PIA01675 – Microsoft 365: MS OneDrive, MS Teams, and Related MS Azure Services

PIA REVIEW – EXECUTIVE REPORT

PREFACE

This document forms part of UBC Safety & Risk Services (SRS) internal documentation for support and administration of the Privacy Impact Assessment (PIA) Review Process. In particular, it documents the final report of the specified PIA review.

This section of the assessment serves to provide and record document control capabilities for this document.

Document Control – PIA Report

The following sub-sections provide a record of the base document template revision history and control. This sub-section is not intended to reflect or record changes or content related to the documenting of an individual PIA review.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Belsito, Mark	UBC IT Collaborative Technologies	Manager, Operations, Communication & Collaboration Technologies
Hancock, Paul	Office of the University Counsel	Legal Counsel, Information and Privacy
Lonsdale-Eccles, Michael	PrISM, Safety & Risk Services	Director, PrISM SRS
Loder, Jay	PrISM, Safety & Risk Services	Manager, PrISM SRS
Tremonti, Robert	PrISM, Safety & Risk Services	Sr. Privacy and Information Security Risk Advisor

REPORT REVISION HISTORY

REVISION #	START DATE	REVISED BY	DESCRIPTION
0.10	2020-07-28	Tremonti, Robert	▪ New report, combining initial intended MS OneDrive and MS Teams PIA reports
0.20	2020-08-14	Tremonti, Robert	▪ Information collection and review of services with project team on applications and configurations
0.30	2020-08-16	Tremonti, Robert	▪ Discussions and review with Legal, SRS PrISM, and project regarding risks and mitigations
0.40	2020-09-18	Tremonti, Robert	▪ Final reviews with Legal, SRS PrISM, and project

REPORT REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00			Initial release of document

TABLE OF CONTENTS

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Background

The purpose of a PIA is to determine whether a Project or Initiative complies with the Freedom of Information and Protection of Privacy Act (FIPPA), UBC's Policy #SC14 (Acceptable Use and Security of UBC Electronic Information and Systems) and UBC's Information Security Standards. This document is to advise that the PIA review of the Project has been completed. The following outlines the scope, risks, and conclusions associated with this PIA.

Due to the COVID 19 crisis, UBC's PIA team has conducted a PIA under the oversight of the University Counsel to determine if Microsoft 365 and related Microsoft Azure services[1] can be used at UBC to support remote learning and administrative uses. The scope of this PIA is described in the scope section, and will be adjusted as Microsoft Services are adopted.

The initial PIA will specifically address the use of two Microsoft 365 (M365) products and services that UBC IT is making available for use by UBC faculty, staff, and students:

- **MS OneDrive** introduces an enterprise implementation of Microsoft OneDrive, which will replace the current file sharing and file storage capabilities of Workspace
- **MS Teams** implements a new collaborative tool for use by faculty, staff, and students

The PIA is based on information and materials provided directly and/or indirectly by the project / initiative, including presentations, discussions, e-mails and attachments, or references to information sources.

1.2 Unit and Program Area

CAMPUS	UBC-V and UBC-O
FACULTY OR DEPARTMENT	Office of the Chief Information Officer
PROGRAM AREA	Strategic Initiatives
ADDITIONAL INFORMATION	This PIA consolidates several reviews related to the enterprise-level implementation of Microsoft 365 and related Microsoft Azure services.

Figure 1 - UBC Unit and Program Area

[1] *Related Microsoft Azure Services* include Azure Active Directory and a number of Security & Compliance Tools such as Conditional Access for Multi-Factor Authentication and Terms of Service presentation/tracking.

1.3 Contact Information

NAME	Liza Jose
TITLE / POSITION	Associate Director, End User Technologies
FACULTY OR DEPARTMENT	Office of the Chief Information Officer
UBC TELEPHONE NUMBER	604-822-8819
UBC E-MAIL ADDRESS	liza.jose@ubc.ca

Figure 2 - PIA Submission Contact Information

1.4 Description of the Program, System, Application, or Initiative Assessed

This initiative aims to implement Microsoft collaborative technology for use by UBC employees (faculty and staff) and UBC students to foster and support collaboration within the workplace and in the learning environments. This project also intends to align with a growing demand for the implementation of Microsoft 365 (M365) across the institution.

Microsoft recently introduced Microsoft 365 (M365), a bundle of existing products under one license, geared towards businesses and educational institutions. The name is similar to the already existing Office 365 (O365). Office 365 is a cloud-based suite of productivity apps like Outlook, Word, PowerPoint, and more. Microsoft 365 is a bundle of services including Office 365, plus several other services including Windows 10 Enterprise. For an overview of the M365 ecosystem, please refer to the diagram provided in the Appendix.

