UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

Privacy Impact Assessment
Microsoft 365

PIA #20-007 (Office of the University Secretariat to assign)

Why do I need to do a PIA (Privacy Impact Assessment)?

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 Information Governance Officer to determine internal policies for review and sign-off of the PIA. If you have any questions about this PIA template or FIPPA generally, please contact Adam Cullum (Information Governance Officer) at adam.cullum@unbc.ca or (250) 960-5139 or visit http://www.unbc.ca/foippa.*

Part 1 – General

Name of Department:	*Information Technology Services*		
PIA Drafter:	*Kevin Schretlen*		
Email:	*kevin.schretlen@unbc.ca*	*Phone:*	***250-960-5653***
Program Manager:	***Trevor Fuson***		
Email:	*trevor.fuson@unbc.ca*	*Phone:*	***250-960-5687***

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

The current set of communication and collaboration tools that UNBC is using are becoming outdated and unsustainable. Upgrades to existing on premise solutions will require considerable time and human resources detracting from the ability for UNBC Information Technology Services ("ITS") to meet the demands of UNBC students, faculty, and staff. ITS is proposing the adoption of the Microsoft 365 platform to facilitate collaborative communication technologies and support high quality and agile academic delivery.

This privacy impact assessment will cover the following products: Office ProPlus, Teams, Sway, Exchange Online, Sharepoint Online with OneDrive, and Azure Active Directory Fabric Services.

Overview of Microsoft 365

Microsoft 365 consists of:
1. Office ProPlus (desktop and cloud-based traditional Microsoft suite of software);
2. Unified Communications (Exchange email and Teams, which includes audio and video conferencing, Sway services, Voice over IP, etc.);

3. Microsoft 365 SaaS fabric services (security and compliance management tools that overlay all application services); and,
4. SharePoint (Web-enabled collaboration services), including OneDrive (similar to DropBox and Sync.com).

Supporting Microsoft 365 is a web-based administrative interface that allows users to configure settings delegated to them by client administrators. In this way, both administrators and individual users can utilize privacy and security protections and preferences available to them. For example, administrators can restrict the domains that are permitted to interact with a service, and the users can further limit this as necessary. Program areas with particularly sensitive data may add additional safeguards. See the information documented under the questions in Part 3 of this PIA for more details.

Azure Active Directory (AAD)
Azure Active Directory supports Microsoft 365 by providing an identity and access management service. It combines core directory services, identity governance and application access management. Azure Active Directory is a modern identity management solution spanning on-premises and cloud, providing the necessary security capabilities for application access control, federation, identity management, user provisioning, information protection, standard protocols support, comprehensive development libraries, and more.

Azure Rights Management Service
Azure Rights Management Service intends to protect information at the data level using encryption, user identity, and authorization policies to help secure files and email in transit across multiple devices—phones, tablets, and PCs. This service allows the province to encrypt shared data and apply policies on data to limit or allow actions by the recipient of the data.

Exchange Online
Microsoft Exchange Online is an email, calendar and contacts solution delivered as a cloud service, hosted by Microsoft. Exchange Online provides end users with a familiar email experience across PCs, the Web and mobile devices, while giving UNBC IT administrators web-based tools for managing their online deployment.

Exchange Online Protection (EOP)
Exchange Online Protection is the enterprise-class spam and malware filtering service offered in conjunction with Exchange Online. EOP can utilize layers of protection features deployed across a global network of data centres, simplifying the administration of messaging environments; however, for the purposes of UNBC, EOP will be deployed only through Canadian data centres.

Teams
Teams is an instant messaging client with audio and video chat capabilities. The real-time communications server software provides the infrastructure for enterprise instant messaging,

presence, VoIP, ad hoc and structured conferences (audio, video and web conferencing) and public switched telephone network (PSTN) connectivity through a third-party gateway or SIP trunk.

A feature of Teams is a function called Meeting Broadcast using a product called Stream. This component enables M365 users to produce and broadcast a meeting on the internet with up to 10,000 attendees, who can attend from a browser on virtually any device. With Stream, users can host large virtual meeting such as webinars, all-hands meetings, and other one-to-many presentations. Scheduling options allow attendance to be limited to people within UNBC.

SharePoint Online

SharePoint Online, part of the Microsoft 365 suite for online productivity solutions, and the successor to Business Productivity Online Services (BPOS), provides a platform for UNBC to enhance and extend the functionality of existing on-premises SharePoint deployments using a cloud-based service. SharePoint Online provides a single, integrated location where people can:

- *Collaborate with team members and external parties;*
- *Find organizational resources;*
- *Look up corporate information; and*
- *Glean business insights for better-informed decisions.*

OneDrive for Business is an integral part of Microsoft 365 and is provided by Microsoft 365's SharePoint Service. It provides a secure cloud storage location where employees can store, share, and sync their work files. OneDrive allows employees the ability to easily share files between their different devices.

Microsoft 365 (M365) is a software-as-a-service (SaaS) product. M365 was selected as the optimal choice because Microsoft operates datacenters for the services UNBC would like to utilize that are hosted in Canada.

Provided the appropriate safeguards, authentication, and logging are in place, UNBC will be able to work with Microsoft to enable and empower the employees and students to achieve better outcomes with a better experience.

2. Scope of this PIA

All faculty, staff, administrators, students will use M365 to manage most of the unstructured data they generate for as long as that data and its accompanying personal information remains in the custody and control of the university. Any alumni, researchers, visiting scholars, and external consultants that are provided access to any office productivity software at UNBC will be using M365. All faculty, staff, students, alumni, donors, vendors, consultants, and other payees will have at minimum identity information managed in Azure Active Directory.

This PIA does not include data management resulting through integration with Blackbaud Raiser's Edge NXT.

This PIA covers A3 License Features available as of June 2020. The option exists to move to A5 licensing for more security features which will be evaluated in future addendums.

3. Related Privacy Impact Assessments

PIA 17-007 for Office 365 was suspended because UNBC could not confirm whether this service was compliant and chose not to assume risk for deploying this serivce. With enough time and change to the plan for the delivery of Microsoft's services, this new PIA has been initiated.

4. All Elements of Information or Data

System or Service Data

System or Service Data is information about, and generated by, an information system or cloud service, and is non-personal in nature. Examples of service data include: remaining storage capacity, system health indicators, network traffic volume and bandwidth consumption. All of these are examined or used solely for the purpose of providing the cloud service. System data is distinct from UNBC content and is used solely for the purpose of providing, operating and maintaining the service, or diagnosing and/or troubleshooting in the event of problems or system outages.

Employee Contact Data

Employee Contact Data is information to identify and differentiate users of the cloud service. This includes User ID, Organizational ID and basic user contact information (e.g. phone number or email address). This information is used by Microsoft staff in order to troubleshoot service and access issues (e.g. jsmith cannot access file A). The majority of Employee Contact Data is considered either non-personal information, or business contact information.

UNBC Content Data

Customer content consists of data, information, documents, spreadsheets and other records that are authored, edited, communicated, maintained and eventually disposed of by the client. For the purposes of analysis, customer content is assumed to be, or assumed to contain personal information. Specific content will range in type, volume and sensitivity according to the client activities in using Microsoft Cloud Services. UNBC Content Data will not be stored in Microsoft Cloud Services outside of Canadian data centers.

Elements of User Data that will be synchronized with Microsoft Azure Active Directory

Attribute	IsExported	IsMandatory	Comments
accountEnabled	TRUE	TRUE	Defines if an account is enabled
accountName	TRUE	FALSE	
altRecipient	TRUE	FALSE	
assistant	TRUE	FALSE	
authOrig	TRUE	FALSE	
c	TRUE	FALSE	Country Abbreviation
cloudUserCertificate	TRUE	FALSE	
cloudUserSMIMECertificate	TRUE	FALSE	
cn	TRUE	FALSE	Common Name
co	TRUE	FALSE	Country Code
company	TRUE	FALSE	UNBC
countryCode	TRUE	FALSE	Region Code
dLMemRejectPerms	TRUE	FALSE	
dLMemSubmitPerms	TRUE	FALSE	
department	TRUE	FALSE	Department – populated from banner into AD on premise
description	TRUE	FALSE	UNBC filled in on occasion to help distinguish work accounts
deviceId	TRUE	FALSE	
deviceOSType	TRUE	FALSE	
deviceTrustType	TRUE	FALSE	
displayName	TRUE	FALSE	The customizable name – the preferred or given name in some cases
distinguishedName	TRUE	FALSE	The full location path within active directory.
domainFQDN	TRUE	FALSE	
domainNetBios	TRUE	FALSE	
employeeID	TRUE	FALSE	This is not the UNBC number – and is not populated by default
extensionAttribute1	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute10	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute11	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute12	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute13	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute14	TRUE	FALSE	Custom Attribute from UNBC-AD

