SFU OFFICE OF GENERAL COUNSEL AND UNIVERSITY SECRETARY
Archives and Records Management Department

PRIVACY IMPACT ASSESSMENT
For
Azure Active Directory (AD) and Microsoft 365

1. Purpose of the Privacy Impact Assessment (PIA)

This form is used by SFU to determine if a current or proposed policy, system, project, program or activity meets or will meet the protection of privacy requirements under Part 3 of the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA). The Act makes it a legal requirement that SFU conduct a PIA in accordance with the directions of the minister responsible for the Act. The PIA is a compliance and risk management tool used to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly system, program, service, or process redesign; privacy complaints or breaches; and harm to personal, professional and institutional reputation.

See Schedule A for definition of terms.

Archives and Records Management Department use only

Office of primary responsibility	IT Services	**Approved date**
PIA #	2021-001	**OIPC notified date**
Type of PIA	☐ **Department** ☒ **Corporate** ☐ **Update**	**OIPC response date**
Type of PIA review (Check all that apply)	☐ **Policy** ☒ **System** ☒ **Project** ☐ **Program** ☐ **Activity**	
Other applicable PIA provisions (Check all that apply)	☐ **Common or integrated program** ☐ **Data-linking initiative** ☐ **Information sharing agreement**	

2. General Information

2.1. Unit and Program Area

Identify the Department and Program submitting this PIA

Department:	IT Services
Program:	Microsoft 365

2.2. Contact

Identify the individuals best positioned to speak to the contents of this PIA

Name of PIA Drafter:	Stephen MacGregor		
Position Title:	Information Compliance Architect		
Phone:	22319	E-Mail:	smacgreg@sfu.ca
Name of Program Manager:	Eric Leung		
Position Title:	Service Owner, Microsoft 365		
Phone:	604-725-2581	E-Mail:	eleung@sfu.ca

2.3. Description of the Current or Proposed Policy, System, Project or Program

Provide as background a general description of the initiative and the context in which it functions. This could include the purpose of the initiative and its benefits, what larger process it is part of, how it functions, how it integrates with or consolidates other information systems, how it aggregates and stores together information that was previously maintained separately, how it converges different record keeping systems, the parties involved, how it will automate or otherwise change the existing business workflow, etc. Describe in the sections immediately following the background (if applicable) specific details with respect to the individual actors involved in the business process, focusing on how their personal information will be collected, accessed, used, disclosed and retained.

Include copies of documentation (if it exists) that describe the business requirements, functional analysis, conceptual overview, etc. that helps explain the initiative.

2.3.1. Background

SFU's Microsoft 365 (M365) Program aims to deliver an enterprise, cross-departmental collaboration platform, powered by Microsoft 365, that aligns with the University's journey towards unified communications. In October 2021, SFU will be launching M365 for all SFU users with an SFU Computing ID (faculty, staff, students, sponsored accounts, retirees). M365 has already seen widespread adoption by the post-secondary sector in British Columbia. Simon Fraser University's implementation aligns with its sister institutions within the province.

The focus of this document will be on the following services:

Microsoft Azure Active Directory
Cloud-based; data is hosted globally

SFU has managed an on-premise Active Directory (AD) service for many years, and all SFU Computing Accounts have a corresponding on-premise AD user account. However, SFU users who wish to use Microsoft 365 products will need have an Azure Active Directory (AAD) account created and populated with data from the on-premise AD service using one-way synchronization tools administered by SFU IT Services. Azure Active Directory (AAD) is Microsoft's cloud-based identity and access management service, where data is hosted globally.

Microsoft 365 Products
Cloud-based; all data is hosted exclusively in Microsoft's Canadian servers

Microsoft 365 is the name for Software as a Service ("SaaS") subscription plans that include access to Microsoft Office applications plus other productivity services. These connected services are hosted in Microsoft data centres and enabled over the Internet, colloquially referred to as "cloud" services. Microsoft Canada's cloud services provide an opportunity for modernization, increased agility, and robust information security and privacy practices, all while lowering the overall cost and complexity of delivered information technology services.