1.5 Scope of PIA

The scope of this PIA is the implementation of M365 products and services, and related Microsoft Azure Services implemented for direct use by UBC faculty, staff, students, and other individuals who are authorized to use these products and services on behalf of UBC.

SCOPE INCLUSIONS

The scope of review of Microsoft 365 is limited to those aspects which are required for the implementation of the services and products UBC has elected to deploy, and includes related Microsoft Azure Directory Services and Security and Compliance tools as appropriate.

SCOPE EXCLUSIONS

The scope of this PIA excludes review and considerations of:

- the content or use of the content of files created, stored, or shared by users via M365 and MS Azure service offerings
- enterprise implementation and/or use of previously installed Microsoft Office products and services such as Exchange or Outlook
- individual implementation and/or use of any other Microsoft services by students, faculty, or staff
- review of other Microsoft services not related to the implementation of MS Teams and MS OneDrive at UBC
- physical security and other controls associated with devices used to access services
- Microsoft products not specifically included in the Appendix

- Integration of Microsoft 365 and related Microsoft Azure services with other third-party applications or services

Implementation of MS Teams provides access to web-based versions of Microsoft Office's basic productivity tools including Word, Excel, and PowerPoint. While the web-based versions of these products are not as full featured as UBC's current implementation of the products, they are essentially similar and are excluded from the scope of this review.

Notwithstanding the review of the MS OneDrive implementation, data residency of files created using the abovementioned web-based products is also excluded from the scope of this review. Normal use of the web-based applications by faculty and staff, especially in conjunction with the planned MS OneDrive implementation, will maintain data residency of files. However, as with the existing UBC non-web-based implementation of these products, individual users can intentionally specify that a given file be stored on non-UBC storage location outside of Canada.

1.6 Related UBC PIAs

There are no directly related PIAs completed within UBC

1.7 Elements of Information or Data

MS Data Categories

Microsoft defines data as falling in one of several categories. Definitions of the data categories appear in several documents and some definitions may be superseded on a per-service basis.

For the purposes of this PIA, the personal information (PI) collected through the use of Microsoft 365, Microsoft OneDrive, and Microsoft Teams is categorized as follows:

CATEGORY OF PI	DESCRIPTION
CUSTOMER DATA	All data, including all text, sound, software, image or video files that are provided to Microsoft or its Affiliates by, or on behalf of, UBC through use of Online Services. Any of this information could contain personal information.
AZURE ACTIVE DIRECTORY DATA ("AAD DATA")	The data elements used to synchronize users' Enterprise Active Directory accounts to Microsoft's Azure Active Directory (AAD) are documented by the project in the UBC *Microsoft 365 Teams Provisioning Approach* and *UBC Campus Wide Login (CWL) Synched Identity Attribute to Azure* documents. For faculty and staff users, this information is not personal information because it falls under the definition of "business contact information". For student users, this information is personal information if it identifies the student using their name or another unique identifier such as student number. The PI data elements shared for students are the CWL, UBC student e-mail address, and UBC affiliation. **NOTE:** Users may, at their own discretion, also provide personal profile information (including images) session preferences, and session customization data which may also be stored in the Azure AAD.
META DATA	For the purpose of this Privacy Impact Assessment, non-content meta data, such as Internet Protocol (IP) addresses, are not considered personal information.

Figure 3 - Categories of PI Collected Using Microsoft 365, Microsoft OneDrive, and Microsoft Teams

1.8 Storage or Access Outside of Canada (including back-ups and recovery)

CATEGORY OF PI	STORAGE LOCATION
CUSTOMER DATA	The following Customer Data is stored in Canada per Microsoft's Online Services Terms: **Location of Customer Data at Rest for Core Online Services** For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each a Geo) as follows: • Microsoft 365 Services. If Customer provisions its tenant in Australia, Canada, the European Union, France, Germany, India, Japan, Norway, South Africa, South Korea, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft will store the following Customer Data at rest only within that Geo: 1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments) 2) SharePoint Online site content and the files stored within that site, and 3) Files uploaded to OneDrive. **NOTE:** Currently the Microsoft Online Service Terms (OST) documentation does not indicate that MS Teams is, or can be, tenanted within Canada. However, the Microsoft websites[2] indicate that MS Teams is tenanted within Canada. E-mails exchanged with Microsoft's Canada National Office 365 Lead - Education[3] confirms that this is to be interpreted that MS Teams is tenanted within Canada and that the OST documentation has not yet undergone a regular review and update cycle in which this information would be included.
AZURE ACTIVE DIRECTORY DATA (AAD DATA)	AAD Data is generally stored outside of Canada. There is no available option to allow this data to be stored in Canada. AAD Data comprises data that UBC transmits to Microsoft to enable UBC services to function, and profile data submitted that may be by the customer.