extensionAttribute15	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute2	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute3	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute4	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute5	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute6	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute7	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute8	TRUE	FALSE	Custom Attribute from UNBC-AD
extensionAttribute9	TRUE	FALSE	Custom Attribute from UNBC-AD
facsimileTelephoneNumber	TRUE	FALSE	Not populated
givenName	TRUE	FALSE	Name
hideDLMembership	TRUE	FALSE	
homePhone	TRUE	FALSE	If populated by the user
info	TRUE	FALSE	
initials	TRUE	FALSE	Single Initial
ipPhone	TRUE	FALSE	Not populated
isIntuneManagedDevice	TRUE	FALSE	This is about a computer object, so is not PII
l	TRUE	FALSE	City
legacyExchangeDN	TRUE	FALSE	System attribute
mail	TRUE	FALSE	
mailNickname	TRUE	FALSE	
managedBy	TRUE	FALSE	Contact information – if employee
manager	TRUE	FALSE	Contact information – if employee
member	TRUE	FALSE	
middleName	TRUE	FALSE	
mobile	TRUE	FALSE	If populated by user – some UNBC mobiles are published
msDS-HABSeniorityIndex	TRUE	FALSE	
msDS-PhoneticDisplayName	TRUE	FALSE	
msExchArchiveGUID	TRUE	FALSE	
msExchArchiveName	TRUE	FALSE	
msExchAssistantName	TRUE	FALSE	
msExchAuditAdmin	TRUE	FALSE	
msExchAuditDelegate	TRUE	FALSE	
msExchAuditDelegateAdmin	TRUE	FALSE	
msExchAuditOwner	TRUE	FALSE	

msExchBlockedSendersHash	TRUE	FALSE	
msExchBypassAudit	TRUE	FALSE	
msExchBypassModerationLink	TRUE	FALSE	
msExchCoManagedByLink	TRUE	FALSE	
msExchDelegateListLink	TRUE	FALSE	
msExchELCExpirySuspensionEnd	TRUE	FALSE	
msExchELCExpirySuspensionStart	TRUE	FALSE	
msExchELCMailboxFlags	TRUE	FALSE	
msExchEnableModeration	TRUE	FALSE	
msExchExtensionCustomAttribute1	TRUE	FALSE	Custom Attribute from UNBC-AD
msExchExtensionCustomAttribute2	TRUE	FALSE	Custom Attribute from UNBC-AD
msExchExtensionCustomAttribute3	TRUE	FALSE	Custom Attribute from UNBC-AD
msExchExtensionCustomAttribute4	TRUE	FALSE	Custom Attribute from UNBC-AD
msExchExtensionCustomAttribute5	TRUE	FALSE	Custom Attribute from UNBC-AD
msExchHideFromAddressLists	TRUE	FALSE	
msExchImmutableId	TRUE	FALSE	
msExchLitigationHoldDate	TRUE	FALSE	
msExchLitigationHoldOwner	TRUE	FALSE	
msExchMailboxAuditEnable	TRUE	FALSE	
msExchMailboxAuditLogAgeLimit	TRUE	FALSE	
msExchMailboxGuid	TRUE	FALSE	
msExchModeratedByLink	TRUE	FALSE	
msExchModerationFlags	TRUE	FALSE	
msExchRecipientDisplayType	TRUE	FALSE	
msExchRecipientTypeDetails	TRUE	FALSE	
msExchRemoteRecipientType	TRUE	FALSE	
msExchRequireAuthToSendTo	TRUE	FALSE	
msExchResourceCapacity	TRUE	FALSE	
msExchResourceDisplay	TRUE	FALSE	
msExchResourceMetaData	TRUE	FALSE	
msExchResourceSearchProperties	TRUE	FALSE	
msExchRetentionComment	TRUE	FALSE	
msExchRetentionURL	TRUE	FALSE	
msExchSafeRecipientsHash	TRUE	FALSE	
msExchSafeSendersHash	TRUE	FALSE	
msExchSenderHintTranslations	TRUE	FALSE	

msExchTeamMailboxExpiration	TRUE	FALSE	
msExchTeamMailboxOwners	TRUE	FALSE	
msExchTeamMailboxSharePointLinkedBy	TRUE	FALSE	
msExchTeamMailboxSharePointUrl	TRUE	FALSE	
msExchUserHoldPolicies	TRUE	FALSE	
msOrg-IsOrganizational	TRUE	FALSE	
msRTCSIP-ApplicationOptions	TRUE	FALSE	
msRTCSIP-DeploymentLocator	TRUE	FALSE	
msRTCSIP-Line	TRUE	FALSE	
msRTCSIP-OptionFlags	TRUE	FALSE	
msRTCSIP-OwnerUrn	TRUE	FALSE	
msRTCSIP-PrimaryUserAddress	TRUE	FALSE	
msRTCSIP-UserEnabled	TRUE	FALSE	
oOFReplyToOriginator	TRUE	FALSE	
objectSid	TRUE	FALSE	Used to ensure that AAD and ADDS are in sync
onPremisesUserPrincipalName	TRUE	FALSE	
otherFacsimileTelephoneNumber	TRUE	FALSE	
otherHomePhone	TRUE	FALSE	Not populated
otherIpPhone	TRUE	FALSE	Not populated
otherMobile	TRUE	FALSE	Not populated
otherPager	TRUE	FALSE	Not populated
otherTelephone	TRUE	FALSE	Not populated
pager	TRUE	FALSE	Not populated
physicalDeliveryOfficeName	TRUE	FALSE	UNBC address
postOfficeBox	TRUE	FALSE	N/A
postalCode	TRUE	FALSE	UNBC Address
preferredLanguage	TRUE	FALSE	
proxyAddresses	TRUE	FALSE	
publicDelegates	TRUE	FALSE	Contact information
pwdLastSet	TRUE	FALSE	Used by both password synchronization application and federation tools
registeredOwnerReference	TRUE	FALSE	
reportToOriginator	TRUE	FALSE	
reportToOwner	TRUE	FALSE	
securityEnabled	TRUE	FALSE	
sn	TRUE	FALSE	Surname

sourceAnchor	TRUE	TRUE	Immutable identifier to maintain relationship between ADDS and AAD
st	TRUE	FALSE	UNBC Work Street
streetAddress	TRUE	FALSE	UNBC Work Address
targetAddress	TRUE	FALSE	
telephoneAssistant	TRUE	FALSE	
telephoneNumber	TRUE	FALSE	
thumbnailPhoto	TRUE	FALSE	Photo – if they have put one into outlook or OWA.
title	TRUE	FALSE	Title
unauthOrig	TRUE	FALSE	
url	TRUE	FALSE	
usageLocation	TRUE	FALSE	Used for license assignment
userCertificate	TRUE	FALSE	Public Key Certificate
userPrincipalName	TRUE	TRUE	Contact Information – UPN is the login ID for the user
userSMIMECertificate	TRUE	FALSE	S/MIME Public Key Certificate
wWWHomePage	TRUE	FALSE	

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

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

Microsoft's Canadian data centers are located in Quebec City and Toronto. Across its business, Microsoft stores Customer Data at rest within certain major geographic areas (a "GEO"). Canada has been defined as a "GEO", meaning that for UNBC's purposes, all customer created content will be resident within Canada.

System data is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. Its use is controlled and limited to the provisioning, maintenance, support and ongoing operation of cloud services. System data does not contain any personally identifiable information.

UNBC's Content Data will not be moved or copied to data centers outside Canada without UNBC's explicit permission and technical authorization. This technical authorization is done by a process called Customer Lockbox, in short in the event that a Microsoft employee needs access to data owned by UNBC in the course of troubleshooting then UNBC M365 administration will have to give explicit permission to that technician in order to review the data/logs. This permission is time based and will automatically be revoked. A key premise of the model is that the customer controls and owns their content, Microsoft has no standing access to the service components that UNBC is responsible for (applications configurations, and all application data) in their cloud SaaS solution. Customer Lockbox functionality applies to the Microsoft 365 server applications: Exchange, Skype, SharePoint, OneDrive and related services; as well as the Azure Service Fabric including the Azure Active Directory and related services.

There are opportunities amongst open fields for personal information to be present in Employee Contact Data such as the "home phone number" attribute. Attributes which are considered to contain personally identifiable information will not be stored in Microsoft Cloud Services outside of Canadian data centers.

*6. Data-linking Initiative**

In FIPPA, "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 the Information Governance Officer to discuss the requirements of a data-linking initiative.	*N/A*

*7. Common or Integrated Program or Activity**

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

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

Active Directory attributes are synchronized between on-premises systems and Microsoft Cloud Services globally, but no personally identifiable information is synchronized within Active Directory from on-premises systems. UNBC Content Data will regularly contain different types of personal information. The UNBC Content Data that flows between UNBC employees, officers, administration of UNBC, and all employees and associates of service providers using Microsoft 365 Services on behalf of UNBC to communicate with students, clients or members of the public may contain personally identifiable information. Each individual Content Data owner is responsible for understanding the flow of this data from collection to disposal.

See the appendices A-H containing the data flow diagrams of each of the major features of Microsoft 365.

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	***Mitigation Strategy***	***Likelihood***	***Impact***
1.	[redacted]			
2.				
3.				
4.				
7.				

	[redacted]
8.	
9.	
10.	

10. Collection Notice

After first sign in users will be notified of, and must agree to, the following Terms of Use based on their relationship to UNBC. Consent must be collected before the individual begins using the service or at the first opportunity to request the consent. Further consent documentation may be needed to address new services or changes to information management practices.

