Privacy Impact Assessment (PIA)

Version 0.4e

Microsoft Office 365

Program Manager:
Alex Diaz
Director of Infrastructure and Operations,
Office of the Chief Information Officer

Author:
Crawford Millen
Security Architect
Office of the Chief Information Officer

Date:
2021-03-10

UNIVERSITY OF THE FRASER VALLEY

Version History

Ver	Date	Author	Description
0.1			
0.2			
0.3			
0.4			
0.5			
0.6			
0.7			
0.8			
0.9			
1.0			
1.0b			

s. 22

Table of Contents

Part 1 – General

Name of Department/Branch:	ITS		
PIA Drafter:	Crawford Millen, Director Information Security, OCIO, UFV		
Email:	crawford.millen@ufv.ca	Phone:	X4889
Program Manager:	Alex Diaz, Dir Infrastructure & Operation, OCIO, UFV		
Email:	alex.diaz@ufv.ca	Phone:	X5320

The objective of a Privacy Impact Assessment (PIA) is to determine how a program or service, could affect the privacy of individuals. It aims to identify and reduce any possible negative effects on privacy that might result from implementing a program or service. This specific PIA's objectives are first to determine if there are privacy issues or risks associated with the University of the Fraser Valley's proposed adoption of Microsoft Office 365 (M365); and if so, to provide recommendations and mitigation strategies. This will include identification of issues with compliance with regard to the *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165 ("FIPPA"), and determine how UFV can avoid or minimize the loss, damage, misuse or abuse of personal information.

In addition, this PIA is a way for UFV to demonstrate its commitment to protecting the privacy of individuals, promote transparency and accountability, and contribute to continued public confidence in the way that the University of the Fraser Valley (UFV) manages personal information. It helps prepare UFV to implement the project with proper consideration of relevant privacy requirements, including those privacy requirements in the architecture, design, and configuration.

This PIA is guided by the requirements laid out in FIPPA:

Section 69(5.3) of the Freedom of Information and Protection of Privacy Act (FIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

This PIA also explains the process UFV followed, the factors considered, and the steps taken or will undertake to make sure this decision does not adversely affect the privacy of the UFV community. This undertaking is part of UFVs commitment to make careful and considered decisions in safeguarding the personal information

of staff, students, and all other stakeholders. It explains our reasons for the move, the context within which we made the decision, the key privacy risks identified as potential barriers to cloud use, and the reasons these can be overcome.

This report is meant to aid information technology, information management, and access to information and privacy staff, along with the directors and executive directors, to be better informed about the risks, and recommend appropriate safeguards in order to securely transition to the cloud. It also assumes that the M365 A3 package will be used and thus all of its associated services are available to UFV. While the UFV initiative focuses on the implementation of Exchange Online, since this implementation will require both Azure Active Directory (AAD) and M365, therefore this PIA covers these technologies.

1. Description of the Initiative

The current (2021) UFV student email service (Zimbra) is approaching the end of support and requires replacement. UFV is proposing the adoption of Microsoft Exchange Online ("MEO") hosted in Microsoft's Azure Cloud Service for the delivery of student email services. The suite of tools offered through M365 represents an improvement to the university's status quo in the form of ubiquitous email, calendaring, larger inbox quotas, and an optional web interface for users. This initiative will not include migration of student mailboxes and existing email; which will be retained on a Zimbra server hosted in the UFV data center.

Microsoft Office365 is the name for Software as a Service ("SaaS") subscription plans that include access to Microsoft Office applications plus other productivity services. These connected services are hosted in Microsoft data centers and enabled over the internet, colloquially referred to as "cloud" services. Microsoft Canada's cloud services provide an opportunity for modernization, increased agility, and robust information security and privacy practices, all while lowering the overall cost and complexity of delivered information technology services. In order to meet the expectations of stakeholders, while providing reliable information services, UFV must move toward more cost-effective, innovative, and secure technological solutions. Microsoft cloud services meet these requirements with features that cannot be accomplished with current technical capacity.

This project represents a shift in the way UFV provides technology services to staff and faculty. Student email will be stored off-campus in data centres that are run by Microsoft within Canada. The addition of document collaboration tools will also result in data being stored in off-campus data centres. This departure from internally managed email/document collaboration requires the need to establish an appropriate level of trust with Microsoft. Although Microsoft ensures the security of the services and information stored on its systems, UFV will be responsible for the management and administration of information, including data security policies, classification, and retention.

2. Scope of this PIA

The scope of this PIA is centered on the UFV's adoption of MEO, a component of Office 365 ("M365"), a cloud-based SaaS collaboration and productivity suite. The technical details are aligned with version 2101 of Office365, which was released on January 26, 2021. This version introduced improvements and additional data privacy controls. The technical materials referenced are were part of the s. 17, s. 15(1)(l)

Within scope is the personal information data that flows between UFV's on-premises directory, and the Azure registry being processed in the Microsoft data centres. Also, the processing of personal data and Diagnostic Data, as defined in Section 4 below when using the selected Office365 version 2101 on UFV's standard operating system Windows 10 build 1909. In addition, the processing of personal information stored within the data centres managed by Microsoft for supporting Office services.

