.	
Exchange Online	givenName Contains the given name (first name) of the user.	
Exchange Online	homePhone	The person's (user or contact) main home telephone number.
Exchange Online	info This attribute is currently not consumed for groups.	
Exchange Online	Initials Strings of initials of some or all of an individual's names, except the surname(s).	
Exchange Online	l City	
Exchange Online	legacyExchangeDN Distinguished Name from Legacy system	
Exchange Online	mailNickname Alias of the users mailbox.	
Exchange Online	managedBy The distinguished name of the user that is assigned to manage this object.	
Exchange Online	member The list of users that belong to the group.	
Exchange Online	mobile The primary mobile phone number.	
Exchange Online	msDS- Phonetic display name of an object. In the absence of a phonetic display name, the existing PhoneticDisplayName display name is used.	
Exchange Online	msDS-HABSeniorityIndex Hierarchical address book	
Exchange Online	msExchArchiveGUID The GUID of the user's archived mailbox.	
	msExchArchiveName Archive Name msExchAssistantName GUID	
	msExchAuditAdmin Audit Admin Flags msExchAuditDelegate Audit Delegate Flags	
	msExchAuditDelegateAd Audit Delegate Admin Flags msExchAuditOwner Audit Owner Flags	
	msExchBlockedSendersH Populated through an upgrade from Business Productivity Online Standard Suite. Not synced from on premises.	
Exchange Online	msExchAuditDelegateAd Audit Delegate Admin Flags msExchAuditOwner	
Exchange Online	msExchBlockedSendersH Populated through an upgrade from Business Productivity Online Standard Suite. Not synced	
Exchange Online	msExchBypassAudit True/False	
Exchange Online	msExchCoManagedByLin Group only attribute	
Exchange Online	msExchDelegateListLink Delegates list. User only atrribute	
Exchange Online	msExchELCExpirySuspens Litigation Hold End Date	

Service Name	Attribute Name	Comment
Exchange Online	msExchELCMailboxFlags Contains Litigation Hold	
Exchange Online	msExchEnableModeratio True/False - Related to O365 Group Moderation	
Exchange Online	msExchHideFromAddress Indicator to control the visibility of a mail recipient for name resolution.	
Exchange Online	msExchImmutableID GUID	
Exchange Online	msExchLitigationHoldDat Litigation Hold Date	
Exchange Online	msExchLitigationHoldOw Owner of Litigation Hold	
Exchange Online	msExchMailboxAuditEna True/False	
Exchange Online	msExchMailboxAuditLog Numeric	
Exchange Online	msExchMailboxGuid The GUID of the user's mailbox.	
Exchange Online	msExchModeratedByLink Set in conjunction with msExchEnableModeration tells you who is the group moderator	
Exchange Online	msExchRemoteRecipientT Numerical.	
	msExchRequireAuthToSe True/False - When enabled for a distribution list (DL), unauthenticated users are rejected.	
Exchange Online	msExchResourceDisplay Room Display	
Exchange Online	msExchResourceDisplay Room Display	
Exchange Online	msExchResourceMetaDat Meta Data associated with the room	
Exchange Online	msExchResourceSearchPr Search properties associated with a room.	
Exchange Online	msExchRetentionComme Retention Comment	
Exchange Online	msExchRetentionURL Retention URL	
Exchange Online	msExchSafeRecipientsHas Populated through an upgrade from Business Productivity Online Standard Suite. Not synced h from on-premises.	
Exchange Online	msExchSenderHintTransl Mailtips	
Exchange Online	msExchTeamMailboxExpi Date attribute	
Exchange Online	msExchTeamMailboxOwn GUID List	
Exchange Online	msExchTeamMailboxShar Team mailbox SharePoint URL	
Exchange Online	msExchUserHoldPolicies Litigation Hold allows cloud services to determine which users are under Litigation Hold	
Exchange Online	msOrg-IsOrganizational True/False. Constructed attribute (NOT PART OF IDIR SCHEMA)	