Student and Community Member accounts (all individuals that do not have an employment or contractual relationship with UNBC) during the first interaction with this service:

I recognize that The University of Northern British Columbia ("UNBC") is providing me with a Microsoft 365 account to communicate to me throughout my admission review process and to provide tools to support my learning experience if I choose to become a student at UNBC. The Microsoft 365 services ("M365") that UNBC is providing me are managed on a cloud service based in Eastern Canada. While UNBC controls how M365 manages my data, UNBC does not own the cloud infrastructure itself and there may be information management decisions made outside of UNBC about this infrastructure and M365 services. In the future, Microsoft may choose to change how it manages the cloud infrastructure and M365 services including where my personal information that I create, and the personal information created about me from other students and employees, resides. This may mean my personal information in part or in full could be transferred outside of Canada. UNBC will take reasonable measures to ensure that my personal information remains on Microsoft's Canadian servers. UNBC will notify me if they discover that my personal information has been disclosed and stored outside of Canada. By completing my application to UNBC and using the M365 services, I understand and consent to UNBC managing my personal information through M365 based on conditions of this notice. If I need to know more information about how my information is managed through the use of M365 services I can contact the IT Service Desk at 250-960-5321.

Staff, Faculty, Consultants / Contractors, (all individuals that have an employment or contractual relationship with UNBC):

The University of Northern British Columbia ("UNBC") is using Microsoft 365 services ("M365") to manage the majority of the information required for the regular activities of the university. In the process of managing information created, used, stored, disclosed and disposed through the M365 services, I understand that I must adhere to the UNBC Acceptable Use Policy and the Privacy and Access to Information Policy. I understand that under these policies I am responsible for the appropriate use of M365 to manage information to comply with the laws of British Columbia and Canada including but not limited to British Columbia's Freedom of Information and Protection of Privacy Act. If I have any questions or concerns about how I am expected to manage information using features of this platform, I will contact privacy@unbc.ca with my questions and I understand that I may need to be redirected to other departments on campus to support my information management needs.

Part 3 – Security of Personal Information

Please consult with the Information Governance Officer, the Chief Information Officer or the IT Security Officer when filling out this section if you have any questions.

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

[redacted]

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

[redacted]

[redacted]

[redacted]

13. Does your department rely on any security policies? If so, indicate here:

[redacted]

[redacted]

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.

[redacted]

[redacted]

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

[redacted]

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?

Azure Active Directory, where attributes about users are kept, will have the data synchronized with the on-premise active directory at least once a day in the case of normal attributes. [redacted] This is a fully automated process.

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

Any decisions made based on the data contained within Microsoft 365 would be the same decisions that would be made if the data had been stored on premises. The data steward for that information would be responsible for complying with the Act when managing personal information.

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

The data steward for UNBC Content Data will be responsible for ensuring that information is accurate and complete. ITS will ensure that any personal information found in Service and System Data is accurate and complete.

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

Each data steward for UNBC Content Data within Microsoft 365 is responsible for disposing of data in compliance with applicable statutes and regulations. Once a user decides to delete their data in any of the M365 services, the deleted data will be retained for 1-month, unless other arrangements have been specially made with the employee acting as either Privacy Officer or University Records Manager.

Each data steward is responsible for contacting the Information Governance Officer, or equivalent position acting as University Records Manager, to guide them on appropriate records management practices including collection, use, storage, disclosure and disposal for their office.

Part 5 – Further Information

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

No.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact the Information Governance Officer.	*N/A*

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 the Information Governance Officer, the UNBC Research Office or UNBC Archives.	*N/A*

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 FIPPA. Under this same section, this information is required to be published in a public directory.

Yes

Azure Active Directory contains user profile information matching employees to appropriate access to information and information management controls within databases containing structured and unstructured data. This PIB is designed to track the activities of all users of UNBC's M365 platform to ensure system compliance, security of information contained on UNBC's instance of the M365 platform, and integrity of user access controls.

In addition to user ID which is how the PIB arranges individuals, this PIB tracks: name, type of user, last logon time, location of user, how user interacts with the system, job title, direct supervisor.

Type of user is separated into categories including: Employees, Students, Alumni, Consultants, Post-Doctoral Fellows, Contractors, Prospective Students, Visiting Scholars, and any other types of users that may need to be defined as users on the M365 platform in the future.

The collection of the personal information constituting this PIB is compliant with section 26 (c) of the Act.

On campus, only the Information Technology Services department (ITS) has direct access to this Personal Information Bank and only utilize this PIB for the purposes mentioned above. Microsoft technicians may require limited access to this PIB to complete repairs and upgrades on the database.

Question 4 contains a table that defines the attribute types that may be available in this PIB.

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

Part 6 – Information Governance Officer Comments

This PIA is based on a review of the material provided to the Information Governance Officer 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 for approval.

The purchase of this service occurred without a specified purchase agreement for M365 cloud services. The purchase of this service was bundled into offline offerings that did not undergo a Privacy Impact Assessment at the time because these were internally managed resources.

Without a Privacy Protection Schedule attached to a contractual agreement with Microsoft, Microsoft may not understand their legal requirement as a service provider to a British Columbia public body to exclusively manage our data in Canada. For example in 2017, the Canadian GEO was defined as being inside "Toronto ON, Quebec City, QC and other United States datacentres" which accounts for the capacity to interpret a Canadian GEO as being managed in part outside of Canada. Microsoft has since adjusted this language to remove "and other United States datacentres" in their public facing documentation about the Canadian GEO, but it demonstrates that UNBC has to be aware that Microsoft can redefine the Canadian GEO again while we depend on their services to continue operations.

UNBC ITS will be responsible for ensuring that all new features, upgrades, available services, and data infrastructure changes continue to be managed in Canada by finding and maintaining a regular contact within Microsoft that can attest to the company meeting our data residency needs in all of their information management practices of our data in Canada.

The terms of service functionality can be used alongside a consent notice during the admission process to protect our lack of certainty regarding the ongoing management of personal information inside Canada. The unstructured records created and edited through the ProPlus suite (the online versions of Microsoft office applications including Word, Excel, PowerPoint, OneNote, Access, Publisher and Outlook) may contain personal information created or altered by third parties which may or may not be subject to circumstances where storage doesn't meet data residency requirements in the future. There isn't a reasonable means to manage informed consent from all users whose information interacts with this service because this system is a set of tools within an infrastructure to manage all of UNBC's functions, not provide a specific set of information management processes to consent to. There would be a difference between the information types that a student reasonably understands and can consent to being managed inside and outside of Canada (grades management, contact information, application and degree evaluation information) and what the student wouldn't possibly predict they would need to consent to having managed inside or outside of Canada (allegations of plagiarism, allegations of sexual assault, human resources complaints and case management, Health Services and Counselling records, disability management information if that disability develops while attending or working at the university).

Due to my comments indicated above, and the lack of a service agreement with a Privacy Protection Schedule attached that would give UNBC recourse if Microsoft were not to meet our data residency needs either intentionally or unintentionally, I cannot confirm with confidence that UNBC's use of the M365 suite will comply with the Act. The approval for the use of this service will need to escalate to our senior leadership team to address whether UNBC is in a position to assume this risk based on the contents of this PIA. My recommendation would be that this decision be brought to the Board of Governors for final approval.

Part 7 – Program Area Signatures

Kevin Schretlen		
Name of Individual leading the Program/Project (Normally the individual who completed the PIA)	*Signature*	*Date*
Trevor Fuson		
Program/Department Manager or Project Sponsor	*Signature*	*Date*
Dave Kubert		
Contact Responsible for Systems Maintenance and/or Security (if applicable)	*Signature*	*Date*
Adam Cullum	As per Part 6 cannot provide approval for FIPPA compliance	July 24 2020
Information Governance Officer	*Signature*	*Date*
Colleen Smith		
Vice President Finance and Administration (for Institutional Risk Management)	*Signature*	*Date*

Once the PIA has been approved with or without conditions, the Information Governance Officer will collect signatures from the individuals indicated above. A copy will be provided to all signatories for convenience or to attach to a requisition or file with a contract.

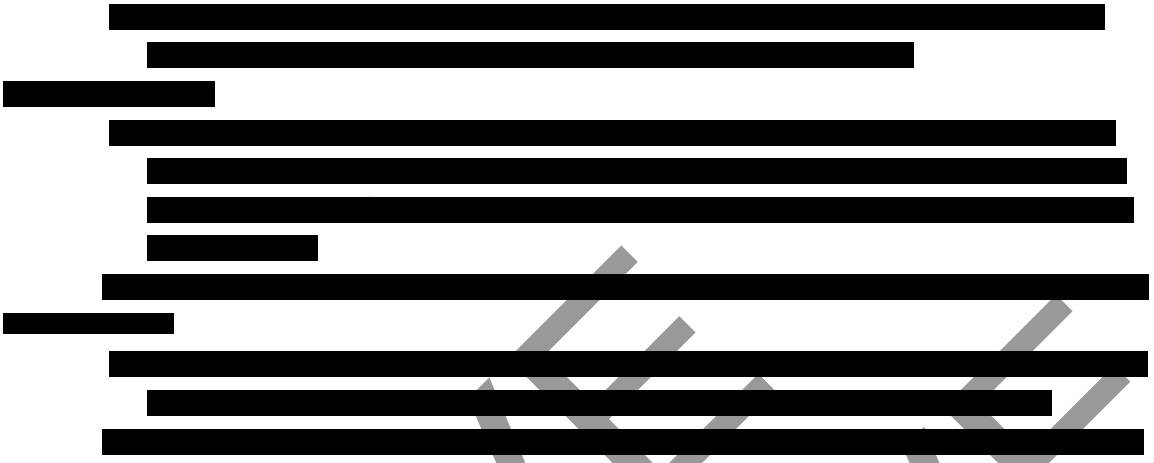
A final copy of this PIA (with all signatures) will be kept on record with the Information Governance Officer.

