Microsoft Office 365 Privacy Impact Assessment

Project Code	TBD
Submission Date	April 30, 2020
Administrative Authority	Wency Lum, Associate Vice-President University Systems & CIO, cio@uvic.ca
Author and Contact Information	Garry Sagert, Director UVic Online Systems, gsagert@uvic.ca
Reviewed By	Brad Weldon, Chief Privacy Officer and General Counsel, cpo@uvic.ca Nav Bassi, Director & Chief Information Security Officer, navbassi@uvic.ca
Review Date	April 30, 2020 Next Review Date: July 30, 2020

Purpose:

University Systems is implementing the Microsoft Office 365 (O365) platform as an enterprise service for students, faculty and staff. A key driver for implementation is for instructional use of Microsoft Teams as a collaboration tool, but Teams will be available to UVic members for a multitude of uses including administration, student support, and general research storage, in addition to instructional use.

Effective March 16, 2020, UVic transitioned from face-to-face to alternative modes of instruction and evaluation for the remainder of the term in response to the BC Provincial Health Officer's direction to post-secondary institutions. This transition was expedited using the existing technologies at UVic, such as CourseSpaces (Learning Management System), BlueJeans, the existing video conferencing service available through BCNET as well as Blackboard Collaborate (web-conferencing platform used primarily by HSD).

The recent announcement by the Provost that Summer Session 2020 will be delivered through online learning requires the delivery of approximately 700 courses to undergraduate and graduate students. The existing tools are not adequate for the mode, class size, scale and scope required to deliver these courses fully online. As such, University Systems and LTSI have been working together to deploy the O365 platform components of OneDrive, Stream, and Teams to enable remote learning, teaching, collaboration, and services at the University of Victoria for May 2020. University Systems will also pursue the deployment of Exchange Online and SharePoint Online at a later date.

The purpose of this Privacy Impact Assessment (PIA) is to assess risks associated the implementation of Teams, as well as OneDrive, and Stream. The use and configuration of Azure Active Directory (Azure AD) underpins the entire O365 platform, therefore this PIA will also discuss the implementation and configuration of Azure AD and document how it will be configured and managed to remain compliant with the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Due to the accelerated process used for the creation and approval of this PIA, the document will be reviewed and updated before August 1, 2020 prior to the use of MS Teams, OneDrive and Stream for the fall term.

In future, any expansion of the Microsoft O365 platform will result in a revision to this Privacy Impact Assessment.

Roles:

The role of University Systems is to configure and operate the O365 platform for general meetings and collaboration, and to support the UVic community with the effective use of O365 for general meetings and collaboration as required.

The role of the Division of Learning and Teaching Support and Innovation (LTSI) is to support faculty and instructional staff with the effective use of O365 in a virtual classroom environment as required.

The role of the Privacy Office is to review this document and provide guidance regarding privacy policy and legislative compliance and risks to the University.

1.0 Privacy Context

1.1 Description

The Microsoft Corporation provides a number of remote cloud-based Software as a Service (SaaS) tools which are within the scope of this PIA:

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

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

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

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

Stream is a video sharing service. Like most video streaming services, Stream offers a platform to upload and share videos, as well as stream live content. Stream also comes with some additional features, such as text analysis/transcription, and integrated forms to embed polls and forms into videos.

UVic is planning to use O365 OneDrive, Stream, and Teams for remote learning purposes as well as administrative purposes starting in May 2020. These tools are already being used by several other large educational institutions for these purposes.

UVic is planning to deploy Exchange Online and SharePoint Online at a later date.

Exchange Online is 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.

SharePoint Online is 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.

1.2 Privacy Issues Related to this Project

Microsoft is headquartered in Redmond, WA, and uses Azure cloud-based data centres around the world. In the standard configuration, data provided by users may be stored on any of these data centres. Microsoft offers an option to store user data (e.g. files) in Canada, however user account information (e.g. name, email address, UVic affiliation) is stored in Active Directory (AD) which is a global service.

1.3 Privacy Impact Assessment Scope

The scope of this PIA is limited to the use of the O365 components of OneDrive, Stream, Teams, Exchange Online, and SharePoint Online. Other tools such as Azure IaaS and Microsoft CRM Online are out of scope of this PIA.