Figure 4 - Categories of PI Collected for AAD

1.9 Data-Linking Initiative

This initiative is not considered a data linking initiative as contemplated in s.36.1 of FIPPA.

1.10 Is this a Common or Integrated Program or Activity?

This initiative is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

1.11 Risk Classification Level

The inherent risk classification level of this PIA submission is VERY HIGH due to the volume and nature of the personal information handled by this technology.

[2] https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations?ms.officeurl=datamaps#canada
[3] E-mails exchanged on June 22 and June 23, 2020 with UBC's Senior Project Manager, Strategic Initiatives.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

The following sub-sections present that personal information data flows for different components of the M365 and related Microsoft Azure Services offerings.

AZURE ACTIVE DIRECTORY

The following presents the data flow of student personal information for the Azure Active Directory (AAD). This flow is common to all uses of the M365 and Microsoft Azure Services offerings.

Data Flow for AAD Data				
	Description/Purpose	**Personal Information**	**Type**	**FIPPA Authority**
1.	Before students are given access to services, they are requested to provide consent for disclosure of their AAD data outside Canada, and to other members of the UBC community. If they do not wish to provide consent, they are prompted to change their AAD data to something non-identifying, and then provide consent.	AAD Data for faculty or staff is not personal information.[4] AAD Data for students is personal information if the data contains a personal identifier such as name or other identifying number. Some information such as profile images may be propagated in documents (such as authorship info, etc.)	Collection	26(c)
2.	UBC uploads AAD data to MS Azure Active Directory outside Canada.		Use / Disclosure	32/ 33.1(1) (e.1)/ 33.1(1)(b)
3.	The student's AAD data is made available to all UBC M365 users.		Disclosure	33.1(1)(b)
4.	Users update their personal profile and session preferences which may be stored in AAD.			

Figure 5 - AAD Data Flow

[4] FIPPA defines personal information as recorded information about an identifiable individual other than business contact information (i.e., the name, position name or title, business telephone number, business address, business email or business fax number of the individual).

MS ONEDRIVE

The following presents the data flow of personal information for the MS OneDrive implementation.

Data Flow for Customer Data				
	Description/Purpose	**Personal Information**	**Type**	**FIPPA Authority**
1.	User uploads Customer Data to OneDrive service in Canada.	Customer Data could contain personal information of various sorts.	Use / Disclosure	32/ 33.1(1) (e.1)
2.	User shares Customer Data with others.		Disclosure	33.1(1)(e) 33.1(1) (e.1)/ 33.1(1)(b)

Figure 6 - Data Flow for MS OneDrive Customer Data

MS TEAMS

The following presents the data flow of personal information for the MS Teams implementation.

Data Flow for Customer Data				
	Description/Purpose	**Personal Information**	**Type**	**FIPPA Authority**
1.	User uploads Customer Data to MS Teams service in Canada	Customer Data could contain personal information of various sorts.	Use / Disclosure	32/ 33.1(1) (e.1)
2.	User shares Customer Data with others		Disclosure	33.1(1)(e) 33.1(1) (e.1)/ 33.1(1)(b)

Figure 7 - Data Flow for MS Teams Customer Data

2.2 Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the respective intended mitigation steps.

Figure 8 - Risk Mitigations

RISK STATEMENT	RISK MITIGATION
PI stored / accessible outside of Canada: Storing information or permitting access to personal information outside of Canada creates the risk of non-compliance with FIPPA and/or UBC policies and standards.	▪ Secure the consent of students for inclusion of their PI within AAD ▪ Contractual commitment of MS Teams tenanting in Canada ▪ Limit ability to sync OneDrive to external services
Retaining PI longer than necessary: Not having adequate processes to ensure personal information is protected with strong access controls and retention policies increases the risk of non-compliance with FIPPA and/or UBC policies and standards.	▪ Microsoft retains for 90 days past contract termination ▪ Users must apply retention policies & procedures to own data ▪ Retention processes required for learning environment teams ▪ Retention processes required for learning environment use of MS Teams if teams or groups are “recycled” between course sessions ▪ Processes required for removal of individuals from teams if memberships are based on course enrolment or UBC employment
Unauthorized collection of PI: Not ensuring that Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to	▪ Ensure minimal collection of data for AAD account creation ▪ Batch loading of account data to AAD must be reviewed and addressed ▪ Users must accept Terms of Service upon login