Appendix A

Microsoft Authentication Dataflow

NOTE: While there are many possible sites that you can login to, portal.office.com will be the site that is referenced here. All sites using the same credential set will have the same functionality.

DEFINITION: Hash – a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size and is a one-way function, that is, a function which is practically infeasible to invert.

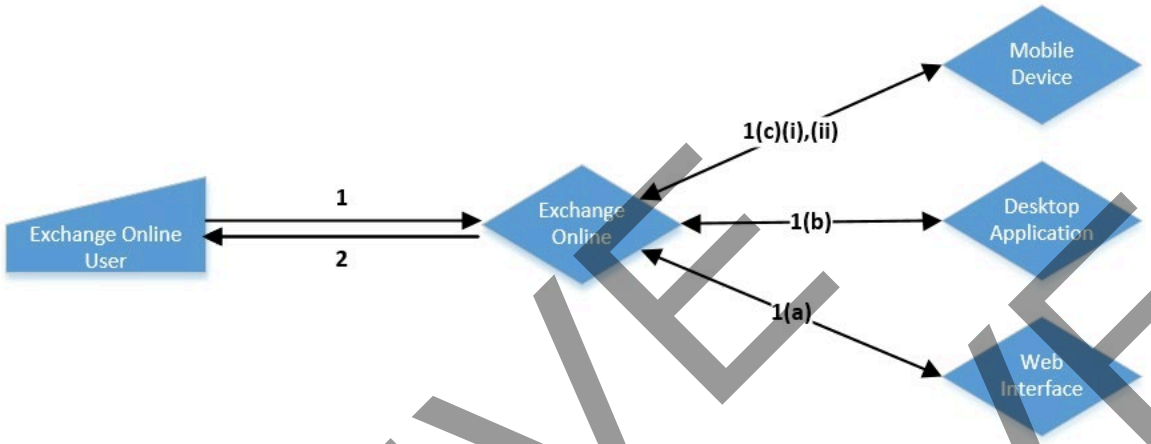


Appendix B

Microsoft Bookings Dataflow

1. A client/customer goes to a public website that asks for the following information
    a. The Service that they want to book (for example a campus tour)
    b. The individual with which they want to book the service (employee of UNBC)
    c. The Date & Time that they want to book
        i. Query made to Exchange Online to determine availability
    d. Name (does not need to be a real name, but must be filled in)
    e. Email Address (used for reminders of the booking)
    f. Optional – Phone Number
    g. Optional – Address
    h. Optional – Additional Notes / Special requests
2. Once the form is completed they submit the booking and are notified that a confirmation will be sent shortly
    a. The Client/Customer receives a email with the booking and a calendar schedule
3. The Employee also receives an email with the following information
    a. Name of the person who booked
    b. Link to the booking
4. The Employee's calendar is updated to reflect the booking. The calendar item has the following information
    a. Booking Time (Start, End, Date)
    b. Customer Information
        i. Name (1d)
        ii. Email (1e)
        iii. Phone Number (1f)
        iv. Address (1g)
        v. TimeZone (system generated)
    c. Booking information
        i. Service Information
        ii. Price (if applicable)
    d. Buffer time
        i. Time padded before of after booking
    e. Internal Notes
        i. Notes added by customer (1h)
5. As the scheduled booking comes closer, optional alerts can be sent out to help reduce no-shows and remind the client/customer that they are scheduled.

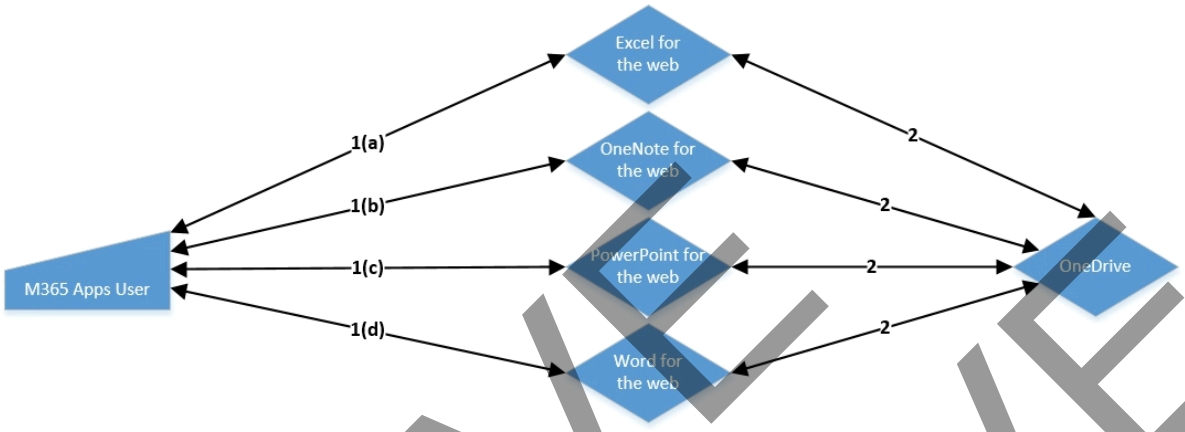
Data Flow – Exchange Online



1. Exchange User accesses the Exchange Online system through one of three methodologies
    a. Web Interface – available on any internet connected device with a modern browser, commonly known as OWA (Outlook Web Application)
    b. Desktop Application – Exchange is accessed through Outlook for PC, or Outlook for Mac. There are a variety of other applications that can be used to access Exchange online including Thunderbird. Non-Microsoft Access applications are outside of the scope of this PIA.
    c. Mobile Device – There are two different approaches for mobile devices.
        i. Active-Sync connections to Exchange Online
        ii. Outlook Application for the Mobile Device
2. Exchange Online data is exchanged with the user's access methodology in a secure, encrypted fashion

Appendix D

Data Flow – Microsoft365 Apps for Enterprise (Office ProPlus



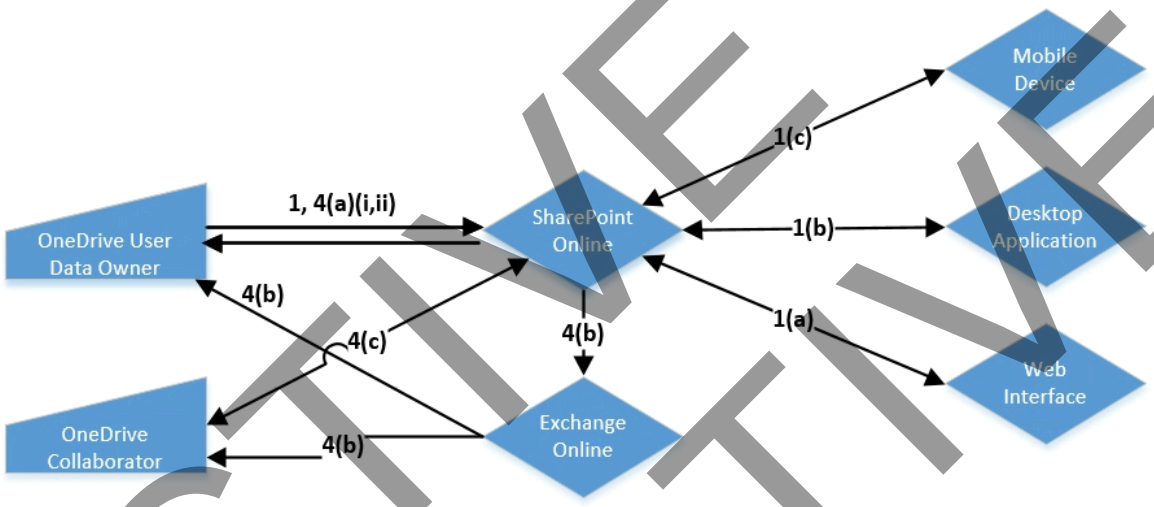
Note: Microsoft 365 Applications for Enterprise is the new name for Office 365 ProPlus.
Note: The suite of applications included for windows users is Word, Excel, PowerPoint, Visio, Outlook, and OneNote.
Note: Outlook is a tool used to interface with Exchange Online and on-premises Exchange servers, so will not be part of this data flow diagram as it is covered in other diagrams.

1. M365 Apps for Enterprise Users can access and open the applications either as a download to their desktop, on a modern web-browser
    a. Excel for the web – mirrors functionality of the full application for basic use
    b. OneNote for the web – mirrors functionality of the full application for basic use
    c. PowerPoint for the web – mirrors functionality of the full application for basic use
    d. Word for the web – mirrors functionality of the full application for basic use
2. M365 Apps for Enterprise work with OneDrive (a SharePoint enabled service)

Appendix E

Microsoft OneDrive Dataflow

1. Once the form is completed, they submit the booking and are notified that a confirmation will be sent shortly
    a. The Client/Customer receives an email with the booking and a calendar schedule



2.

Individual Use – Not Shared

3. A OneDrive user can work with the OneDrive application in one of the following ways
    a. Online through a web browser
    b. Through a full-featured application on a computer or laptop
    c. Through a mobile application on their phone or device.
4. Data housed within the OneDrive system is available on all methods of access, and can be selectively synchronized with locations on demand or by explicit rules.
5. Data flows between the user access method and the SharePoint online storage location by way of encrypted methods.