Service Name	Attribute Name	Comment
Exchange Online	objectSID mechanical property. AD user identifier used to maintain sync between Azure AD and AD.	
Exchange Online	oOFReplyToOriginator True/False. Only applies to distribution lists	
Exchange Online	otherFacsimileTelephone A list of alternative facsimile numbers.	
Exchange Online	otherHomePhone	A list of alternative home numbers.
Exchange Online	otherTelephone A list of alternative office telephone numbers.	
Exchange Online	pager The primary pager number.	
Exchange Online	physicalDeliveryOfficeNa Contains the office location in the user's place of business.	
Exchange Online	Populated through an upgrade from Business Productivity Online Standard Suite. Not synced msExchSafeSendersHash from on premises.	
Exchange Online	postalCode	The postal or zip code for mail delivery.
Exchange Online	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
Exchange Online	publicDelegates	This attribute stores the user that was configured as a delegate
Exchange Online	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
Exchange Online	reportToOriginator	True/False. The return path to a primary email address.
Exchange Online	reportToOwner	True/False. The return path to a primary email address.
Exchange Online	securityEnabled	Derived from groupType
Exchange Online	sn	Last Name
Exchange Online	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Exchange Online	st	State/Province
Exchange Online	streetAddress	Street Address
Exchange Online	targetAddress	The TargetAddress property specifies the delivery address to which e-mail for this recipient should be sent. This property is read-only.
Exchange Online	telephoneAssistant	Assistant Phone Number
Exchange Online	telephoneNumber	The primary telephone number.
Exchange Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
Exchange Online	title	Contains the user's job title.
Exchange Online	unauthOrig	Email addresses that cannot send messages to this email address

Service Name	Attribute Name	Comment
Exchange Online	usageLocation	mechanical property. The user's country. Used for license assignment.
Exchange Online	userCertificate	Public key certificate.
Exchange Online	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
	The attribute on the Distribution Group indicates if the auto DL approval feature has been	
	msExchModerationFlags enabled. wWWHomePage Web site	
	msExchRecipientDisplayT Numerical value that signifies the type of recipient msExchRecipientTypeDet Numerical value that signifies the type of recipient	
Exchange Online	userSMIMECertificates	S/MIME Public Key Certificate
SharePoint Online	accountEnabled	Defines if an account is enabled.
SharePoint Online	Additional names for a person (user or contact), for example, middle name, patronymic, middleName matronymic, or other names.	
SharePoint Online	authOrig	Relationship that indicates that the mailbox for the target object is authorized to send mail to the source object.
SharePoint Online	c	Country abbreviation
SharePoint Online	cn	Common name or alias. Most often the prefix of [mail] value.
SharePoint Online	co	Country
SharePoint Online	company	The user's company name.
SharePoint Online	countryCode	Specifies the country/region code for the user's language of choice.
SharePoint Online	department	The name of the person's (user or contact) department.
SharePoint Online	description	Contains the description to display for an object.
SharePoint Online	displayName	A string that represents the name often shown as the friendly name (first name last name).
SharePoint Online	dLMemRejectPerms	Distribution reject permission list.
SharePoint Online	dLMemSubmitPerms	Distribution submit permission list.
SharePoint Online	extensionAttribute1	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute10	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute11	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.

Service Name	Attribute Name	Comment
SharePoint Online	extensionAttribute13	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute14	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute15	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute2	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute3	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute4	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute5	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute6	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute7	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute8	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute9	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	facsimiletelephonenumb	Contains telephone number of the user's business fax machine.
SharePoint Online	givenName	Contains the given name (first name) of the user.
SharePoint Online	hideDLMembership	True/False. Hide distribution list.
SharePoint Online	homephone	The person's (user or contact) main home telephone number.
SharePoint Online	info "Notes" field on "Telephone" tab of ADUC.	
SharePoint Online	initials Strings of initials of some or all of an individual's names, except the surname(s).	
SharePoint Online	ipPhone TCP/IP Address of common area phone	
SharePoint Online	l City	
SharePoint Online	mail The list of email addresses for a contact.	
SharePoint Online	mailnickname Alias of the users mailbox.	
	managedBy The distinguished name of the user that is assigned to manage this object.	
SharePoint Online	manager manager properties set to this distinguished name.	
SharePoint Online	member The list of users that belong to the group.	
SharePoint Online	mobile The primary mobile phone number.	