1.4 Related Privacy Impact Assessments

We reviewed PIAs for Azure IaaS from BCNET, as well as O365 services from Langara College and the University of the Fraser Valley during the preparation of this PIA. The Azure IaaS PIA from BCNET covers the underlying infrastructure on which the Canadian data (e.g. files) are stored, and is included as Appendix B.

1.5 Elements of Information or Data

Microsoft will have custody of three (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 generally not personal information, but can contain usernames, 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 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.

iii. System Data for Teams, OneDrive, Stream, Exchange Online and SharePoint Online is stored at rest inside Canada.

b) Account Data

Account Data is basic information used to identify or differentiate users within the cloud service. Examples include Name, User ID, Organizational ID and basic user contact information such as email address. This information may be accessed by Microsoft staff providing requested level 2 support in the event that UVic's IT help desk are unable to resolve an access issue. Microsoft is never provided with a user's password.

[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.

Account Data for UVic employees, when used for this purpose authenticating, identifying, differentiating, and otherwise contacting employees using O365 in the course of their employment is being used to facilitate contact with and between these employees at their place of business, is therefore "contact information" and not "personal information" as defined by Schedule 1 of FIPPA.

Account Data of UVic students and other individuals who are not employees of UVic is not being used to contact students at their place of business. Therefore these data are not contact information, and are considered to be their personal information, as defined by Schedule 1 of FIPPA.

Account Data for Teams, OneDrive, Stream, Exchange Online and SharePoint Online is stored outside Canada in the Azure Active Directory (Azure AD) cloud service for identity and access management; therefore, the majority of this PIA focuses on Azure AD.

c) Customer Content

Customer (in this case, UVic) 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 UVic users.

i. Content is considered sensitive in nature and is likely to include personal information. 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 UVic 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 UVic, would be able to investigate and/or fix an ongoing problem with a cloud service.
iv. Customer Content for Teams, OneDrive, Stream, Exchange Online and SharePoint Online is stored at rest inside Canada and includes:
    i. Teams: Files, chat, history
    ii. OneDrive: Files
    iii. Stream: Recordings, video uploads, transcriptions, comments
    iv. Exchange Online: Emails, meetings, attachments
    v. SharePoint Online: Files, wiki, blogs, web contents, lists
v. Customer Content may be temporarily processed outside of Canada for automated analytical services such as spell check, meeting transcription, and text analysis, but results are stored at rest in Canada.

All customer content is owned by a designated individual or group, which in turn has designated individuals as owners. UVic users/owners control their user-created content and the content which they receive from others, including the deletion of such content, and adherence to UVic data retention guidelines. By default all customer content is private to the individual or group to which it belongs, unless it is explicitly shared by the individual or a group member. Group owners are notified when group content is shared by members.

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

2.0 Protection of Personal Information

2.1 Storage or Access outside of 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. System or Service Data for UVic's instances of Teams, OneDrive, Stream, Exchange Online and SharePoint Online is stored at rest in Microsoft's Canadian facilities located in Sec. 15
2. **Account Data** in Microsoft Cloud Services will be stored in Microsoft Azure AD. All replication of such data around the globe happens within Microsoft's global, private network[2]. Account Data for UVic's instances of Teams, OneDrive, Stream, Exchange Online and SharePoint Online is stored in the Azure AD in North America, but outside of Canada.

   Data from Sec. 15 domain synchronizes with Azure AD upon account creation and thereafter approximately every 30 minutes; there are also push triggers that may be activated. Azure AD 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 Azure AD data around the globe happens within Microsoft's secure global, private network. The information is not disclosed to the public or to other Microsoft customers, rather it remains accessible only to the authorized users in the same customer tenant. The elements of the AD that would sync to Azure AD are limited to data that is considered business contact information for employees but would be considered personal information for students. Azure AD attributes are listed in Appendix A.

   Once authenticated, data transactions occur directly between the user and Microsoft. The important differences between how UVic currently manages the Microsoft services and features on campus versus O365 in the cloud is that user data will be stored (at rest) on Microsoft's servers, as opposed to Sec. 15 and email between UVic account holders will now travel on the internet, whereas previously the data was only processed on Sec. 15 network.
3. **Customer Content** for UVic's instances, of Teams, OneDrive, Stream, Exchange Online and SharePoint Online, which is likely to contain personal information, is encrypted at rest and stored in Microsoft's Canadian facilities located in Sec. 15 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 UVic using mechanisms such as the Office 365 Customer Lockbox. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with UVic's consent, effect temporary movement to another data centre location to ensure customer services and data are not lost.