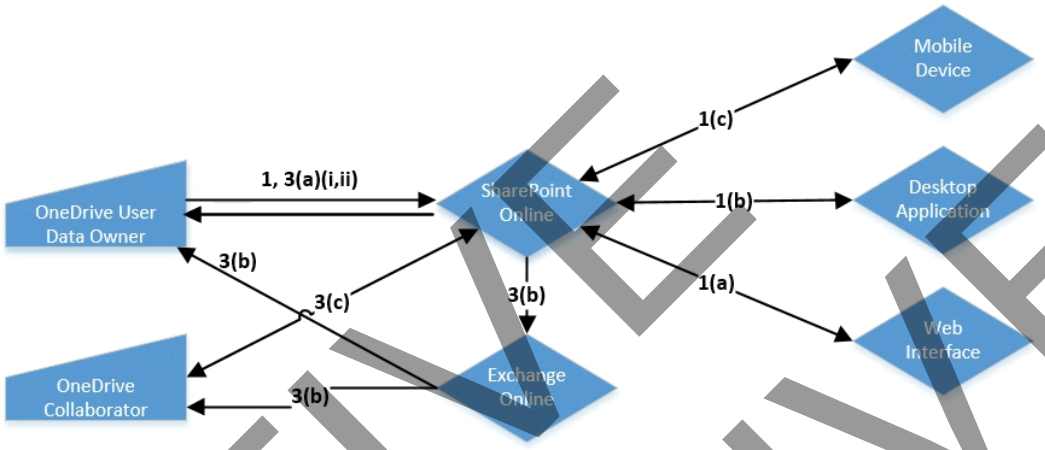
Sharing files with other people

4. A single file, or folder containing multiple files can be shared with one or more people inside our outside the organization from a personal OneDrive. The following steps outline the communication process that happens when this occurs
    a. The owner of the file selects share, and enters in the following information
        i. If they are inside the organization, then they need only enter the person's name
        ii. If they are outside the organization, they need to enter the persons' email address

b. The system, using exchange online, sends an invite link, carbon copying the owner of the files so that the owner is aware of the share.
c. The recipient of the link can open and modify the documents as they see fit.

Appendix F

Data Flow – Sharepoint Online

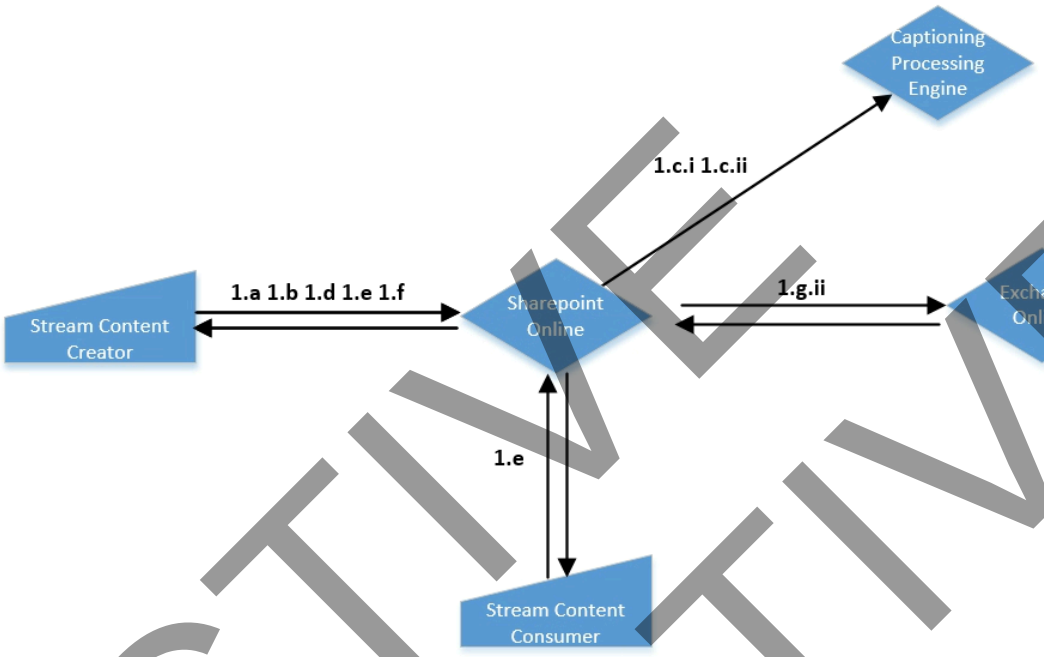


1. SharePoint User accesses the SharePoint online system through one of three methodologies
    a. Web Interface – available on any internet connected device with a modern browser
    b. Desktop Application – SharePoint is accessed through integrated applications. For example the Microsoft Teams Application, or OneDrive Application
    c. Mobile Device – iOS and Android versions of the SharePoint application are available to download and install.
2. SharePoint Data is exchanged with the user's access methodology in a secure, encrypted fashion
3. Sharing of documents can be setup for those that need it the process is as follows

    A single file, or folder containing multiple files can be shared with one or more people inside our outside the organization from a personal OneDrive. The following steps outline the communication process that happens when this occurs
    a. The owner of the file selects share, and enters in the following information
        i. If they are inside the organization, then they need only enter the person's name
        ii. If they are outside the organization, they need to enter the persons' email address
    b. The system, using exchange online, sends an invite link, carbon copying the owner of the files so that the owner is aware of the share.
    c. The recipient of the link can open and modify the documents as they see fit.
4.

Appendix G

Microsoft SharePoint Data Flow



DEFINITION: SharePoint Online is a collection of SharePoint sites, each of which has its own document management repository, notebook, wiki, and other related services.

1) A Stream Content Creator uploads a video to the stream service. The uploads are located in the Tenant's SharePoint Site.
    a. The Content Creator will be prompted to name the video (default behaviour will use the file name of the video)
    b. The Content Creator will be asked for an optional description of the video.
    c. Captions will be automatically created – the user can choose which language they prefer the captions be created in (the default is the user's default language that they have chosen in their profile)
        i. Caption creation can be disabled per video in the options on the video.
        ii. This can be enabled/disabled by the content creator or by anyone who has "owner" privileges on the video.
    d. The Content creator sets the viewable permissions on the video
        i. Default behaviour is that everyone inside the organization can see the video – this can be unselected by the content creator (check box)
        ii. The content creator can add specific groups and grant permissions to those groups as groups who can see the video or groups that can be co-owners of the video, which will allow people within the owners group to

add additional viewers, or change the description or other data about the stream video.

iii. If groups are too broad for permissions, individual users can be added to viewer permission or owner permission.

e. Comments can be enabled or disabled on each video individually as per the Content Creator or by anyone who has been assigned as an “owner” of the stream video.

f. Subtitles can be added manually by either the content creator or by anyone with an ownership level of permissions on the video.

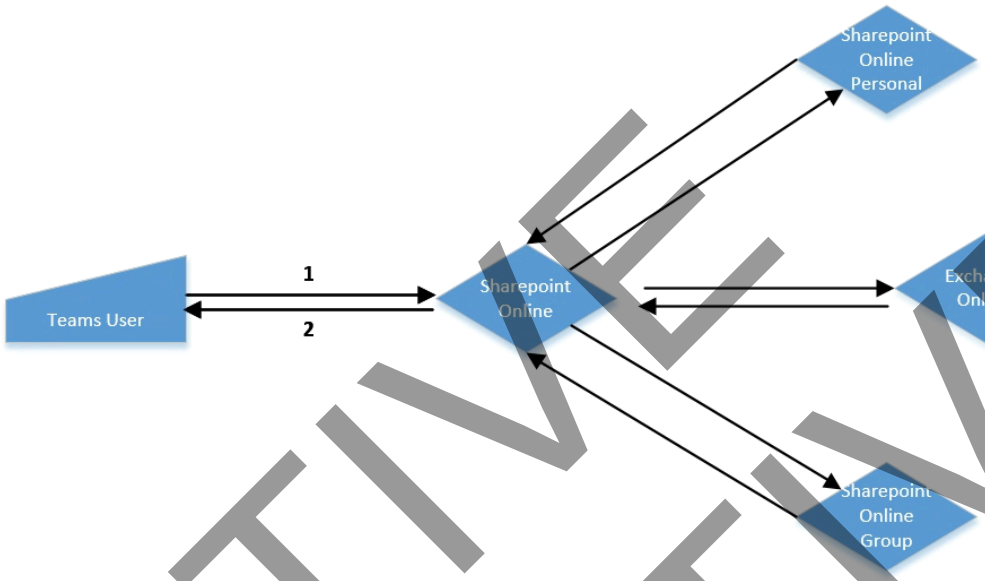
g. Content Creators can either Publish or Share

   i. Publish – it will make the video that the Content Creator requested with the settings that they requested.

   ii. Share – the recipient must be a M365 user within UNBC’s tenant. Note this can be imbedded within web pages as well, but only authorized UNBC M365 users will be able to view the content and post comments if they are enabled.

Appendix H

Microsoft Teams Data Flow



DEFINITION: SharePoint Online is a collection of SharePoint sites, each of which has its own document management repository, notebook, wiki, and other related services.
DEFINITION: a Group in this case is a Microsoft 365 Group (which exists in Azure Active Directory). This group is a collection of individuals and includes by default an Exchange Online mailbox (with an email address, Inbox and Calendar), and a SharePoint site (with document library), a Planner, a OneNote notebook and potentially other services.