Included in this analysis are these specific components:

- Azure Active Directory (AAD),
- Microsoft Exchange Online (MEO),
- Office 365 ProPlus (aka Microsoft365, including Outlook, Excel, Word, PowerPoint, OneNote)
- Office for Web (aka "office.com") ,
- Teams

The PIA is limited to the processing of user and Diagnostic Data by the specific services and applications mentioned and does not address the use of Azure as either Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

3. Related Privacy Impact Assessments

In 2019 UFV performed a Privacy Impact Assessment of Office365 (UFV-PIA M365) for the migration of the UFV staff and faculty from on-premise Exchange to Exchange Online. The conclusion of the M365 PIA was that the implementation of M365 while introducing new technology was compliant with *FIPPA.*

UFV has performed a s. 17, s. 15(1)(l)

Other BC institutions have conducted PIAs, and these have been referenced in preparing this report. BC Ministry of Technology conducted PIA (#MTICS16024) to assess the privacy impacts of utilizing M365 for official government systems. This assessment included the Microsoft Office365 and Azure computing environment, and how the service met BC Privacy legislation requirements.

s. 17, s. 15(1)(l)

4. Elements of Information or Data

This PIA uses the terms Contact Information (CI), Personal Identity Information (PII) and Personal Information (PI) as defined in Schedule 1 of FIPPA.

> *"personal identity information" means any personal information of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual;*
> *"personal information" means recorded information about an identifiable individual other than contact information;*
> *"contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;*

To describe the data elements used in the initiative, we will describe the types of data used, who controls the data types, the flow of information, and the elements that can potentially hold CI, PI or PII data.

Data Types

With regard to this initiative, there are four types of information shared with, collected and used by Microsoft in delivering M365 services:

- Diagnostic Data,
- Functional Data,
- Authentication Data,
- Customer Data.

Diagnostic Data is produced by system components for the purpose of maintaining and providing the service. While this may be produced by user activity, it is not customer information or generated content. Diagnostic Data is used to keep services secure and up-to-date, detect, diagnose and remediate problems, and facilitate product improvements. Microsoft defines Diagnostic Data as referring only to telemetry data collected about the specific use of Microsoft Office software.

Functional Data is data that is necessary only for a short period of time, to communicate with services on the Internet, including Microsoft's own apps and services. Examples of Functional Data are the data stream necessary to allow the user to authenticate, SSL certificates, or verification of a valid M365 service license. The key difference between Functional Data and Diagnostic Data is that Functional Data should be transient.

Authentication Data is used by Microsoft to facilitate authentication and identification of each user. This includes the user's userPersonalName (the user's login ID, referred to hereafter as "UPN"), the user's full name, and a Microsoft token.

Customer Content is user-created content which is defined as information in the user's profile, emails, calendar and other information that the user themselves decides to place into the service. This information is created by the user and may be personal, work-related, administrative, research or educational and may contain personal information that they place into the service.

Control of Data

Under the privacy requirements, *Diagnostic* and *Functional Data* meet the FIPPA conditions for:

> *33.2(1)(p.2) if the information is metadata that*
>
> *(i) is generated by an electronic system, and*
>
> *(ii) describes an individual's interaction with the electronic system,*
>
> *and if,*
>
> *(iii) if practicable, personal information in individually identifiable form has been removed from the metadata or destroyed, and*
>
> *(iv) in the case of disclosure to a service provider, the public body has prohibited any subsequent use or disclosure of personal information in individually identifiable form without the express authorization of the public body;*

Therefore, these data types do not have data that correlates with the definition of PI or PII contained under FIPPA (2019).

Customer Content is placed into the SaaS by the end-user, and this consists of data, information (including potentially PI of staff, students, alumni, and faculty), documents, spreadsheets and other artifacts that are authored, edited, communicated, maintained and eventually deleted by UFV users. Therefore, PII may be stored in Azure by either the user themselves (voluntary) or as part of UFV's normal operations.

In both cases protection of such PII within a SaaS is regarded as the responsibility of UFV, not the data processor (Microsoft). As part of the demarcation of responsibility, the Customer Data placed into the service will be protected by physical or logical controls configured and managed by UFV. This may include Data Loss Prevention and Data Classification capabilities that are offered in M365.

Customer Content is not accessible or visible to Microsoft administrators, except in exceptional maintenance scenarios. In these cases, Microsoft, with explicit consent from UFV, would be able to investigate and/or fix an ongoing problem within the UFV tenant (i.e. the space used by UFV in the

cloud to store its data) or cloud services. This would be consistent with UFV's commitment to FIPPA as any disclosure would be compliant with the following:

> *33.1(1)(ii) in the case of disclosure outside Canada, results in temporary access and storage that is limited to the minimum period of time necessary to complete the installation, implementation, maintenance, repair, trouble-shooting, upgrading or data recovery referred to in subparagraph (i);*

Authentication Data is used to uniquely identify the individual and includes UPN and password. This information will remain within UFV's control. Information about Azure users is primarily stored in the Azure Active Directory ("AAD"). AAD is a version of Microsoft's Active Directory that runs in the cloud and is responsible for authentication and authorisation. UFV's tenant administrators will have control over UFV's AAD instance, for example, to manage account information.

User account information in the AAD registry is synchronized with the information stored in UFV's on-premise AD via "Microsoft AD Connect". The on-premise Active Directory account's UPN is used as the unique identifier to link the AD and AAD accounts. Synchronisation ensures that account information in AD is securely and promptly copied to the corresponding UFV account in AAD.

The replication mechanism in AD Connect can be configured to replicate all or specific objects, and selected attributes from AD to AAD. For Exchange hybrid mode, a limited number of mailbox specific attributes are also written back to AD from AAD. The full list of AD objects and account attributes that are copied to AAD are detailed in the next section.

Authentication Data stored in the AAD may be accessed by Microsoft staff providing requested level 2 support in the event that UFV's resources are unable to resolve an issue. Similar to Customer content protections, such authorised access would be compliant with FIPPA under 33.1(1)(p.1). For technical details on the directory synchronisation see the s. 17, s. 15(1)(l).

Data Elements

The following tables list the possible data elements that are replicated from UFV's on-premise AD to AAD. The first table lists the anticipated standard AD objects replicated to UFV Azure tenant for M365. These represent different types of entities represented in UFV's AD.