2.2 Consent for disclosure outside of Canada

The only personal information that is stored outside of Canada when using O365 is Account Data of non-employees, primarily students. In UVic's implementation of O365 this personal information will be comprised of **name, email address, and affiliation with UVic (e.g. department)** which will be disclosed to Microsoft in Azure AD. As noted above, Azure AD is stored outside of Canada within Microsoft's global private network. In order to authorize the disclosure of this limited personal information UVic will require consent from non-employee users of O365. This consent will be collected from all users when they first register for an O365 account, by presenting such users with the following consent notice and requiring them to consent in order to proceed with registering their account:

> *Microsoft 365 is a cloud-based unified communication and collaboration platform that combines persistent chat, video meetings, software, services, and file storage (including collaboration on files) used for online learning,*

[2] Additional information available online at: http://download.microsoft.com/download/A/A/4/AA48DC38-DBC8-4C5E-AF07-D1433B55363D/Azure-AD-Data-Security-Considerations.pdf

teaching, collaboration and providing services at the University of Victoria. Most Microsoft 365 data (e.g. files) will be stored in Canada, however some data elements are stored outside of Canada in Microsoft's global network. By continuing you consent to the disclosure of your ***name*** *and* ***uvic.ca email address, UVic affiliation*** *and* ***device information*** *to Microsoft's global network. Use of Microsoft 365 is subject to the UVic Terms of Service (link to be inserted). If you have questions regarding this disclosure of your personal information, please contact the Privacy and Access to Information Office at privacyinfo@uvic.ca.*

2.3 Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table – Typical Use Cases			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Account Data of non-employees (name, uvic.ca email address, and UVic affiliation) is disclosed to Microsoft global Active Directory.	Disclosure and storage outside Canada	30.1 (b) 33.1(1)(b)
2.	System or service data is stored on Microsoft server inside Canada	Disclosure	33.2(a, c)
3.	Customer Content is processed by Microsoft outside of Canada to enable features of O365 (e.g. spell check) without being stored.	Disclosure outside of Canada	33.1(1)(p.1)
4.	Customer Content disclosed to Microsoft and stored in Azure Canada data centre	Disclosure	33.2 (a, c)
5.	Microsoft administrators may monitor session, at UVic's request, in order to install, implement, maintain, repair, troubleshoot or upgrade the system. No data stored.	Disclosure outside of Canada	33.1(1)(p)

2.4 Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Non-compliance with FIPPA requirement that personal information not be stored or accessible outside of Canada without consent.	Minimize AD attributes that are synchronized with Microsoft Global AD, collect consent for said disclosure at service sign-up.	Low	Medium
2.	UVic administrators of O365 improperly configure UVic tenant resulting in exposure of sensitive or personal information.	Systems staff will have technical training to ensure they understand the settings and how to configure the environment. Third-party consultants have also been engaged to review and make recommendations on configurations and best-practices.	Low	High
3.	Non-compliance with FIPPA privacy notification requirement.	All users receive a detailed privacy notification at sign-up for the O365 service. Students are advised of the use of the O365 tool in the course syllabus.	Low	Low

4.	Individuals may not wish to have their information, including contact information, shared with Microsoft.	Guidance for faculty, staff, and students in place. Faculty and staff member AD attributes are not personal information as defined in FIPPA. Students must consent to this disclosure in order to take some classes at UVic.	Low	Low
5.	Unauthorized interception or access to personal information transmitted by or stored in the system	Microsoft has reasonable security controls in place. It uses encryption and UVic administrators will ensure that identified vulnerabilities are patched. Also, UVic global configurations minimize the personal information that will be collected and stored.	Low	High
6.	Individuals share sensitive customer content with unauthorized individuals	Instructors and staff receive privacy training. There is training available so they can be aware of the principles that govern the protection of privacy and the disclosure of personal information.	Low	Low
7.	Personal information is retained longer than required	We have limited this risk by limiting the amount of personal information stored by Microsoft.	Low	Low
8.	Users are not appropriately authenticated, leading to unauthorized access to personal information	Access to UVic faculty, staff and students is via NetLink ID. Access to community members is via emailed invitation. However, any recipient can email the invitation to others without limitation. Program design, through limiting the sensitivity of recorded information, limits this risk.	Low	Low
9.	Faculty or staff may not have appropriate security controls in place if they are delivering classes while working remotely.	UVic has as guidance in place for remote working.	Medium	Low
10.	Vendor may change terms of use of the service in a manner that adversely impacts FIPPA compliance.	UVic will negotiate its enterprise license to address this, as well as develop appropriate exit strategies as required.	Low	Medium
11.	Inappropriate use of 0365 beyond what was intended may result in compliance issues.	UVic will clearly articulate and continue to evolve service catalogue language around appropriate usage.	Medium	Low