RISK STATEMENT	RISK MITIGATION
collect, use, and disclose personal information, unless FIPPA permits, creates the risk of non-compliance with FIPPA and/or UBC policies and standards. Indirectly collecting personal information, unless permitted by FIPPA, creates a risk of non-compliance with FIPPA and/or UBC policies and standards.	
Excessive collection of PI: Over collection of personal information creates the risk of non-compliance with FIPPA and/or UBC policies and standards, and increases the risk of reputational harm.	▪ Users should be trained on good data collection practices
Use of PI for alternate purpose: Using information for purposes other than for which that information was collected, or for a use not consistent with that purpose creates the risk of non-compliance with FIPPA and/or UBC policies and standards and increases the risk of reputational harm.	▪ Microsoft makes public & contractual commitments as to use of Customer Data
Unauthorized access to PI during design and development: Using information for purposes other than for which that information was collected, or for a use not consistent with that purpose creates the risk of non-compliance with FIPPA and/or UBC policies and standards and increases the risk of reputational harm.	▪ Microsoft makes public & contractual commitments as to use of Customer Data
Disclosing to or allowing unauthorized users access: Disclosing to or allowing unauthorized users access to personal information creates the risk of non-compliance with FIPPA and/or UBC policies and standards, and increases the risk of reputational harm.	▪ Microsoft makes public & contractual commitments regarding sharing and disclosure of PI, including release to law enforcement and foreign agencies, etc. ▪ Retention process required for learning environment use of MS Teams if teams or groups are “recycled” between course sessions ▪ Processes required for removal of individuals from teams if memberships are based on course enrolment or UBC employment ▪ Review of configuration settings at implementation to ensure PI is not exposed by configuration choices
Not ensuring individuals are informed about collection: Not ensuring that Individuals are (a) informed about what information is collected about them, (b) the choices available to them, and (c) that implicit or explicit consent is required, unless FIPPA permits, creates the risk of non-compliance with FIPPA and UBC policies and standards.	▪ Develop and deploy Terms of Use and consent processes
Not ensuring informed PI sharing with third parties: Not ensuring that individuals are informed that their personal information may be disclosed to third parties for purposes other than those identified or for which the individual has provided implicit or explicit consent unless FIPPA permits, creates the risk of non-compliance with FIPPA and/or UBC policies and standards.	▪ Develop and deploy Terms of Use and consent processes
Inadequate controls to safeguard mobile devices or removable media: Inadequate controls to safeguard mobile devices or removable media increases the risk of unauthorized access.	Persistent log-in of mobile apps could potentially allow access when no longer authorized or to individuals sharing use of a non-UBC mobile device ▪ Require locking of mobile devices which use mobile apps ▪ Require regular refresh of mobile device log-in
Weak or absence of technical security controls: Designing systems where personal information is not adequately or appropriately protected, stored, and	▪ Project and stakeholders to address Complimentary User Entity Controls

RISK STATEMENT	RISK MITIGATION
used creates the risk of non-compliance with FIPPA and/or UBC policies and standards.	
Not performing PIA on new system or project: Not performing a PIA on the full application creates risks of inappropriate collection, use, retention, and/or disclosure of personal information which may result in non-compliance with FIPPA and/or UBC policies and standards. There may also be security risks for unsupported applications.	▪ Change management processes must be applied to any changes related to: ○ M365 eco-system ○ existing related applications & services ○ initially agreed configuration settings

Refer to ***Part 7 - Product Specific Considerations*** for additional information for specific risks relating to the implementation of Microsoft OneDrive and Microsoft Teams.

2.3 Collection Notice

AAD DATA

This falls under the scope of the collection notice that is provided to students & employees when they apply to the university. In addition, student all users should be notified that information they choose to provide, such as personal profile information or session preferences, are retained in AAD and as such are stored outside of Canada and available to other users. Some personal profile information, such as images or nicknames, may also be visible in documents provided to or created using the services, and may also be visible to external parties with whom those documents are shared. For example, images may be visible in meeting notifications and invitations, or in documents in which change tracking or authoring information is retained.

CUSTOMER DATA

The use of MS OneDrive and MS Teams to store personal information presupposes that the information has been collected in a lawful manner, using collection notices where appropriate.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

With tenanting of services within Canada, storage and access to Customer Data is generally not a concern unless configuration settings create potential scenarios for unintentional disclosure outside of Canada. An example of such a potential situation arises if syncing of UBC enterprise OneDrive and a user's personal OneDrive is permitted.

CUSTOMER DATA

As this information is stored and accessed in Canada, no consent is required.

AAD DATA

As this information is stored and accessed outside Canada, a procedure must be established for providing notification and obtaining informed consent from students to store their personal information in the MS Azure Active Directory outside of Canada.