Active Directory Objects replicated to Azure Active Directory		
Object Types	**Source**	**Comment**
Computer	UFV AD	No PII in object
Contact	UFV AD	No PII in object
Container	UFV AD	No PII in object

Active Directory Objects replicated to Azure Active Directory		
Object Types	**Source**	**Comment**
Domaindns	UFV AD	No PII in object
foreignSecurityPrincpal	UFV AD	No PII in object
Group	UFV AD	No PII in object
organizationalUnit	UFV AD	No PII in object
User (inetorgPerson)	UFV AD	AD User Objects may contain PII (see AD Attributes)

This table lists the required Active Directory user object attributes replicated to Azure, including FIPPA data type designation. For clarity, attributes not explicitly listed are not replicated.

Active Directory User Attributes Replicated			
Attribute Name	**User**	**Type**	**Description**
accountEnabled [1]	X		Defines if an account is enabled.
cn [1]	X	CI	Common Name
displayName [1]	X	CI	Customizable name
objectSID [1]	X		AD user identifier used to maintain sync between Azure AD and AD. (system level property)
pwdLastSet [1]	X		Used to know when to invalidate already issued tokens. Used by both password sync and federation. (system level property)
sourceAnchor [1]	X		Immutable identifier to maintain relationship between ADDS and Azure AD. (system level property)
usageLocation [1]	X		The user's country. Used for Azure license assignment. (system level property)
userPrincipalName [1]	X	CI/PII	UPN is the login ID for the user. Most often the same as [mail] value. It is composed of the username and the domain. By default, this attribute is the user's first and last name. For staff and faculty such information is classified as contact information but for students it is personal information

Anticipated AD Exchange specific attributes to be replicated to AAD for Exchange Online. Indicates if data is required for users, contacts, and groups. PII is coded as not PII (N), PII data (Y), contact info (CI). Attributes are coded with (X) if to be replicated (UFV-AD to AAD), and (-) if available but not replicated by UFV.

Exchange Active Directory Attributes to be Replicated in Azure Active Directory					
Attribute Name	**User**	**Contact**	**Group**	**PII**	**Comment**
accountEnabled [1]	X			N	Defines if an account is enabled.
Assistant	-	-		N	UFV - Not Required
altRecipient	X			N	
authoring	-	-	-	N	UFV - Not Required
C	X	X		N	Country Abbreviation
Cn [1]	X		X	CI	Common Name
Co	X	X		N	Country
Company	X	X		CI	Organization (UFV)
countryCode	X	X		N	Region Code
Department	X	X		CI	Department
Description			X	N	UFV -
displayName [1]	X	X	X	CI	Display (alias) Name
dLMemRejectPerms	X	X	X	N	Distribution reject permission list.
dLMemSubmitPerms	X	X	X	N	Distribution submit permission list.
extensionAttribute1	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute10	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute11	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute12	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute13	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute14	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute15	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute2	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute3	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute4	X	X	X	N	Custom attribute from UFV-AD (if required)

Exchange Active Directory Attributes to be Replicated in Azure Active Directory					
Attribute Name	**User**	**Contact**	**Group**	**PII**	**Comment**
extensionAttribute5	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute6	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute7	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute8	X	X	X	N	Custom attribute from UFV-AD (if required)
extensionAttribute9	X	X	X	N	Custom attribute from UFV-AD (if required)
facsimiletelephonenumber	-	-		Y	UFV - Not Synchronized
givenName	X	X		CI	Name
homePhone	-	-		Y	Home Phone Number (Not Synchronized)
Info	-	-	-	N	
Initials	X	X		CI	Single Initial
L	X	X		N	City
legacyExchangeDN	X	X	X	N	DN from legacy Exchange Systems
mailNickname	X	X	X	PI	PI
Manager	X	X		CI	Contact Info
Mobile	X	-		CI	UFV mobile number
msDS-HABSeniorityIndex	X	X	X	N	Hierarchical address book index
msDS-PhoneticDisplayName	X	X	X	N	Phonetic display name of an object
msExchArchiveGUID	X			N	GUID of the user's archived mailbox.
msExchArchiveStatus*	X			N	Online Archive
msExchArchiveName	X			N	Archive Name
msExchAssistantName	X	X		N	Assistant Name
msExchAuditAdmin	X			N	Audit Admin Flag
msExchAuditDelegate	X			N	Audit delegate Flag
msExchAuditDelegateAdmin	X			N	Audit Delegate Admin Flag
msExchAuditOwner	X			N	Audit Owner Flag
msExchBlockedSendersHash *	X	X		N	Exchange Hybrid
msExchBypassAudit	X			N	Boolean if Audit Bypassed
msExchBypassModerationLink			X	N	Group Only

Exchange Active Directory Attributes to be Replicated in Azure Active Directory					
Attribute Name	**User**	**Contact**	**Group**	**PII**	**Comment**
msExchCoManagedByLink			X	N	Group Only
msExchDelegateListLink	X			N	User Attribute
msExchELCExpirySuspensionEnd	X			N	Litigation Hold End Date
msExchELCExpirySuspensionStart	X			N	Litigation Hold Start Date
msExchELCMailboxFlags	X			N	Litigation Hold Flag
msExchEnableModeration	X		X	N	Boolean – M365 Group Moderators
msExchHideFromAddressLists	X	X		N	Visibility of email from GAL
msExchImmutableID	X			N	GUID Immutable Link between AD and AAD
msExchLitigationHoldDate	X	X		N	Litigation Hold Date
msExchLitigationHoldOwner	X	X		N	Litigation Hold Owner
msExchMailboxAuditEnable	X			N	Boolean
msExchMailboxAuditLogAgeLimit	X			N	Numeric
msExchMailboxGuid	X			N	GUID of users Mailbox
msExchModeratedByLink	X	X	X	N	Link to Group Moderator
msExchModerationFlags	X	X	X	N	Moderator Flag
msExchRecipientDisplayType	X	X	X	N	Room Display Type
msExchRecipientTypeDetails	X	X	X	N	Recipient descriptors
msExchRemoteRecipientType	X			N	Recipient Type
msExchRequireAuthToSendTo	X	X	X	N	Authorization
msExchResourceCapacity	X			N	Number of Attendees
msExchResourceDisplay	X			N	Display in Room
msExchResourceMetaData	X			N	Room descriptors
msExchResourceSearchProperties	X			N	Properties of Room
msExchRetentionComment	X	X	X	N	Comment
msExchRetentionURL	X	X	X	N	Location of retention safe
msExchSafeRecipientsHash*	X	X		N	Recipient authentication hash
msExchSafeSendersHash*	X	X		N	Senders authentication Hash
msExchSenderHintTranslations	X	X	X	N	Languages
msExchTeamMailboxExpiration	X			N	Date
msExchTeamMailboxOwners	X			N	group
msExchTemMailboxSharePointUrl	X			N	URL to Sharepoint