3.0 Security of Personal Information

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

Many international, industry, and regional organizations independently certify that Microsoft cloud services and platforms meet rigorous security standards[3] and are trusted. Although not all the standards apply to the UVic's implementation of Office 365, they are a good indicator of the depth and breadth of Microsoft's compliance.

The standards most applicable to UVic'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

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

UVic undergoes regular audits and assessments (e.g. IT General Controls, PCI), and Microsoft's data centres and services are subject to other robust third party audits and assessments (e.g. ISO27001, ISO27018, SOC 2). Therefore any security or privacy breaches are most likely to be caused by misconfiguration or misuse by our own faculty and staff, which could also happen with our own on-premise service offerings. As such, we are confident that the O365 offerings are at least as secure as our "standard" Microsoft service offerings in our own data centre e.g. Exchange, SharePoint, Netdrive, and are therefore suitable for data classified as "highly confidential" per the UVic Information Classification Procedures[4].

We also recognize that some research projects Sec. 15 come with very specific security requirements (e.g. physical data separation) for which we will assess the suitability of O365 on a case-by-case basis.

The tables below provide descriptions of the comprehensive controls and security safeguards available in Office 365[5].

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,	Administrators can use these reports to determine how information is being used within the organization, manage

[3] 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

[4] UVic Information Classification Procedures available at: https://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf#page=14

[5] 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=0ahUKEwif7L2r5-7OAhUJ4GMKHWooALcQFghFMAA&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**
	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.	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 • 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	**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:**

Data Privacy		
Safeguard	**Description**	**Additional Information**
	necessary for support or operations, and then revoked when no longer needed.	• 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.	
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.	

Data Privacy		
Safeguard	**Description**	**Additional Information**
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. 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.	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.

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 datacentre over a network to a customer device. All email content is encrypted on disk using BitLocker 256-bit Advanced Encryption Standard (AES) encryption.
Data at Rest	Office 365 and other SaaS services use encryption at rest to protect customer data on Microsoft servers.	Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, and search

Data Encryption and Rights Management		
		content index files, transport database files, transport transaction log files, and page file OS system disk tracing / message tracking logs.

Identity and Access		
Safeguard	**Description**	**Additional Information**
UVic controls access to 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	**Service Security:** Secure engineering (SDL), access control and monitoring, anti-malware

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

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
Microsoft Digital Crimes Unit	Microsoft's Digital Crimes Unit (DCU) seeks to provide a safer digital experience for every person and organization on the planet by protecting vulnerable populations, fighting malware, and reducing digital risk.	
Prevent Breach, Assume Breach	In addition to the Prevent Breach Practices of threat modeling, code reviews, and security testing, Microsoft takes an "assume breach" approach to protecting services and data: • Simulate real-world breaches • Live site penetration testing • Centralized security logging and monitoring • Practice security incident response	From a people and process standpoint, preventing breach involves auditing all operator/ administrator access and actions, zero standing permission for administrators in the service, "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and segregation of the employee email environment from the production access environment. Employees who have not passed background checks are

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

Proactive Testing & Monitoring		
Safeguard	**Description**	**Additional Information**
	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 • 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. 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.	**Built-In Security:** Within Microsoft datacentres, access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting

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

3.3 Does your department rely on security policies other than the Information Security Policy?
No.

3.4 Please describe any access control and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.
Administrative functions within the O365 environment are managed by University Systems, and access to administrative functions is protected with multifactor authentication (MFA).

3.5 Please describe how you track who has access to the personal information.
Changes to administrative capabilities are requested and tracked through Request Tracker (rt.uvic.ca).

4.0 Accuracy/Correction/Retention of Personal Information

4.1 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 university notify them of the update, correction or annotation?

Individuals are able to update or correct their account details by contacting the appropriate administrative authority at the University of Victoria (e.g. Human Resources, Office of the Registrar) to update their name, or University Systems to update their NetLink ID, which are used as data sources for attribute release to Microsoft.