1. Inform students that their identifier will be included in the AAD, including profile data they chose to submit, will be stored outside of Canada.
2. Inform students that their identifier will be included in a directory that will be available to other students, faculty, and staff.

3. Inform students that if they have any concerns about being identifiable, they can change their identifier to something that does not identify them, such as a first name, nickname, or other alias and that they will not be allowed to change this without strong rationale.
4. Inform students about what the mechanism is for changing their identifier and give them a deadline to do so.

It is not necessary to seek consent from faculty and staff users to upload their name and work contact information into the directory because this is not personal information. However, they should be informed that any additional profile information that they elect to upload to the directory, such as photographs, will be stored outside of Canada and may be visible to other users.

Under the current Ministerial Order[5], it is acceptable to store the information in AAD before the above consent procedure has been completed, if that is necessary for development or testing purposes.

2.5 Consent Withheld Procedure

Users (students) who elect to exercise their right to withhold consent for storage of their Azure AD data outside of Canada are provided an opportunity to "anonymize" their information via creation of a non-identifying CWL via the CWL myAccount service. (Please refer to Appendix for further details.)

Users who continue to elect to withhold consent, but do not take advantage of the capabilities to create a non-identifying CWL account will not be able to access the M365 service offerings.

[5] https://www.bclaws.ca/civix/document/id/mo/mo/2020_m085

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

Microsoft's M365 and related MS Azure service offerings are hosted at data-centers owned and managed by Microsoft. Physical protection of these data-centers is managed by Microsoft and is reported in their SOC 2 type II audits and in other security reports and reviews. UBC relies on documentation made publicly available by Microsoft and documentation which is made available by Microsoft under licensing agreements and non-disclosure agreements.

Physical security measures of the UBC faculty and staff environments and computers are not within scope of this review; physical security of these environments and hardware is governed by UBC Policy SC14 and its associated Information Security Standards.

3.2 Technical Security Measures

Microsoft's SOC 2 Type II report specifies a set of security controls which fall outside its jurisdiction in regards to maintaining the security and integrity of Customer Data. The Complementary User Entity Controls (CUEC) are controls which the client (user entity) must address, and it falls to UBC to ensure that these controls and security measures are addressed appropriately and effectively.

The project must ensure that appropriate UBC stakeholders are engaged to address the CUECs, including determination if any of the CUECs are not applicable to the UBC environments.

3.3 Security Policies, Procedures, and Standards

Microsoft's published information security policies and standards, and governance and compliance processes apply to Microsoft's delivery and provisioning of M365 and related MS Azure services for UBC's use.

UBC's information security policies and standards apply to all files, and the content of said files, which UBC users upload to and share on Microsoft Cloud Services. UBC faculty and staff are individually responsible for ensuring they adhere to UBC policies and standards in regards to information under their control.

3.4 Tracking Access / Access Controls

The following sub-sections describe any access controls and/or ways in which the initiative will limit or restrict unauthorized changes (such as additions or deletions) to personal information, and how it tracks who has been granted access to the personal information.

UBC Customer Data

Access to personal information contained within files and information categorized as Customer Data is managed through UBC access controls, including CWL integration.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Responsibility and accountability for processes which allow individuals to update and correct their personal information stored within UBC files which are used via or reside on M365 or MS Azure services offerings are the responsibility of UBC and the individual projects and initiatives which collect and process such information.

4.2 Decisions That Directly Affect an Individual

The use of either M365, MS OneDrive, or MS Teams service offerings does not, in and of itself, contribute to decisions which directly affect an individual as contemplated in section 31(b) of the FIPPA.

4.3 Records Retention and Disposition Schedule

Records retention and disposal procedures and practices process are required for both "Customer Data" and "AAD Data". The sub-sections address the status of retention and disposal for each of these categories.

CUSTOMER DATA

The following are the current status for retention and disposal of "Customer Data".

UBC

UBC departments and faculties, individual faculty and staff members, projects, and initiatives which elect to process and store information using M365 services capabilities are responsible and accountable for the implementation of appropriate records retention and disposal policies and procedures for individual files and records in order to meet their own and UBC's needs.

UBC departments and faculties, individual faculty and staff members, projects, and initiatives are responsible for implementing and managing UBC Records Retention Schedules which apply to any and all information they store using M365.

General retention schedules of at least 1 year should be established and communicated for student controlled or managed environments, such as student created team sites.

Microsoft

In regards to retention and disposal of UBC data upon termination of services, the Microsoft Online Services DPA of April 2020 states:

> **Data Retention and Deletion**
> At all times during the term of Customer's subscription, Customer will have the ability to access, extract, and delete Customer Data stored in each Online Service.
>
> Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the

90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law, or authorized under this DPA, to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data or Personal Data as described in this section.