Service Name	Attribute Name	Comment
SharePoint Online	msExchTeamMailboxExpi Date attribute	
SharePoint Online	msExchTeamMailboxOwn GUID List	
SharePoint Online	msExchTeamMailboxShar GUID. Who linked the mailbox to a SharePoint URL	
SharePoint Online	msExchTeamMailboxShar Team mailbox SharePoint URL	
SharePoint Online	objectSID mechanical property. AD user identifier used to maintain sync between Azure AD and AD.	
SharePoint Online	oOFReplyToOriginator True/False. Only applies to distribution lists	
SharePoint Online	otherFacsimileTelephone A list of alternative facsimile numbers.	
SharePoint Online	otherHomePhone	A list of alternative home numbers.
SharePoint Online	otherIpPhone A list of alternative TCP/IP addresses for the telephone.	
SharePoint Online	otherMobile A list of alternative mobile numbers.	
SharePoint Online	otherPager A list of alternative pager numbers.	
SharePoint Online	otherTelephone A list of alternative office telephone numbers.	
SharePoint Online	pager The primary pager number.	
SharePoint Online	physicalDeliveryOfficeNa Contains the office location in the user's place of business.	
SharePoint Online	postalCode	The postal or zip code for mail delivery.
SharePoint Online	postOfficeBox	Postal box identifiers that a postal service uses when a customer arranges to receive mail at a box on the premises of the postal service.
SharePoint Online	preferredLanguage	The preferred written or spoken language for a person.
SharePoint Online	proxyAddresses	Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
SharePoint Online	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password sync and federation.
SharePoint Online	reportToOriginator	True/False. The return path to a primary email address.
SharePoint Online	reportToOwner	True/False. The return path to a primary email address.
SharePoint Online	securityEnabled	Derived from groupType
SharePoint Online	sn	Last Name
SharePoint Online	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
SharePoint Online	st	State/Province

Service Name	Attribute Name	Comment
SharePoint Online	streetAddress	Street Address
SharePoint Online	targetAddress	The TargetAddress property specifies the delivery address to which e-mail for this recipient should be sent. This property is read-only.
SharePoint Online	telephoneAssistant	Assistant Phone Number
SharePoint Online	telephoneNumber	The primary telephone number.
SharePoint Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
SharePoint Online	title Contains the user's job title.	
SharePoint Online	unauthOrig Email addresses that cannot send messages to this email address	
SharePoint Online	url	The list of alternative web pages.
SharePoint Online	usageLocation mechanical property. The user's country. Used for license assignment.	
SharePoint Online	userPrincipalName UPN is the login ID for the user. Most often the same as [mail] value.	
SharePoint Online	wWWHomePage Web site	

Skype for Business Online	accountEnabled Defines if an account is enabled.	
Skype for Business Online	c Country abbreviation	
Skype for Business Online	cn Common name or alias. Most often the prefix of [mail] value.	
Skype for Business Online	co Country	
Skype for Business Online	company The user's company name.	
Skype for Business Online	manager manager properties set to this distinguished name.	
Skype for Business Online	department The name of the person's (user or contact) department.	
Skype for Business Online	description Contains the description to display for an object.	
Skype for Business Online	displayName A string that represents the name often shown as the friendly name (first name last name).	
Skype for Business Online	facsimiletelephonenumb Contains telephone number of the user's business fax machine.	
Skype for Business Online	givenName Contains the given name (first name) of the user.	
Skype for Business Online	homephone	The person's (user or contact) main home telephone number.
Skype for Business Online	ipPhone TCP/IP Address of common area phone	