Exchange Active Directory Attributes to be Replicated in Azure Active Directory					
Attribute Name	**User**	**Contact**	**Group**	**PII**	**Comment**
msExchUserHoldPolicies *	X			N	Litigation Hold policies
msOrg-IsOrganizational			X	N	Boolean. Constructed Attribute
objectSID	X		X	N	(System Attribute) Used to maintain sync between Azure AD and AD.
oOFReplyToOriginator				N	Boolean. Distribution lists (Not Synced)
physicalDeliveryOfficeName	X	X		CI	Contact Info - UFV address - Replicated
postalCode	X	X		CI	Contact Info - Replicated
proxyAddresses *	X	X	X	CI	Contact Info - UFV address - Replicated
publicDelegates *	X	X	X	CI	Contact Info - UFV address - Replicated
pwdLastSet	X			N	(System Attribute) Used by both password sync and federation
reportToOriginator			X	N	Distribution lists (Group)
reportToOwner			X	N	Distribution lists (Group)
sn	X	X		CI	Surname
sourceAnchor	X	X	X	N	(system Attribute) Immutable identifier to maintain relationship between ADDS and Azure AD
st	X	X		CI	Contact Info - UFV Work street
streetAddress	X	X		CI	Contact Info - UFV Work Address
telephoneNumber	X	X		CI	Contact Info - UFV Office
thumbnailphoto				PI	Not Replicated
title	X	X		CI	Title
unauthOrig	X	X	X	N	email addresses blocked by this mailbox
usageLocation	X			N	(System Attribute) Used for license assignment
userCertificate	X	X		N	Public key certificate
userPrincipalName	X			Y	This is the user's login ID. By default, this attribute is the user's first and last name. For staff and faculty such information is classified as contact information but for students it is personal information
userSMIMECertificates	X	X		N	S/MIME Public Key Certificate
wWWHomePage	X	X		N	

* Attribute used by Hybrid Exchange mode write back.

[1] Attributes required for Azure RMS, Office 365

If personal information is involved in your initiative, please continue to the next page to complete your

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Storage

Microsoft has stipulated that all subscriber application and customer-generated content is stored at-rest in Microsoft's Canadian data centres. All data communications between UFV and the tenant in Microsoft's data centre are encrypted 'in transit' between sites, as well as encrypted 'at-rest' in the data centre. Since UFV information will be stored and processed on data centres located in Canada, data residency requirements will be satisfied.

In 2016 Microsoft opened two data centres in Canada (Canada Central and Canada East) providing data centre level redundancy while providing alignment with data residency requirements. s. 17, s. 15(1)(l), s. 21

[redacted]

Exception for Authentication Data

While Customer Data is stored at-rest only in Microsoft's Canadian data centres, the same is not true of Authentication Data. Authentication data, specifically, the user's User Principal Name ("UPN"), is stored within Microsoft's global private network.

A summary of the details regarding the UPNs of UFV users is as follows:

a. A User Principal Name (UPN) is the name of a user and consist of the login name, @, and domain name – (i.e. : first.last @student.ufv.ca") for employees, their first and last name is considered business contact information but for students it is considered to be personal information;
b. The UPN is propagated (stored) in the Microsoft global network so could be "at rest" in a non-Canadian location;
c. the student email address does not necessarily comprise the student's legal first and last names, but can be different due to collisions in the account namespace. (e.g.: bobsmith14 @student.ufv.ca) and, as stated above, would be considered 'personal information' as defined by FIPPA;
d. The UPN is issued by UFV and the prefix (i.e. the first and last names) can be changed if required by changing the account name;
e. The UPN suffix (@student.ufv.ca) is fixed by the domain;
f. The Azure UPN is synchronized from the UFV AD directory, so must be identical in both;

g. A UPN can be removed from Azure AD.

s. 13 [redacted]

Access

Access to data held within the tenant is protected by Azure's security configuration and Office365 access controls. Properly configured, Azure will grant access to data only to authenticated and authorized users. This configuration is under UFV's control, and area of responsibility. Following best practice models will help ensure data is appropriately protected.

Additionally, customer generated content can also be secured, using a feature called "M365 Lockbox".

s. 17, s. 15(1)(l), s. 21 [redacted]

Diagnostic and Functional Data is generated from the ongoing operation of M365 and Microsoft Azure Cloud Services. This data does not contain explicit personal information, is held within Microsoft's Cosmos data stores residing across the global private network infrastructure and is accessible by authenticated administrators inside and outside of Canada. The Functional Data required for service and maintenance is accessed and contained within Microsoft's global private network.