AZURE ACTIVE DIRECTORY (AAD) DATA

There are currently no processes in place for retention or disposal of account data (and related PI) retained in Azure Active Directory. The project has indicated that such plans may be a further consideration but has not provided any associated timelines.

UBC

The project has indicated that UBC does not currently delete EAD or Azure accounts. If an account is active in EAD and has been synced to Azure, and then later becomes disabled in EAD, the account's ability to log-in to Azure will be disabled, however, the account's record will remain in place both in EAD and Azure and not be deleted.

Microsoft

Based on descriptions provided by the project, Microsoft does not initiate or perform deletion of the associated Azure Active Directory (AAD) records for accounts which UBC has disabled.

UBC administrators must explicitly configure the EAD / Azure synchronization process to delete the AAD record, at which point it is placed in the AAD "recycle bin" for 30 days, after which the record is permanently deleted.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

There is ongoing (systematic) disclosure of account information to Microsoft Azure Active Directory and of directory information to other UBC students, faculty, and staff. However, an Information Sharing Agreement (ISA) is not required as disclosure is addressed in the consent processes, and in the associated terms & conditions of use / service (TOU / TOS) for the in-scope M365 and related MS Azure services.

5.2 Access for Research or Statistical Purposes

Not applicable.

5.3 Other Applicable Legislation

There is no additional applicable legislation for this review.

5.4 Other

This initiative is not considered to be part of, or to create, a Personal Information Bank as contemplated in s.69 of FIPPA.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Conclusions

This Privacy Impact Assessment has determined that, *provided the conditions listed below are implemented,* the services in scope can be delivered in compliance with FIPPA and UBC policies. Should the scope of the program change, further assessments may be required as new related or expanded services are considered, and through post implementation to ensure the programs delivered match those proposed.

OneDrive and Teams are services that will be used to store and share a large amount of information, some of which is extremely sensitive. Therefore, the project team must request a further PIA review if it ever has any reason to believe that the terms of use or the security of any of these systems has changed in a material way.

6.2 Conditions of Approval

The following are the conditions which apply for the completion of this PIA review. The project team should update the PrISM SRS team as to the progress and completion of each of these conditions, including any substantial delays or inability to completion or reasonably fulfill any of the listed conditions.

6.2.1 Condition #1: Ensure Canadian Tenanting

One of the significant prerequisites for approval of this PIA is Canadian hosting of Customer Data. Selection of tenanting of Online Services within a specific geographic region ("geo") is accomplished via configuration controls. It is not clear whether the project team has any process in place to ensure that the correct tenanting is selected, and that tenanting is periodically reviewed to ensure there have been no unauthorized changes in the tenanting situation.

Processes to address the above issues should be devised and implemented to ensure ongoing data residency compliance of current and planned MS Cloud Services contracted by UBC.

As outlined in section 1.8 above, at the time of this review, UBC also does not have contractual confirmation that MS Teams is tenanted in Canada. The project team must take steps to ensure that UBC's implementation of Microsoft Teams is tenanted in Canada.

The project responded on 2020-09-28 that this condition has been addressed, and provided a supporting narrative.

6.2.2 Condition #2: Implement Procedure for De-identification of Identifiers in Azure Active Directory

Students must be given the opportunity to de-identify the identifiers used in AAD before that information is stored outside Canada or made available to others. This de-identification procedure is essential as it represents the student's consent to make the information available.

All students must be informed that data they voluntarily submit to Microsoft for profile personalization (e.g. photos or images, personal interests, session customization preferences, etc.) may be disclosed outside Canada and disclosed to other students. Students should also be informed that certain profile information they provide may be propagated in Microsoft Word or other documents they edit and therefore visible to other users, including external users, with whom they chose to share these documents.

All faculty and staff must be informed that data they voluntarily submit to Microsoft for profile personalization (e.g. photos or images, personal interests, session customization preferences, etc.) may be disclosed outside Canada and disclosed to other users. Faculty and staff should also be informed that certain profile information they provide may be propagated in WORD or other documents they edit and therefore visible to other users, including external users, with whom they chose to share these documents.

The project has indicated that faculty and staff will be shown the ToS at log-in.

Under the current Ministerial Order[6], it is acceptable to store the information in AAD before the above consent procedure has been completed, if that is necessary for development or testing purposes.

The project responded on 2020-09-28 that this condition has been addressed, and provided a supporting narrative.

6.2.3 *Condition #3: Implementation of Retention and Disposition Process for Azure Active Directory Data*

The project has indicated that Azure Active Directory data is not deleted once an account is disabled or no longer valid. Present practices are to retain data indefinitely, however there does not appear to be any formal documentation of this requirement or decision.