NOTE: A Microsoft 365 Group must be created in Azure Active Directory, this provisions the underpinning SharePoint Online and Exchange Online requirements.

1) An individual opens the Microsoft Teams app through one of three methods, via the web application available on all platforms, the full client application available on Microsoft and Mac, and mobile client versions available on iOS and Android.
2) An individual will receive an invitation email from the Team's Site (SharePoint) through the Exchange Online service.
3) If they are part of a M365 Group that has a corresponding Team, they will see a list of Teams in which they are members.
4) An individual can interact with Teams largely in two ways, through channels, or chats.
    a. Channels (Public)
        i. All data uploaded to a channel, shared documents, wiki pages are stored on the team's SharePoint site. They are searchable by the team and are available to anyone that is part of that team
    b. Channels (Private)

    i. All data uploaded to a private channel is housed in a hidden folder within the same SharePoint site

c. Chats (up to two people)
    i. All data uploaded to a chat is kept in a user's personal SharePoint repository. This repository is shared with the OneDrive service.

d. Chats (three or more people)
    i. All data is uploaded to the user's SharePoint site who uploaded the content. For example if someone shares a picture of their cat, that image would be available for everyone in the chat to see, but would be only stored on the person's SharePoint site who uploaded the image.

Security and Compliance

Published: January 2016

Introduction

When moving your organization to cloud services, security concerns add another layer of consideration; one of trust. You have to be able to trust your service provider with processing the data that you provide to the service provider through your use of the online service, which is "your data." Security, compliance, and privacy in Office 365 has two equally important dimensions:

- The first dimension includes Microsoft-managed service-level capabilities that include technologies, operational procedures, and policies that are enabled by default.
- The second dimension includes customer-managed controls that enable you to customize your Office 365 environment based on the specific needs of your organization, while still maintaining security and compliance.

Security and compliance is an ongoing process, not a steady state. It is constantly maintained, enhanced, and verified by highly-skilled, experienced and trained personnel. We strive to keep software and hardware technologies up to date through robust processes. To help keep Office 365 security at the top of the industry, we use processes such as the Security Development Lifecycle; we also employ techniques that throttle traffic and prevent, detect, and mitigate breaches.

For the latest information on Office 365 security and compliance, visit the Office 365 Trust Center.

Service-Level Security

Microsoft is recognized as an industry leader in cloud security. Using decades of experience building enterprise software and running online services, our team is constantly learning and continuously updating our services and applications to deliver a secure cloud productivity service that meets rigorous industry standards for compliance.

At the service level, we use a defense-in-depth strategy that protects your data through multiple layers of security (physical, logical and data):

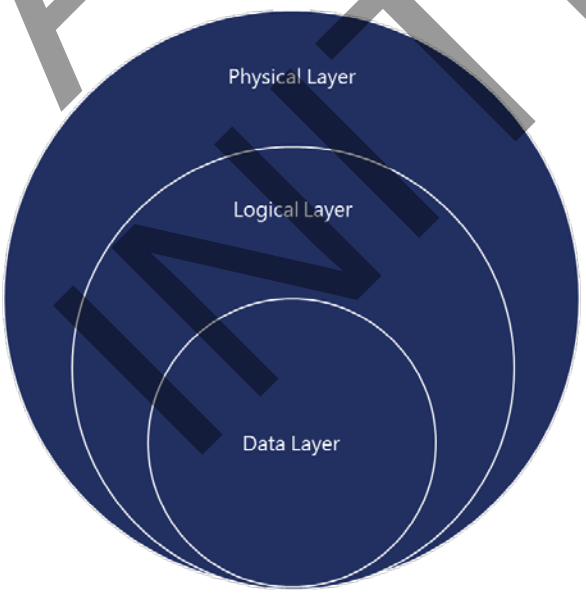


Figure 1 - Multiple layers of defense in depth

A defense-in-depth strategy ensures that security controls are present at various layers of the service and that, should any one area fail, there are compensating controls to maintain security at all times. The strategy also includes tactics to detect, prevent, and mitigate security breaches before they happen. This involves continuous improvements to service-level security features, including:

- Port scanning and remediation
- Perimeter vulnerability scanning
- Operating system security patching
- Network-level distributed denial-of-service (DDoS) detection and prevention
- Multi-factor authentication for service access

For more information on how Office 365 is protected against DDoS attacks, see Defending Office 365 against denial of service attacks, available for download from the Service Trust Portal (STP). Note, you must be enrolled in the STP to access this document. Enrollment is free and easy for all Office 365 tenants (including trial subscriptions). See Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions for steps to enroll.

With regards to people and process, preventing breaches involves:

- Auditing all operator/administrator access and actions
- Zero standing permission for administrators in the service
- Just-In-Time access and elevation that is granted on an as-needed and only-at-the-time-of-need basis to troubleshoot the service
- Segregation of the employee email environment from the production access environment
- Mandatory background checks for high-privilege access. These checks are a highly scrutinized, manual-approval process.

Preventing breaches also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services.

We continue to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. We are also continuously evolving a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. We regularly conduct penetration tests to enable continuous improvement of incident response procedures. These internal tests help our security experts create a methodical, repeatable, and optimized stepwise response process and automation.

Physical Layer – Facility

Customer data is stored in our Office 365 datacenters that are geographically distributed while taking regional data location considerations into account. Our datacenters are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Datacenter access is restricted 24 hours a day by job function—with only customer application and services access given to essential personnel. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video

surveillance, and two-factor authentication. The datacenters are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems and seismically braced racks where necessary.

Physical Layer – Network

Perimeter protection is implemented through the use of controlled devices at the network edge and on points throughout the network. The overarching principle of our network security is to allow only connections and communications that are necessary to allow systems to operate, blocking all other ports, protocols and connections. Access Control Lists (ACLs) implemented in the form of tiered ACLs on routers, IPsec policies on hosts, firewall rules and host based firewall rules are implemented in the network with restrictions on network communication, protocols, and port numbers. Edge router security allows the ability to detect intrusions and signs of vulnerability at the network layer. Networks within the Office 365 datacenters are further segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces.

Logical Layer

The logical layer of security involves many controls and processes implemented to secure the host machines, applications running on those hosts and from administrators that may perform any work on those host machines and applications.

Automated Operations

Most of the operations performed on hosts and applications by administrators are automated so that human intervention is reduced to a minimum, reducing the possibility of an inconsistent configuration or a malicious activity. This automated approach extends to the deployment of systems within our datacenters.

Admin Access to Data

Administrator access to Office 365 and your data is strictly controlled. Core tenets of this process are role based access and granting personnel least privilege access to the service that is necessary to perform specific operations. These tenets are followed whether the access is physical (i.e., to the datacenter or the servers) or logical. An example where this comes to life is a process called “Lockbox” that administrators use to request access for elevated privileges.

Access control happens at various levels:

- Personnel level to ensure that there are appropriate background checks and strict account management so that only those essential to the task may perform the task
- Role based access control
- A Lockbox process which allows:
    - Just-in-time accounts with high-entropy passwords
    - Access for a limited amount of time
    - Access to take specific actions based on the role
- The servers in the Office 365 service have a pre-determined set of processes that can be run using Applocker
- Auditing and review of all access

Security Development Lifecycle

The Microsoft Security Development Lifecycle (SDL) is a comprehensive security assurance process that informs every stage of design, development, and deployment of our software and services, including Office 365. Through design requirements, analysis of attack surface, and threat modeling, the SDL helps us predict, identify, and mitigate vulnerabilities and threats from before a service is launched through its entire BitLocker production lifecycle. We continuously update the SDL using the latest data and best practices to help ensure that new services and software associated with Office 365 are highly secure from day one.

Anti-malware, Patching, and Configuration Management

The use of anti-malware software is a principal mechanism for protection of your assets in Office 365 from malicious software. The software detects and prevents the introduction of computer viruses and worms into the service systems. It also quarantines infected systems and prevents further damage until remediation steps are taken. Anti-malware software provides both preventive and detective control over malicious software.

Our standard baseline configuration requirements for servers, network devices, and other Microsoft applications are documented where the standards outline the use of a standard package. These packages are pretested and configured with security controls.

Changes, such as updates, hotfixes, and patches made to the production environment, follow the same standard change management process. Patches are implemented within the time frame specified by the issuing company. Changes are both reviewed and evaluated by our review teams and the Change Advisory Board for applicability, risk, and resource assignment prior to being implemented.

Data Layer

Office 365 is a highly scalable multi-tenant service, which means that your data securely shares the some of the same hardware resources as other customers. We have designed Office 365 to host multiple customers in the service in a highly secure way through data isolation. Data storage and processing for each tenant is segregated through Azure Active Directory and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Azure Active Directory isolates your data using security boundaries. This safeguards your data so that the data cannot be accessed or compromised by co-tenants.

Data Integrity and Encryption

Office 365 has several cryptography and encryption features. For details on these features, see Data Encryption Technologies in Office 365, available for download from the Service Trust Portal (STP). Note, you must be enrolled in the STP to access this document. Enrollment is free and easy for all Office 365 tenants (including trial subscriptions). See Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions for steps to enroll.