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) 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

With reference to the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, (amended 2019), personal information processing between Microsoft and UFV can be performed as approved under the following stipulations 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. 33.1(1) (p) if the disclosure

(i) is necessary for

(A) installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment that includes an electronic system, or

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

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

(p.1) if the disclosure

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

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

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

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

(p.2) if the information is metadata that

(i) is generated by an electronic system, and

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

and if,

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

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

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;

AD to AAD Information Flow

The AAD registry performs the same functions as the standard on-premise AD – authentication, and authorization of users to resources. In order to provide ease of administration, and ease of use for the end-users, s. 13

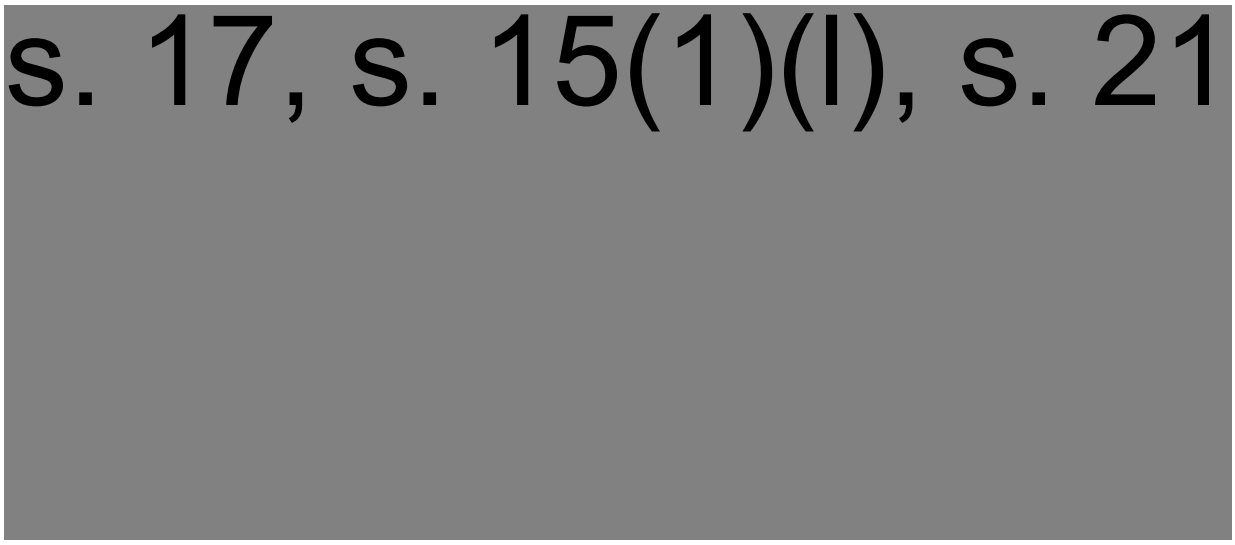

Figure 1: Azure Active Directory Connect

AAD Connect is the preferred option for synchronizing on the premise AD records (computers and users) to matching AAD records. s. 17, s. 15(1)(l), s. 21

The synchronization has several key factors that decide what AD data will be replicated to the cloud. The first factor is the "*sourceAnchor*", a single attribute that will be immutable for the lifetime of the object, used to uniquely identify an object in both AD and AAD. It's used by the synchronizing service to tie the two objects together and, as such, the *sourceAnchor* must never change. UFV will use the AD attribute *objectGUID* as the sourceAnchor. Since the objectGUID is a unique key only in the context of the UFV AD registry, it has no inherent personal data.

The second is the "userPrincipalName", or UPN which UFV students will enter when they sign in. The UPN comes in the form of*[username]@[domain]*, such as *b.smith@student.ufv.ca*. While this is similar to an email, and often is identical to the users email, it identifies the individual and their associated domain. The domain will be mapped by Microsoft to the Azure tenant, and the username will be an individual's unique designation within that tenant instance. The UPN is not considered to be personal information of staff and faculty. To the extent the UPN contains a student's first and last name, it is considered to be personal information of that student.