The project manager and appropriate UBC stakeholders must establish and implement processes to address excessive retention of Azure Active Directory data and deletion / disposal of the records in a timely manner. The processes should also document the business cases for the selected and approved retention periods.

The project responded on 2020-09-28 that this condition has been completed, and provided a supporting narrative.

6.2.4 *Condition #4: Implementation of Retention and Disposition Process for MS Teams Customer Data*

The intended structure and use of MS Teams in learning settings has not yet been fully established or documented. It is unclear if a team established for a course session will be re-used for subsequent course sessions and how content contributed for a session will be archived or cleared so that subsequent sessions do not have access to any personal information of previous course attendees, and previous course attendees do not have access to content which contains personal information of future course attendees.

The initiative and appropriate UBC stakeholders must establish and implement processes to address excessive retention of Customer Data and deletion or archival of Customer Data between re-uses of a team site in a timely manner. The processes should also document the business cases for selected and approved retention periods.

The project responded on 2020-09-28 that efforts to address this condition have been deferred, and provided a supporting narrative.

6.2.5 *Condition #5: Implementation of Complementary User Entity Controls*

The initiative and appropriate UBC stakeholders must implement and maintain the Complementary User Entity Controls (CUEC) described in the Microsoft SOC 2 Type II reports. The project must review the list of CUECs and provide the PIA team with the following information for each CUEC:

[6] https://www.bclaws.ca/civix/document/id/mo/mo/2020_m085

1. applicability of each CUEC in context of systems which are in-scope of the PIA review
2. stakeholder responsible and accountable for each control
3. existing UBC control or activity that addresses the CUEC
4. planned UBC control or activity that will address the CUEC and timelines for implementation

The above information regarding the CUEC must be reviewed, and updated accordingly, whenever a new system is brought in-scope for this PIA or there are major changes which impact this PIA review.

The project responded on 2020-09-28 that this condition has been addressed, and provided a supporting narrative.

6.2.6 Condition #6: Review and Assessment of Proposed / Agreed Configuration Settings

The initiative and appropriate UBC stakeholders must provide documentation of the proposed and/or agreed configuration settings for each of the in-scope services. The documentation must indicate how the proposed / agreed settings or configurations address or impact the privacy and security risks identified in the PIA review, including any potential conflicts with configurations or settings of other implemented M365 products and services. The initiative is responsible for ensuring, and documenting, that these initial configurations and settings are properly implemented.

The initiative and support teams must ensure that any post-implementation changes to configurations and/or settings of in-scope products and services are documented and subject to UBC IT change management processes. The PIA team must be notified of any changes to existing privacy or security settings, and any changes which may result in a potential or actual privacy or security exposure or increased risk of such exposure.

The project responded on 2020-09-28 that this condition has been addressed, and provided a supporting narrative.

6.2.7 Condition #7: Review and Assessment of Implementation of Products, Services, or Integrations

The initiative and support teams must ensure that implementation or integration of any additional products or services (currently out of scope of this PIA), results in the initiation of a supplementary PIA.

The project responded on 2020-09-28 that this condition has been addressed, and provided a supporting narrative.

6.3 Information or Materials Reviewed

This assessment contains or references documentation and information which are proprietary to a third party. These materials are not publicly available, and were disclosed to UBC for the purposes of this review either under a Non-Disclosure Agreement or restricted access via license.

The following materials were reviewed in the course of this PIA:

MICROSOFT DOCUMENTS

The following documents available from Microsoft were reviewed to determine underlying privacy and security issues and mitigations which Microsoft had addressed and which would aid in the UBC PIA. Documents available from Microsoft's Trust Center were reviewed to determine commitments and compliance in regards to information security and GRC related capabilities. The majority of the documents can only be accessed through an authorized account, and are subject to NDAs.

General Documents

- MS Canadian Foundational PIA Executive Summary
- MS Azure Foundational PIA (December 2016)
- MS O365 Foundational PIA (January 2020)
- MS Volume Licensing Online Services Terms (Worldwide English, April 2020)
- MS Online Services Data Protection Addendum (Worldwide English, January 2020)
- MS Professional Services Data Protection Addendum (February 2020)
- MS Professional Services - Handling Customer Content Q&A Brief (April 2020)
- How Microsoft Categorizes Data

Governance Documents

- Office 365 Core - SSAE 18 SOC 2 Report 9-30-2019
- O365 SOC Bridge Letter Q3 2020
- Microsoft Office ISO 27001:2013 Statement of Applicability
- Azure, Dynamics 365, and Online Services: ISO27001 Certificate
- Office 365—Global and Germany ISO 27001: Information Security Management Standards Certificate
- Microsoft Azure, Dynamics 365, and Other Online Services - ISO27018 Certificate - 6.15.2020
- Microsoft Azure, Dynamics 365, and Other Online Services - ISO27001, 27018, 27017, 27701 Assessment Report - 6.15.2020
- Microsoft Azure, Dynamics 365, and Other Online Services - ISO27018 Certificate - 6.15.2020
- Microsoft Azure, Dynamics 365, and Other Online Services - ISO27001 and 27017 Certificate - 6.15.2020