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

Real-time participation in meetings (e.g. interviews) or classes may result in decisions that directly affect an individual, however the Microsoft O365 platform itself is the venue in which those decisions are made, but is not the source of or the basis for the decisions.

4.3 If you answered "yes" to question 4.2, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

UVic's Records Management Policy (IM7700) and Directory of Records sets out the retention period for UVic records. The use of O365 by UVic employees must comply with IM7200.

Individuals who have personal information stored inside O365 have the right under FIPPA and Protection of Privacy Policy GV0235 to request correction of that information upon request to the department who is responsible for the record.

4.4 If you answered "yes" to question 4.2, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Information stored is subject to UVic's Records Management Policy (IM7700) and Directory of Records.

5.0 Further Information

5.1 Does this initiative involve systematic disclosures of personal information? If yes, please explain.

This initiative does not involve the systematic disclosure of personal information.

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

This initiative does not involve disclosure of personal information for research purposes.

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

No.

5.0 Comments and Signatures

Associate Vice-President University Systems & Chief Information Officer: Wency Lum

Comments:	
Date:	
Sign-Off:	

Administrative Authority: [[Name]]

Comments:	
Date:	
Sign-Off:	

Portfolio Manager: [[Name]]

Project Comments:	
Date:	
Sign-Off:	

Consultation Checklist

IT Projects

The following leaders in each functional area can refer you to an appropriate subject matter expert to help develop the technical elements of your project plan and ensure it is complete.

Service Area	Impact? (Y/N)	Leader	Expert Consulted	Date of Consultation
Senior Management				
Associate Vice-President University Systems and Chief Information Officer		Wency Lum		
Director, Academic & Admin Services, and Chief Information Security Officer		Nav Bassi		
Director, Infrastructure Services		Ron Kozsan		
Director, UVic Online Services		Garry Sagert		
Academic & Administrative Services and Information Security Office				
Client Technologies		Lance Grant		
Computer Help Desk		Marcus Greenshields		
Desktop Support Services		David Street		
Information Security Office		Eric van Wiltenburg		
Infrastructure Services				
Data Centre Services		Kim Lewall		
Network Services		Jane Godfrey		
Research Computing Services		Ryan Enge		
UVic Online Services				
Development Services		Ivan Petrovic		
Production and Technical Support		Rizwan Bashir		
Project Management Process and Budget				
Administrative Officer		Trish Kearley		
Project Management Office		Scott Thompson		
Other Consultations				
Privacy Office		[Expert Consulted]		
[Department/Unit]		[Expert Consulted]		

Revision History

Version	Date	Author	Comments
1.0	April 28, 2020	Garry Sagert	Initial Draft
1,1	April 30, 2020	Brad Weldon	Feedback from CPO

Appendix A – Synchronized AD Attributes

The table below includes the attributes from the Sec. 15 that will be synced with the global MS Active Directory at account creation and approximately every 30 minutes.

Attribute	Mandatory	Requirement
accountEnabled	TRUE	Status of user account
accountName	FALSE	Required for human usability
cn	FALSE	NetLink ID
countryCode	FALSE	Has bearing on locale for MS
department	FALSE	UVic department
displayName	FALSE	Preferred name + Surname
distinguishedName	FALSE	Full LDAP account ID (includes NetLink ID)
givenName	FALSE	First name
mail	FALSE	Email address
mailNickname	FALSE	Email alias
msRTCSIP-ApplicationOptions	FALSE	Teams options
msRTCSIP-DeploymentLocator	FALSE	Fully qualified domain name (FQDN)
msRTCSIP-Line	FALSE	Contains the device ID (either the SIP URI or the TEL URI of the phone the user controls) used by Teams client for telephony
msRTCSIP-OptionFlags	FALSE	Teams options that are enabled for the user
msRTCSIP-OwnerUrn	FALSE	Uniform Resource Name (URN) of the owner for an application contact.
msRTCSIP-PrimaryUserAddress	FALSE	SIP address (equivalent of UVic phone extension) of a given Teams user.
msRTCSIP-UserEnabled	FALSE	User status for Teams.
objectSid	FALSE	Operational attribute
onPremisesUserPrincipalName	FALSE	NetLink ID
proxyAddresses	FALSE	Required for teams
pwdLastSet	FALSE	Date of last password change
securityEnabled	FALSE	Indicates whether the group is security-enabled
sn	FALSE	Surname
sourceAnchor	TRUE	Uniquely identifies an object as being the same object on-premises and in Azure AD
thumbnailPhoto	FALSE	Will be synced if present but not required
userPrincipalName	TRUE	NetLink ID
usageLocation	TRUE	Involved in telling MS this is Canada - need it for valid license validation
C	TRUE	Assists with "usageLocation" attribute