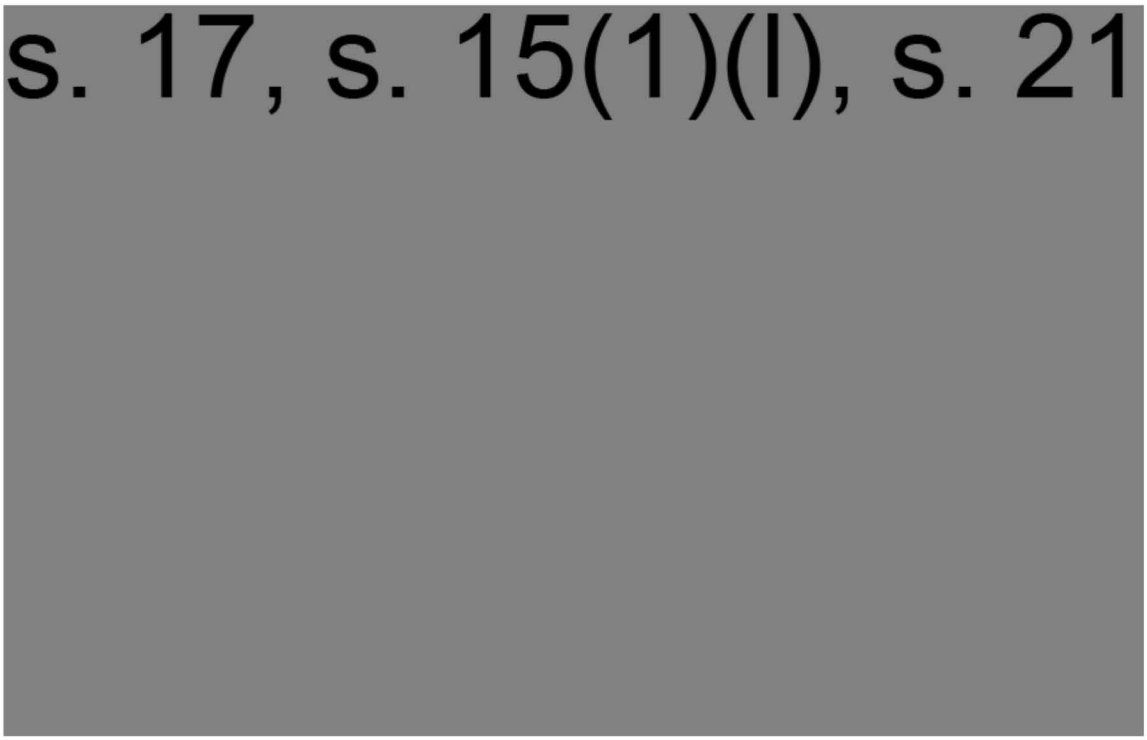

Figure 2: Personal Information Flow -AD Connect

Finally, AAD Connect rules the synchronisation can be adjusted to include or exclude specific attributes, thus allowing data to be retained and managed on at the on-premise registry. The table in "*Question #4 Data Elements*" list the selected elements to be replicated.

Personal Information Flow – AD to AAD			
#	**Description/Purpose**	**Type**	**FIPPA**
1	*AAD established for an individual user (UPN)*	*Disclosure (only as it relates to students who have not changed UPN to be non-identifying)*	*s. 26(c)*
2	*On premise AD account is modified and synchronizes selected CI data with Azure registry*	*Disclosure (only as it relates to students who have not*	s.33.1(1)

		changed UPN to be non-identifying)	
3	*Summary of synchronisation activity is logged by AD Connect on UFV servers*	*Collection*	*26(c)*
4	*Selected data is stored on UFV's tenancy within Microsoft's data center*	*Disclosure*	*33.1(1)*

Exchange Online Information Flow

Exchange Online is the Azure equivalent of the on-premise Exchange server that provides UFV with email and associated services (calendars, meeting scheduling, contacts). Exchange Online stores Customer Data within mailboxes that are hosted within Exchange databases. These databases include user mailboxes, resource mailboxes (e.g. meeting rooms, vehicles), shared mailboxes and public folder mailboxes.

Initially, UFV will be using a hybrid model to transition to Exchange Online. The migration will begin with most users hosted on-premise Exchange, and selected mailboxes hosted in Azure. This helps facilitate a smooth migration as selected user's mailboxes get transferred to Azure while retaining the use of the on-premise Exchange servers. While the hybrid model is in place, using the existing infrastructure, UFV can leverage the Barracuda mail security gateways and services. Once all mailboxes have been migrated, the process can conclude with decommissioning the on-premise systems, and routing email directly to Exchange Online.

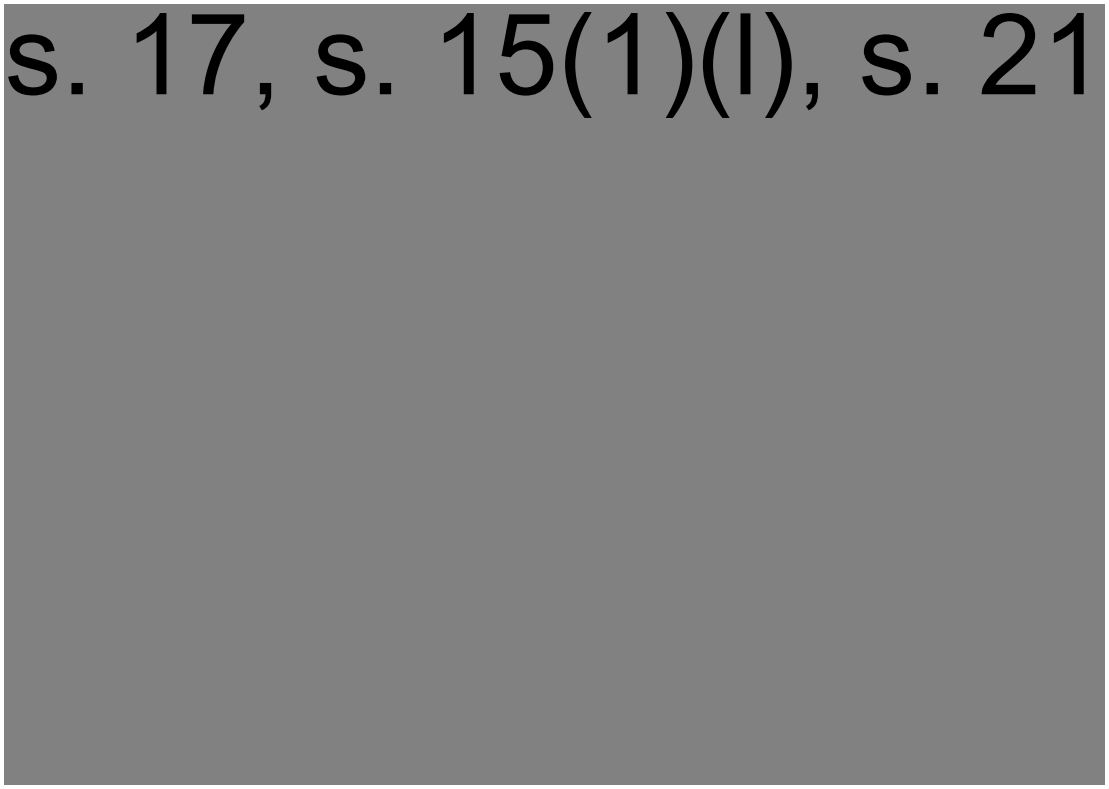

Figure 3: Microsoft Exchange Online Hybrid

Data held within a user mailbox data includes emails and email attachments, calendaring and “free/busy” information, contacts, tasks, notes, groups, and inference data. 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.