IMPLEMENTATION PARTNER DOCUMENTS

- UBC Compugen MS Volume Licensing Agreement – Enrollment for Education Services
- UBC Compugen MS Volume Licensing Agreement – Program Signature Form
- UBC Compugen MS Cloud Services Provider Customer Master Agreement – 2019-12-12

UBC DOCUMENTS

- UBC OneDrive Sharing Essentials
- UBC Synched Identity Attributes to Azure – 2020-06
- AMTRA O365 – OneDrive SP Teams - Configuration
- UBC Mapping Global Configuration Settings
- Microsoft 365 Teams Provisioning Approach v1.0

OTHER / EXTERNAL DOCUMENTS

The following documents were reviewed to determine applicability of the PIA review of Microsoft Cloud Services: conducted by the Province of BC:

- MTICS16024 - Microsoft Cloud Services Phase II PIA – complete

6.4 Information or Materials Not Available for Review

The following materials were not reviewed in the course of this PIA:

Microsoft Documents

The following documentation was not available from Microsoft:

- Contractual documentation assuring Microsoft Teams Canadian tenancy

PART 7: PRODUCT SPECIFIC CONSIDERATIONS

This section addresses risks, issues, and considerations specific to implementation of a given product or service and which are not applicable to the other products or services reviewed.

7.1 MS OneDrive

There are significant privacy and security risks which arise in configuring and permitting the ability of users to synchronize ("sync") the folders and files between the UBC production OneDrive environment and their personal OneDrive accounts. The issue arises as UBC IT is introducing when a user is using a computer (PC, laptop) that is not managed by UBC IT.

Improper configuration of the OneDrive synchronization settings could potentially result in a user unknowingly moving or copying UBC owned files to an insecure external service, or to services outside of Canada. This would result in UBC losing control over the data that would otherwise be in its custody and control, as well as potentially exposing confidential UBC data to unauthorized users, and storing personal information outside of Canada without consent.

Improper configuration of the OneDrive synchronization settings would also place users in jeopardy of violating UBC policies and standards without having the explicit intention of doing so.

The project has indicated that certain setting combinations may lead users to storing UBC files on the local drive of their computer. As UBC policies discourage / do not permit such practices, and UBC data is to remain on UBC managed storage, this issue should also be considered in the selection of configuration settings.

The configuration settings should include limitations on mobile versions of the applications to reduce exposures such as persistent log-in, etc.

7.2 MS Teams

The following sub-sections provided additional information and considerations which are specific to the review of MS Teams only. The more significant risks associated of MS Teams are driven by the intended structure and use of MS Teams that will be implemented within the various learning settings.

The configuration settings should include limitations on mobile versions of the applications to reduce exposures such as persistent log-in, etc.

Student Environments

Teams created and managed by students for their own personal use will generally not be subject to the restrictions or limitations of either Learning or Administrative environments. UBC codes of conduct and UBC's policies of appropriate use and behaviors would apply. The group / team owner would be responsible for ensuring appropriate controls are established in regards to membership, etc.

Learning Environments

If membership of course related teams or groups is populated based on course registration, there is the risk that students no longer registered in a course may be able to view or modify content, including personal information of current and future team members, unless accesses are terminated in

a timely manner. Processes are required for such circumstances to ensure only currently enrolled students can access course related teams, particularly if the team or group is "recycled" between course sessions or semesters.

Processes are required to ensure information placed in Teams which are re-assigned or in Teams that are "re-used" for new semesters are purged of files, calendars, chats, etc., as these may contain personal information of students who participated in a previous semester.

Administrative Environments

Similarly, for departmental teams, processes are required to ensure individuals no longer employed in a department do not continue to be able to view or modify departmental content, including content which may contains personal information of any nature.

There is a risk that certain combinations of configuration settings may allow users to view team content which contains personal information they are not authorized to view (e.g., assignment submissions of other students in a course team or unrelated team), or allow students to continue to participate and view content of teams for a course they are no longer enrolled in. There is a need for the project to document and review proposed configuration settings and document final implementation settings to mitigate this exposure.

APPENDIX

A.1 M365 Ecosystem

Figure 9 - M365 Ecosystem[7]

[7] *The Periodic Table of Office 365* courtesy of www.jumpto365.com