BCNET

Privacy Impact Assessment

Microsoft Azure PIA#

Part 1 – General

Name of Organization	BCNET		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd.		
Email:	bev@hooperconsulting.ca	Phone:	250 896-4272
Program Manager:	Dean Crawford		
Email:	Dean.crawford@bc.net	Phone:	250 721-8477

1. Description of the Initiative

BCNET is taking the lead on the development of this Privacy Impact Assessment (PIA) of Microsoft Azure (Azure) on behalf of its members and affiliations.

BCNET is a federally incorporated not-for profit, services information technology organization that represents the interests of 43 member (to include 25 publicly funded) institutions made up of universities, colleges, institutes, and research institutes across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing and IT services.

This unique and collaborative shared services model provides a multitude of benefits to its members from reducing and containing costs and increasing spending power, to decreasing duplication and improving service quality and productivity. The model cultivates a strong community, where members actively engage with peers to share, explore and develop innovative ideas and solutions as they tackle a broad spectrum of common and unique research and education technology challenges and topics. BCNET strives to add value to its membership by leveraging an advanced network that provides economies of scale to maximize efficiencies and drive down collective costs, while at the same time, continuing to facilitate collaborative innovative solutions that meet the needs of their stakeholders in support of world-class research and education.

As government, education, and non-profit organizations (public-sector) face unique challenges to accomplish complex mandates with limited resources, they are overwhelmingly turning to the power and speed of cloud computing technology/infrastructure to include Azure, to serve citizens more effectively, achieve scientific breakthroughs, and educate students etc.

BCNET

Privacy Impact Assessment

Microsoft Azure PIA#

A key component of facilitating innovative information technology (IT) solutions through this advanced network is ensuring they are hosted, accessed, managed and protected within a secure environment in accordance with Provincial (*Freedom of Information and Protection of Privacy Act,* FOIPPA) privacy laws, regulations and controls. The BCNET community has recently been advised that effective immediately, applications that were previously hosted locally by service providers may now be moving to Azure.

BCNET is committed to ensuring that the use of Azure meets provincial privacy and security legislative requirements, policies and practices, and works with its members to strive to reduce the privacy risks associated with the legislative requirements accordingly. These privacy risks are managed through a combination of technical, administrative and physical controls that mitigate the associated risk. This privacy impact assessment (PIA) is intended to allow BCNET members who wish to utilize applications hosted by Azure to proceed, and to ensure that these services are offered and provided in a way that is compliant with the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Azure is a growing collection of integrated cloud services that developers and IT professionals use to build, deploy, and manage applications through a global network of data centres. Azure is available in 140 countries divided into 42 regions. Azure has two regions in Canada with data centres in Canada Central (Toronto) and Canada East (Quebec City).

Azure is a public cloud service operating at a Hyperscale level. Hyperscale cloud computing is a concept that involves computing resources capable of increasing size rapidly, efficiently and indefinitely with a high degree of automation.

Members can choose from a series of services to develop new, or run existing applications while using features and computing resources associated with cloud-based services. The various offerings under the Azure umbrella allow members to operate in their own 'space' on the cloud but at the same time, interact with other on-premises or cloud applications.

Azure provides both Platform-as-a-Service ("PaaS") and Infrastructure-as-a-service ("IaaS") as well as support for a variety of programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems. When a PaaS offering is used by a member it allows control of applications (and possibly configuration settings), but not management or control of the network, servers, operating systems or storage. When an IaaS offering is used, it allows the member to control and deploy the operating system, storage and applications. It also allows limited control of some network components (eg. Host Firewalls).

Iaas has three components: Compute, Storage and Networking. Paas has seven components: Compute, Web & Mobile, Developer Services, Data, Analytics & IoT, Storage and Networking.