Personal Information Flow - Exchange			
#	Description/Purpose	Type	FIPPA
1	*Exchange mailbox is established for an individual user*	*Collection Disclosure (only as it relates to students who have not changed UPN to be non-identifying)*	*26(c),33.1(1)*
2	*User sends/receives emails from mailbox that may/may not contain personal information*	*n/a*	*n/a*
3	*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)*
4	*Email is stored on UFV's tenancy within Microsoft's servers*	*Disclosure*	*33.1(1)*
5	*Exchange system logs and other data are stored on UFV's tenancy within M365*	*Disclosure*	*33.1(1)*
6	*Approved access by Microsoft Engineer to customer content for the purpose of requested service support*	*Disclosure*	*33.1(1)*

9. Risk Mitigation Table

Risk	Pro-bability	Impact	Microsoft Measure	UFV Measures
#1: Unauthorized system access	Low	High	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#2: Unauthorized access to PII within Azure/M365	Low	High	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#3: Misuse of data by authorized users	Med	High	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)

Risk	Pro-bability	Impact	Microsoft Measure	UFV Measures
#4: That PI data may be stored or accessed outside Canada	Low	Med	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#5: PII leakage via the collection of telemetry data	Low	Med	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)

Risk	Pro-bability	Impact	Microsoft Measure	UFV Measures
#6: Unlawful collection and storage of sensitive/ classified/special categories of data	Low	High	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#7: Lawful request for access by government	Low	Med	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#8: Notification of Breach	Med	Med	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#9: System generated data may contain PII	Med	Low	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)

Risk	Pro-bability	Impact	Microsoft Measure	UFV Measures
#10: PII leakage via Azure and M365 micros-services outside of Canada	Med	Low	s. 17, s. 15(1)(l)	s. 17, s. 15(1)(l)
#11: Perception of PII Vulnerability	Med	Low		s. 17, s. 15(1)(l)

10. Collection Notice

s. 13 [redacted]

Part 3 – Security of Personal Information

A core principle of privacy protection is the use of information only as necessary to fulfill the stated purpose. The Microsoft M365 solution should therefore collect, use and disclose a minimal amount of the user's personal information to achieve the solution's purpose. UFV respects the rights of users' privacy, in accordance with university policies and relevant legislation.

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

s. 15(1)(l), s. 17, s. 21, s. 13 [redacted]

Standards Compliance

Microsoft contractually commits that Azure in-scope services have implemented security safeguards to help UFV protect the privacy of individuals, based on established industry standards. This means Microsoft has had independent auditors assessed their practices in risk, security, and incident management; access control; data integrity protection; and other areas. Microsoft's M365 complies with the following control standards and frameworks: ISO 27001, ISO 27002 Code of Practice, ISO 27018 PII Code of Practice, SSAE 16 SOC 1 Type II, and SSAE 16 SOC 2 Type II.

The major international standards relevant to UFV's privacy requirements are:

- **ISO 27001 –** the International Standards Organization's comprehensive set of benchmarks includes a rigorous set of physical, logical, process and management controls defined by ISO 27001:2013;
- **ISO27018 -** code of practice for the protection of personal data in the cloud. Based on ISO security standard 27002 and provides implementation guidance on ISO27002 controls applicable to public cloud Personally Identifiable Information (PII).

Microsoft allows public review of available independent audit reports for Microsoft's Cloud services. The reports, which provide information about compliance with data protection standards and regulatory requirements, can be accessed at the Microsoft Service Trust Portal at:

https://servicetrust.microsoft.com/

Through the STP, Microsoft offers a searchable archive of compliance reports and trust resources, including:

- SOC 1 / SSAE 16 / ISAE 3402 Independent Audit Reports
- SOC 2 / AT 101 Independent Audit Report
- ISO 27001 (including 27018 controls) Independent Audit Report
- PCI/DSS Independent Audit Reports
- FedRAMP

The available audit reports subjects include Azure, Office 365, InTune, Dynamics, and Windows.

s. 17, s. 15(1)(l), s. 21

Security Breach Protocols

s. 17, s. 15(1)(l), s. 21

s. 17, s. 15(1)(l), s. 21

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

s. 17, s. 15(1)(l)

AUTHENTICATION

s. 17, s. 15(1)(l)

PERMISSIONS

s. 17, s. 15(1)(l)

Role Based Access Control (RBAC)

s. 17, s. 15(1)(l)

ADMINISTRATIVE ACCESS

s. 17, s. 15(1)(l)

LOGGING

s. 17, s. 15(1)(l)

DATA LOSS PREVENTION

s. 17, s. 15(1)(l)

s. 17, s. 15(1)(l) [redacted]

SUMMARY
Azure and M365 feature technical safeguards to protect the data in the system. These measures combined with UFV's controls and procedures ensure proper access to data. Unless explicitly granted, UFV 's M365 implementation is not accessible to anyone outside the UFV. For authorized users, the principle of least privilege is used to grant access to data stored in UFV's Azure tenant.

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

UFV's ITS department respects the rights of users' privacy, in accordance with university policies and relevant legislation. As stated in the Universities Acceptable Use of Computer and Network Resources, UFV will not access a user's account unless they are investigating a case of system abuse or otherwise acting in accordance with FIPPA.

As the SaaS provider, Microsoft supports the appropriate controls for PI data by providing contractual provisions expressed in documents placed online in the Microsoft Trust Centre.