Protection from Security Threats

Threat management strategy for Office 365 is a composite of identifying a potential threats intent, capability, and probability of successful exploitation of a vulnerability. The controls used to safe guard against such exploitations are heavily founded upon security standards. By validating the ISO

27001/27002 and NIST 800-53 controls implemented by Microsoft via the independent audits of these controls, you are able to assess the effectiveness of the controls deployed by us.

The overall cyber threat landscape has evolved from traditional opportunistic threats to also include persistent and determined adversaries. We equip you with a defense-in-depth approach to address the continuum of threats ranging from common "hacktivists" to cyber criminals to nation-state actors.

Our Office 365 security strategy is founded upon a dynamic strategy with four pillars of thought. The mindset shift we made to make our defenses more effective and ever evolving is commonly referred to as "Assume Breach" and assumes that a breach has already happened in the environment and is simply not known. With this mindset, the security teams are continuously attempting to detect and mitigate security threats that are not widely known. One set of exercises is to artificially propagate a security threat and have another group respond and mitigate the threat. The primary goal of these exercises is to make Office 365 resilient so the new vulnerabilities are quickly detected and mitigated.

- The first pillar of the security strategy is referred to as "Prevent Breach." Our investment in this pillar involves continuous improvements to built-in security features. These include port scanning and remediation, perimeter vulnerability scanning, operating system patches, network level Isolation/breach boundaries, DDoS detection and prevention, just-in-time access, live site penetration testing, and multi-factor authentication for service access.
- The second pillar is referred to as "Detect Breach." In this pillar, our system and security alerts are harvested and correlated via a massive internal analysis system. The signals analyze alerts that are internal to the system as well as external signals (for example coming from customer incidents). Based on machine learning, we can quickly incorporate new patterns to trigger alerts, as well as automatically trigger alerts on anomalies in the system.
- The third pillar is referred to as "Respond to Breach." This pillar is used to mitigate the effects if a component is compromised. A diligent incident response process, standard operating procedures in case of an incident, ability to deny or stop access to sensitive data and identification tools to promptly identify involved parties helps ensure that the mitigation is successful.
- The fourth pillar is referred to as "Recover from Breach," which includes the standard operating procedures to return the service to operations. The pillar includes the ability to change the security principals in the environment, automatically update the affected systems, and audit the state of the deployment to identify any anomalies.

Advanced Threat Protection

Office 365 provides robust email protection against spam, viruses and malware with Exchange Online Protection (EOP). But as hackers around the globe launch increasingly sophisticated attacks, many organizations are seeking tools that provide advanced protection. That's why Exchange Online offers Advanced Threat Protection (ATP), an email filtering service that provides additional protection against specific types of advanced threats. ATP for Exchange Online delivers the following benefits:

- Protection against unknown malware and viruses—Today EOP employs a robust and layered anti-virus protection powered with three different engines against known malware and viruses. ATP extends this protection through a feature called Safe Attachments, which protects against unknown malware and viruses, and provides better zero-day protection to safeguard your messaging system. All messages and attachments that don't have a known virus/malware signature are routed to a special hypervisor environment, where a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent. If no suspicious activity is detected, the message is released for delivery to the mailbox.
- Real time, time-of-click protection against malicious URLs—EOP scans each message in transit in Office 365 and provides time of delivery protection, blocking any malicious hyperlinks in a message. But attackers sometimes try to hide malicious URLs with seemingly safe links that are redirected to unsafe sites by a forwarding service after the message has been received. ATP's Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link, as malicious links are dynamically blocked while good links can be accessed.
- Rich reporting and URL trace capabilities—ATP also offers rich reporting and tracking capabilities, so you can gain critical insights into who is getting targeted in your organization and the category of attacks you are facing. Reporting and message tracing allows you to investigate messages that have been blocked due to an unknown virus or malware, while the URL trace capability allows you to track individual malicious links in the messages that have been clicked.

For more information, see Introducing Exchange Online Advanced Threat Protection.

Security Monitoring and Response

Many threats target software vulnerabilities, but others attack operational weaknesses, which is why Microsoft uses the Operational Security Assurance (OSA) framework. OSA supports continuous monitoring, helps to identify operational risks, provides operational security guidelines, and validates that those guidelines are followed. OSA helps make Microsoft cloud infrastructure more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to security threats.

Independent Verification

Office 365 has operationalized security into a scalable process that can quickly adapt to security trends and industry-specific needs. Microsoft engages in regular risk management reviews, and it develops and maintains a security control framework that meets the latest standards. Internal reviews and external audits by trusted organizations are incorporated into the Office 365 service life cycle. Close working relationships with other Microsoft teams result in a comprehensive approach to securing applications in the cloud.

Key standards that give you confidence in Microsoft's security technologies and best practices are independent audits and verifications of adherence to standards embodied in ISO 27001, SSAE 16 SOC1 Type II and HIPAA.

Customer Controls for Security

Office 365 combines the familiar Microsoft Office suite with cloud-based versions of our next-generation communications and collaboration services: Exchange Online, SharePoint Online, and Skype for Business. Each of these services offers individualized security features that you can control. These controls allow you to help adhere to compliance requirements, give access to services and content to individuals in your organization, configure anti-malware / anti-spam controls, and encrypt data.

Along with the encryption technologies in Office 365 that are managed by Microsoft, Office 365 also includes encryption features that customers can manage and configure. These technologies, which offer a variety of ways to encrypt customer data at rest or in-transit, are:

- Rights Management Services
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Secure mail flow with a partner organization

Information on these technologies can also be found in the Office 365 service descriptions.

You also have configuration options for anti-malware/anti-spam controls in the service. You may optionally choose to use your own anti-malware service and route to and from Office 365 via that third-party service. Office 365 uses multi-engine anti-malware scanning to protect incoming, outgoing, and internal messages from malicious software transferred through email.

Your administrators can use the Office 365 Administration Center to manage anti-malware/anti-spam controls, including advanced junk mail options and organization-wide safe and blocked sender lists. Individual users can manage their safe and blocked senders from within their inboxes in Outlook or Outlook on the web.

Content controls and multi-engine malware scanning also help eliminate documents containing malicious code. Based on file name extensions, Office 365 blocks certain file types that can contain malicious code from being uploaded to or retrieved from the service. Office 365 uses an intelligent instant message filter to help protect the service and your networks against malware and spam via IM.

Highly Secure End-User Access

Office 365 customer data and services are secured at the datacenter, network, logical, storage, and transit levels. In addition, it is critical to be able to control access to data and how it may be used. In the Office 365 service, Azure Active Directory is used as the underlying identity platform. This enables your tenant with strong authentication options granular control over how IT professionals and users can access and use the service. Office 365 also allows integration with an on-premises Active Directory or other directory stores and identity systems such as Active Directory Federation Services (ADFS) or third-party secure token systems (STSs) to enable secure, token-based authentication to services.

Federated Identity and Single Sign-on

Your administrators can federate on-premises Active Directory or other directory stores with Azure Active Directory. After federation is configured, all Office 365 users whose identities are based on the federated domain can use their existing corporate logons to authenticate to Office 365. Federation enables secure, token-based authentication. This also allows administrators to create additional authentication mechanisms such as:

- Multi-factor authentication
- Client-based access control, allowing organizations to control how users access information from specific devices or specific locations or a combination of both (for example, limiting access from public computers or from public open Wi-Fi)
- Role-based access control (RBAC), similar to the access control procedure for Microsoft datacenters described earlier in the "Automated operations" section

With IM federation, Skype for Business users can IM in a highly secure environment with users in other organizations that use Skype for Business, on-premises Skype for Business or Lync Server, and even the Skype public IM network. All federated communications are encrypted between the IM systems using access proxy servers. In addition, Skype for Business allows administrators to save IM conversations.

Multi-factor Authentication

Multi-factor authentication enhances security in a multi-device and cloud-centric world. We provide an in-house solution for multi-factor authentication with a phone call, text message, or notification on a dedicated app. We also support third-party multi-factor authentication solutions.

Multi-factor authentication options include:

- Call my mobile phone. The user receives a phone call that asks them to press the pound key. Once the pound key is pressed, the user is logged in.
- Text code to my mobile phone. The user receives a text message containing a six-digit code that they must enter into the portal.
- Call my office phone. This is the same as Call my mobile phone, but it enables the user to select a different phone if they do not have their mobile phone with them.
- Notify me through app. The user configured a smartphone app and they receive a notification in the app that they must confirm the login. Smartphone apps are available for Windows Phone, iPhone, and Android devices.
- Show one-time code in app. The same smartphone app is used. Instead of receiving a notification, the user starts the app and enters the six-digit code from the app into the portal.

Users who are enrolled for multi-factor authentication are required to configure App Passwords in order to use Office desktop applications, including Outlook, Skype for Business, Word, Excel, PowerPoint, and OneDrive for Business.

Once your information worker has logged in with multi-factor authentication, they will be able to create one or more App Passwords for use in Office client applications. An App Password is a 16-character randomly generated password that can be used with an Office client application as a way of increasing security in lieu of the second authentication factor.

For more information, see Multi-Factor Authentication for Office 365.

Privacy by Design

When you entrust your data to Office 365 you remain the sole owner: you retain the rights, title, and interest in the data you store in Office 365. The data you store in Office 365 is "your data."