Additional information regarding the Microsoft Azure platform and its services may be found at:

https://azure.microsoft.com/en-ca/.

https://azure.microsoft.com/en-ca/regions/services/

2. Scope of this PIA

This PIA has been developed with a focus on the privacy protection and security measures deployed by Microsoft Azure in the Canadian Cloud environment to identify and assess potential vulnerabilities to BCNET members and the community at large. This PIA focuses on the information BCNET members provide to enable their subscriptions to Azure IaaS and PaaS services. As Members have full control of the data and applications that they host within their Azure subscriptions, those uses are outside of the scope of this PIA. Azure Active Directory contains subscription information (business contact) for the members only.

This PIA does not speak to the contractual requirements and responsibilities of BCNET members in meeting their privacy obligations when entering into service agreements with Microsoft Azure.

3. Related Privacy Impact Assessments

A comprehensive Foundational PIA (December 2016) has also been completed on this initiative which focuses on the project in detail from a nationwide perspective by Microsoft.

4. Elements of Information or Data

Administration data (business contact information only) will only be provided by the members to Microsoft Azure.

In this context, the personal information (PI) is the PI that is required and provided directly from individuals to the members to participate in any BCNET member's activity or program. The management, collection and control of all personal information from the individual will continue to be the responsibility of the BCNET member (the provincial or public-sector organization managing the application /operating system). Examples of personal information include: name, address, date of birth, phone no., gender etc.

Microsoft has no access to member's virtual machines and/or data at anytime in Azure.

5. Storage or Access outside Canada

Sec. 15, Sec. 21

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;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	NA
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.	NA
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);	No
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	N/A

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**

See https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios.

9. **Risk Mitigation Table**

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes. (within the Azure environment)	Employee Code of conduct and non-disclosure agreements; password-protected access, user access based on need to know, permission restrictions, role based access controls, Just In time administration, time bound administration and monitoring.	Low	High
2.	BCNET member personal information data is compromised during transmission from the member to Azure	Sec. 15, Sec. 21	Low	High
3.	Azure Cloud security breach	Microsoft employs breach strategies and remediation protocols.	Low	High

10. Collection Notice

The BCNET member is responsible for ensuring the appropriate collection notification (for the specific application/program) is in place prior to the collection of personal information and before transmission to Azure.

Part 3 – Security of Personal Information

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

BCNET:

Members and their service providers are responsible at all times for ensuring the physical security of all data while in their custody and/or control (including data at rest and in transit) and must meet all the applicable physical security standards required by their organization.

Azure:

Sec. 15, Sec. 21

https://aka.ms/MCSCE

**Microsoft notes that security is a shared responsibility. "Who is responsible for what (in terms of security) depends on the cloud service model you use. With IaaS, the cloud service provider is responsible for the core infrastructure security, which includes storage, networking and compute (at least at the fabric level – the physical level)."*

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

BCNET:

Members and their service providers are responsible at all times for ensuring the technical security of all data while in their custody and/or control (including data at rest and in transit) and must meet all the applicable physical security standards required by their organization.

Azure:

Sec. 15, Sec. 21

13. Does your branch/department rely on any security policies?

BCNET:

Members and their service providers are responsible for the deployment, dissemination and administration of all organizational security policies etc. as it relates to the handling and management of personal information in their custody and/or control.

Azure:

https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx

https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx

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

BCNET

Members and their service providers are responsible for the strict management and administration of user access based on need to know including the maintenance and enforcement.

Azure:

Sec. 15, Sec. 21

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

BCNET:

Members and their service providers are responsible for ensuring that access to all personal information in their custody and/or control is controlled, monitored, and reviewed/audited on a regular basis.

Azure:

Sec. 15, Sec. 21

Sec. 15, Sec. 21

Part 4 – Accuracy/Correction/Retention of Personal Information

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

    BCNET members are responsible for providing personal information updates to Azure via data transfer (Microsoft has a formal process to allow a member to correct/amend inaccurate personal information as appropriate in compliance with ISO 27018).

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

    No.

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

    N/A

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

    N/A

Part 5 – Further Information

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

No.

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

No.

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

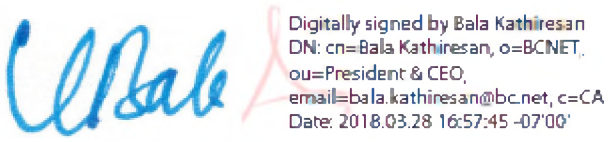
No.

BCNET

Privacy Impact Assessment

Microsoft Azure PIA#

Signed on Behalf of BCNET:



Bala Kathiresan President and Chief Executive Officer BCNET	Signature