Key policy documents for M365 include:

- M365 Privacy Statement: http://www.microsoft.com/online/legal/v2/?docid=22&langid=en-us
- Microsoft's Privacy Statement: http://www.microsoft.com/online/legal/v2/?docid=23
- Azure Trust Center: http://office.microsoft.com/en-us/business/office-365-cloud-privacy-FX103046091.aspx

All these documents reinforce the same statements of the Microsoft approach which is:

- it uses the user data to maintain and provide M365,
- it is Microsoft's policy not to use user data for other purposes,
- Office365 (as a business service) is designed and operated physically and logically separate from Microsoft's consumer services (i.e. Hotmail, etc.),
- Microsoft does not scan emails or documents for advertising purposes.

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.

s. 15(1)(l), s. 17

[redacted]

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

s. 15(1)(l), s. 17

[redacted]

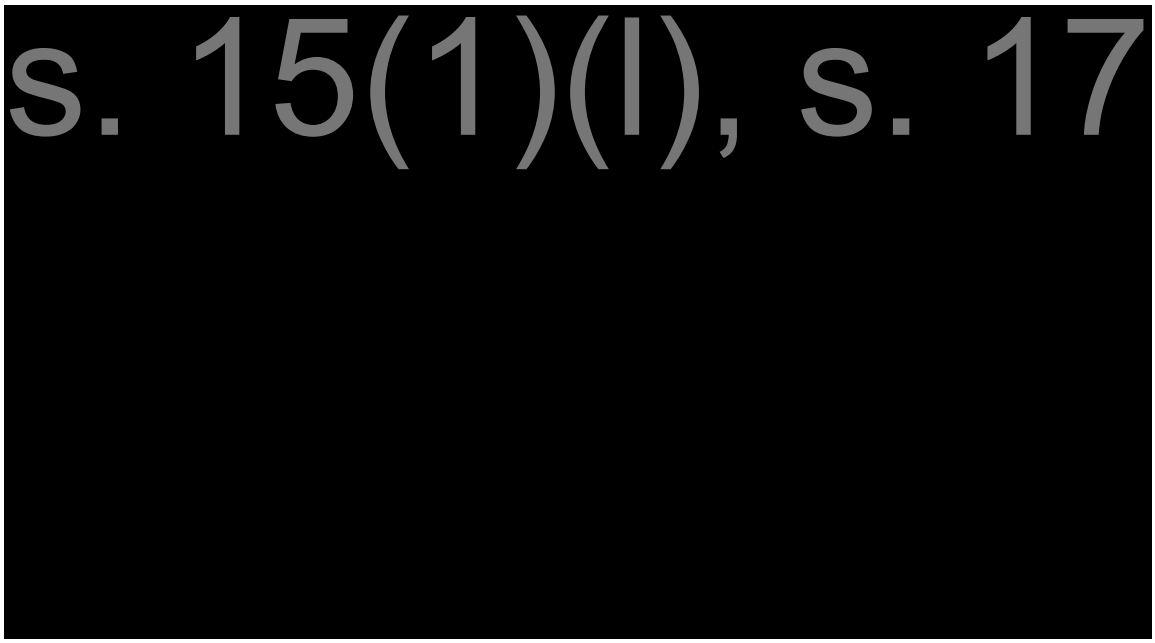

Figure 4: Office 365 Auditing

s. 15(1)(l), s. 17

SERVICE PROVIDER AUDITS

s. 15(1)(l), s. 17

s. 15(1)(l), s. 17

s. 15(1)(l), s. 17

LEGAL DISCLOSURE

s. 15(1)(l), s. 17

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?

In the proposed UFV implementation the university is establishing a connection between the on-premise AD and Microsoft's AAD in the UFV tenant. This connection is primarily designed to authenticate users. When the UFV user attempts to access the M365 application, Microsoft ADFS links the user account back to the user's UFV account (identity) and gets the user's Identity Provider (UFV AD) to authenticate the user before granting them access.

The user data in the two registries (AD and AAD) are synchronized with a mechanism called Azure AD Connect, which has two scheduler processes that are responsible for synchronizing passwords and general objects and attributes. By default, the scheduler runs every 30 minutes. UFV can decide which attributes are passed to the AAD, but generally, the on-premise AD will be the source for all data and all changes to user attributes will be performed against this system. s. 15(1)(l), s. 17 [redacted]

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 16, 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 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. This initiative does not systematically disclose personal information.

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).	

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

No.

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).	

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.

While its primary functions are authentication and authorization, the ADD registry that will be processed in the UFV tenant can be described as a personal information bank. Accordingly, these are the required FIPPA descriptors:

Personal Information Bank	
Personal Information Bank Name	UFV AAD
Personal Information Bank Location	Microsoft Canadian Datacentres: • Canada East (Quebec City) • Canada Central (Toronto)
The purpose of the Collection, Use, and Disclosure of Personal Information	To support day-to-day operations of faculty and staff email 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
Collected Personal Information is About	• Current faculty and staff. • Former faculty and staff may be included if they elect to retain UFV email addresses
Type(s) of Personal Information Collected will include	• Contact Information: (i.e. name, email, phone number). • User Content: (i.e. email content, attached documents, contacts)
In accordance with FIPPA and other applicable laws and policies, personal information may be used by and/or disclosed to	• UFV staff and faculty, for communication, day-to-day operations • Microsoft for service support purposes

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

Part 6 – Privacy Office(r)/or individual responsible comments

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

Maureen Murphy Legal Counsel University of the Fraser Valley	Signature	Date

Part 7 – Administrative Office(r)/or individual responsible comments

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

Jackie Hogan Chief Financial Officer & VP Administration, University of the Fraser Valley	Signature	Date

Part 8 – Program Area Signatures

Steven Banyai Chief Information Officer, University of the Fraser Valley	Signature	Date
Crawford Millen Author/ Director of Information Security OCIO University of the Fraser Valley	Signature	Date
Jacqueline Toering Dir. Risk & Safety, University of the Fraser Valley	Signature	Date
Alex Diaz Dir. Infrastructure & Operations OCIO, University of the Fraser Valley	Signature	Date

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