It is with this clarity of principle that we ensure that we maintain your privacy and operate our online services with certain key principles:

- We use your data only to provide you with the online services you have paid for, including purposes compatible with providing those services
- We do not mine your data for advertising purposes
- If you ever choose to leave the service, you can take your data with you with full fidelity
- We tell you where your data resides, who has access, and under what circumstances
- Access to your data is strictly limited, non-destructive, logged and audited[1]

Beyond this, we have privacy controls to allow you to configure exactly who has access to what within your organization. Strict controls and design elements prevent or mingling of your data with that of other organizations using Office 365 and from Office 365 datacenter staff having access to your data.

In addition, Microsoft redirects government requests for your data to be made directly to you unless legally prohibited and has challenged government attempts to prohibit disclosure of such requests in court.

Customer Controls for Privacy

In addition to service-level capabilities, Office 365 enables you to collaborate through the use of transparent policies and strong tools while providing the distinct ability to control information sharing.

- Customer Lockbox—Allows customers to control Microsoft engineering access to customer data.
- Rights Management in Office 365—Allows individuals and administrators to specify access permissions to documents, workbooks, and presentations. This helps you prevent sensitive information from being printed, forwarded, or copied by unauthorized people by applying intelligent policies.
- Privacy controls for sites, libraries and folders—SharePoint Online, a key component service of Office 365 that provides collaboration functionality has a number of privacy controls. One example is that SharePoint Online sites are set to "private" by default. A second example is that a document uploaded to OneDrive for Business is not shared until the user provides explicit permissions and identifies who to share with.
- Privacy controls for communications—In Skype for Business, another key component service that provides real-time communications in Office 365, there are various administrator-level controls as well as user-level controls to enable or block communication with external users and organizations. One example is blocking access to federation in Skype for Business. Similarly,

[1] Third-party audits are performed to attest that access is only for appropriate business purposes.

there are controls throughout the service for the admins and users to ensure privacy of their content and communications.

Service Compliance

Operating a global cloud infrastructure creates a need to meet compliance obligations and to pass third-party audits. Auditable requirements come from government and industry mandates, internal policies, and industry best practices. Continuous compliance refers to our commitment to evolve the Office 365 controls and stay up to date with IT standards and regulations.

As a result, Office 365 has obtained independent verification, including ISO 27001, ISO 27018, and SSAE 16 audits; is able to transfer data outside of the European Union through the EU Model Clauses; is willing to sign a HIPAA Business Associate Agreement (BAA) with all customers; has received authority to operate from a U.S. federal agency under FISMA; and has disclosed security measures through the Cloud Security Alliance's public registry. Office 365 extends the controls implemented to meet these standards to customers who are not necessarily subject to the respective laws or controls.

ISO 27001

Office 365 service meets ISO 27001 standards and was the first major business productivity public cloud service to have implemented the rigorous set of global standards covering physical, logical, process, and management controls.

ISO 27018

ISO 27018 is the first international standard for privacy in the cloud. Microsoft was the first major cloud service provider to be independently verified as meeting ISO 27018.

SSAE 16

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

FISMA

Office 365 has been granted FISMA moderate Authority to Operate by multiple federal agencies. Operating under FISMA requires transparency and frequent security reporting to our U.S. Federal customers. Microsoft applies these specialized processes across our infrastructure to further enhance our Online Services Security and Compliance program for the benefit of customers who are not subject to FISMA requirements.

HIPAA BAA

Office 365 is the first major business productivity public cloud service provider to offer a HIPAA Business Associate Agreement (BAA) to all customers. HIPAA is a U.S. law that applies to healthcare entities—it governs the use, disclosure, and safeguarding of protected health information (PHI), and imposes requirements on covered entities to sign business associate agreements with their vendors that have access to PHI.

EU Model Clauses

Office 365 became the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union (known as the "EU Model Clauses") with all

customers. The EU Model Clauses address the international transfer of data. Office 365 is one of very few cloud services—if not the only cloud service—that has received broad validation from European data protection authorities (DPAs) regarding its approach to the EU Model Clauses, including from Bavaria, Denmark, France, Ireland, Luxembourg, Malta, and Spain.

Further, the Article 29 Working Party, a consortium of European data protection authorities, has publicly stated that our contractual commitments meet the requirements of the EU Model Clauses. Microsoft is the first cloud services provider to get such an approval from the Article 29 Working Party. You can read more about this here.

Cloud Security Alliance

Office 365 meets compliance and risk management requirements as defined in the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM). The CCM is published by a not-for-profit, member-driven organization of leading industry practitioners focused on helping customers make the right decisions when moving to the cloud. The matrix provides a detailed understanding of the security and privacy concepts and principles that are aligned to CSA guidance across 13 domains. Office 365 has published a detailed overview of its capabilities for the CCM requirements that illustrates how these capabilities meet these requirements and empowers customers with in-depth information to evaluate different offerings in the marketplace today.

Customer Controls for Compliance

With Office 365, we offer a range of compliance features, including data loss prevention (DLP), eDiscovery, and auditing and reporting functionality. Across these capabilities, the user experience is preserved and productivity is not affected, leading to greater user acceptance.

Data Loss Prevention

Although malware and targeted attacks can cause data breaches, user error is actually a much greater source of data risk for most organizations. Exchange Online provides data loss prevention (DLP) technology that identifies, monitors, and protects sensitive data and helps users understand and manage data risk. For example, DLP proactively identifies sensitive information in an email message, such as social security or credit card numbers, and alerts users via “Policy Tips” before they send that message. Your administrators have a full range of controls and can customize the level of restrictions for their organization. For example, users can simply be warned about sensitive data before sending—sending sensitive data can require authorization, or users can be blocked from sending data completely. DLP features scan both email messages and attachments, and your administrators have access to comprehensive reporting about what data is being sent by whom. Administrators can also apply RMS for content that is triggered by a DLP rule.

Additionally, you may encounter scenarios in which individuals in your organization handle many kinds of sensitive information during a typical day. Document Fingerprinting makes it easier for you to protect this information by identifying standard forms that are used throughout your organization.

This data loss prevention capability is being expanded to other aspects of the service like SharePoint Online in the near future.

Auditing and Retention Policies

By using Office 365 auditing policies, your users can log events, including viewing, editing, and deleting content such as email messages, documents, task lists, issues lists, discussion groups, and calendars. When auditing is enabled as part of an information management policy, administrators can view the audit data and summarize current usage. Administrators can use these reports to determine how information is being used within the organization, manage compliance, and investigate areas of concern.

For business, legal, or regulatory reasons, you may have to retain e-mail messages sent to and from users in your organization, or you may want to remove e-mail that you aren't required to retain. Messaging records management (MRM), the records management technology in Office 365, enables you to control how long to keep items in users' mailboxes and define what action to take on items that have reached a certain age.

MRM in Office 365 is accomplished by using ion tags and retention policies. An overall MRM strategy is based on:

- Assigning *retention policy tags* to default folders, such as the Inbox and Deleted Items.
- Applying *default policy tags* to mailboxes to manage the retention of all untagged items.
- Allowing the user to assign *personal tags* to custom folders and individual items.

Separating MRM functionality from users' Inbox management and filing habits. Users aren't required to file messages in managed folders based on retention requirements. Individual messages can have a different retention tag than the one applied to the folder in which they're located.

eDiscovery

The Office 365 Discovery Center can be delegated to your specialist users—such as a compliance officer or human resources personnel—to conduct eDiscovery tasks without having to generate additional overhead for the IT department. Using eDiscovery, compliance officers can retrieve content from across Exchange Online, SharePoint Online (including OneDrive for Business), and Skype for Business. With the integrated Office 365 eDiscovery, you have one single experience for searching and preserving email, documents, and site mailboxes. You can be specific about what to search for and preserve. The ability to find only what you want and nothing more can contribute to a reduction of discovery costs. The eDiscovery process places no burden on the user for preserving and searching for data, because all of these processes are performed in the background.

Data Spillage Management

Office 365 has compliance features to support you if your organization ever needs to manage data spillage. For example, if a federal government organization were to transmit classified data into Office 365, there are ways for the organization to remove the data by themselves. Compliance and security officials with appropriate RBAC privileges can use eDiscovery to search for the message or document and hard-delete them. The hard drives used to store the spilled data are never re-purposed or repaired or otherwise moved out of the physical security of the Office 365 datacenter. They are destroyed if they are no longer used in the Office 365 infrastructure.

Data Deletion

Customer data privacy is one of our key commitments for the cloud. With Office 365, at contract termination or expiration, we will provide at least 90 days for your administrators to confirm all data

migration has been completed, after which point your data will be destroyed to make it commercially unrecoverable. Further, we provide guidelines to your administrators to personally destroy your data if that is preferred. Electronic discovery can be performed to verify that none of your data can be returned.

Summary

Businesses today need productivity services that help users get more done from virtually anywhere while maintaining security in the face of ever-evolving threats. Office 365 supports both of these needs at once with a highly secure, cloud-based productivity platform. Information regarding Office 365 security, privacy, compliance, transparency, and service continuity can be found in the Office 365 Trust Center and the Service Trust Portal. The Office 365 platform incorporates security at every level, from application development to physical datacenters to end-user access. Today, fewer and fewer organizations have the ability to maintain an equivalent level of security on-premises at a reasonable cost.

Importantly, Office 365 applications include both built-in security features that simplify the process of protecting data and the flexibility for administrators to configure, manage, and integrate security in ways that make sense for their unique business needs. When businesses choose Office 365, they get a partner that truly understands business security needs and is trusted by companies of all sizes across nearly every industry and geography.