Skype for Business Online	l City	
Skype for Business Online	Lync/SfB - The device ID (either the Session Initiation Protocol (SIP) uniform resource identifier msRTCSIP-Line (URI) or the TEL URI) of the telephone that the user controls.	
Skype for Business Online	Lync/SfB - True/False - Indicates whether the user is currently enabled for SIP instant messaging, msRTCSIP-UserEnabled as specified in the authoritative (customer, on-premises) directory.	
Skype for Business Online	mail The list of email addresses for a contact.	
Skype for Business Online	mailNickname Alias of the users mailbox.	
Skype for Business Online	managedBy The distinguished name of the user that is assigned to manage this object.	
Skype for Business Online	mechanical property. Used to know when to invalidate already issued tokens. Used by both pwd	
	LastSet password sync and federation.	
Skype for Business Online	member The list of users that belong to the group.	
Skype for Business Online	mobile The primary mobile phone number.	
Skype for Business Online	msExchHideFromAddress Indicator to control the visibility of a mail recipient for name resolution.	
Skype for Business Online	msRTCSIP- Lync/SfB - Fully qualified DNS name of the Microsoft Lync Server 2010 deployment, as specified in DeploymentLocator the authoritative (customer, on-premises) directory.	
Skype for Business Online	msRTCSIP- Lync/SfB - SIP URI for instant messaging, as specified in the authoritative (customer, on-premise) PrimaryUserAddress directory.	
Skype for Business Online	msRTCSIP- Lync/SfB. Option for the application contact.	
Skype for Business Online	msRTCSIP-OptionFlags Lync/SfB	
Skype for Business Online	msRTCSIP-OwnerUrn Lync/SfB	
Skype for Business Online	objectSID mechanical property. AD user identifier used to maintain sync between Azure AD and AD.	
Skype for Business Online	otherTelephone A list of alternative office telephone numbers.	
Skype for Business Online	physicalDeliveryOfficeNa Contains the office location in the user's place of business.	
Skype for Business Online	postalCode The postal or zip code for mail delivery.	
Skype for Business Online	preferredLanguage The preferred written or spoken language for a person.	
Skype for Business Online	proxyAddresses Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.	
Skype for Business Online	securityEnabled	Derived from groupType
Skype for Business Online	sn	Last Name
Skype for Business Online	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Skype for Business Online	st	State/Province

Skype for Business Online	streetAddress	Street Address
Skype for Business Online	telephoneNumber	The primary telephone number.
Skype for Business Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
Skype for Business Online	title	Contains the user's job title.
Skype for Business Online	usageLocation	mechanical property. The user's country. Used for license assignment.
Skype for Business Online	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Skype for Business Online	wWWHomePage	Web site

APPENDIX B – Communication with Microsoft

Shelly Korobanik <shelly@privacyworks.ca>	Fri, Aug 16, 11:52 AM (3 days ago)
to greg.milligan, David	

Hi Greg
David Cresswell at Langara College provided me your email information as i am contracted to complete a Privacy Impact Assessment for their Office 365 implementation. I am seeking information regarding the micro services available associated with O365 and details regarding what information is being transmitted / stored outside of Canada.

Unfortunately, I have not been able to find any information regarding this so am requesting your assistance as Langara has raised this as a concern and we need to address it in the risk assessment.

Also, i recently heard from a colleague that there is something in the MS online terms of service that says MS can move data (including personal information) at their discretion out of Canada. This

obviously would be a concern so would appreciate any clarification on this issue as it pertains to the Langara's implementation of O365 and the MS Azure AD.

Appreciate your assistance on this matter!

Regards
Shelly Korobanik, CIPP/C, CIPP/E, CIAPP-M, MAPP
250.308.5457

Aug 16, 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 BCNET members 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.).

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 datacenters, we update the OST to reflect that. Teams has been the most recent workload to come into the Canadian datacenters 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 datacenters, 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 BCNET members will need to be examined to understand how the vendors used the underlying microservices capabilities of the cloud they run on.

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

REFERENCES

- Security in Office 365 Whitepaper, January 2016
- Microsoft Office 365 Foundational PIA, February 2016
- PIA MTICS15048[12] - 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

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

- END -