Teams is described as a chat-based workspace in Microsoft 365. Teams is a graphical-user interface that integrates many of Microsoft's already existing Microsoft 365 products into one application. Conceptually, Teams is an interface that lays on top of other Microsoft Services (OneDrive, SharePoint, etc.). Teams can be accessed either through the Teams client (installed on workstations or mobile devices) or via web browser. The basic premise of Teams is to provide users with the capability to communicate privately, as well as publicly in groups or "teams", while being able to facilitate document exchange and collaboration on projects. This can be done for internal as well as external parties who also use Microsoft 365, to facilitate secure document exchanges. SharePoint Online provides the back-end document management capabilities available in Teams.

SharePoint Online is a cloud-based service that helps organizations share and manage content, knowledge, and applications to:

- Empower teamwork
- Quickly find information
- Seamlessly collaborate across the organization

OneDrive is a file hosting service that will allow clients to sync and store files from their desktop to their own personal cloud-based client, which is accessible via web-browser and mobile devices. OneDrive is intended as one of the long-term replacement services for SFU Vault, particularly for individual file storage needs.

Generally, SharePoint and OneDrive share many similar features, However, *SharePoint Online* is intended for use in a corporate or group setting, and *OneDrive* is intended for use by an individual to store their own content.

Teams, SharePoint Online, and OneDrive enable the usage of Microsoft Office applications (e.g., Word, Excel, PowerPoint, OneNote) via web browser and desktop integration for real-time collaboration.

It should be noted that the product names "Office 365" and "Microsoft 365" are often used interchangeably. For the purposes of this PIA, "Microsoft 365" will be used; however, "Office 365"

generally refers to the same artifacts in scope for this PIA. “Office 365” properly refers to specific productivity and collaboration apps available on desktops, mobile devices and in the cloud. “Microsoft 365” includes “Office 365”, with additional features covering a wider range of services, such as security tools, the Windows 10 operating systems, and more.

2.3.2. Personal Information

Collection: The following personal information is collected

Microsoft Azure (Azure Active Directory) :

- Last Name
- First Name
- Email address (SFU Computing ID)
- **Date and time of sign-ins** to elements of the M365 suite
  - Date and time of sign-in to M365 portal
  - Date and time of sign-in to M365 web-based applications (interactive, requiring active login with user credentials)
  - Date and time of sign-in for M365 desktop applications such as Teams that require a connection to the organization (non-interactive where the user initially logs into the application and then the application starts in future instances without the user actively entering credentials. For example, starting Teams would be indicated);
- **IP address** from which a sign-in was performed
  - From this, a derived location scoped to a municipality (eg. Port Coquitlam, but not an address)
- **Membership in Microsoft 365 groups** (e.g., member of a Teams team called "SFU Teams - Enterprise IT")
- **Description of devices** used by the person accessing M365 (computers, mobile devices)
- **Audit logs** (changes made to any resources within Azure AD like adding or removing users, apps, groups, roles and policies: this would generally be a record of actions taken by an M365 administrator, not a typical user of M365 applications)
- Optionally (only if set in SFU’s locally hosted Active Directory):
  - Image/avatar
  - Job Title
  - Company Name
  - Department
  - Manager
  - Business Address
  - Office Phone Number
  - Mobile Phone Number

- Online presence, i.e., a user-settable representation of their availability for collaboration. Examples are: available, busy, do not disturb, away, and offline.

Microsoft 365 Teams:

- Documents and files (file content may contain personal information about current, prior, and future staff, students, and faculty, and is excluded from review in this PIA).
- Opinions (chat content)

Microsoft 365 OneDrive:

- Documents and files (file content may contain personal information about current, prior, and future staff, students, and faculty, for business/academic purposes).

Microsoft 365 SharePoint Online:

- Documents, files and list data (content may contain personal information about current, prior, and future staff, students, and faculty, for business/academic purposes).

Access: The data may be accessed by authorized members of SFU faculty, staff and students.

Access control to Microsoft 365 content is hierarchical in nature and can be very granular. Users may be granted access at many levels. Content is generally organized into a parent-child information architecture, and permissions are assigned at higher levels with descending propagation. User access is typically controlled through group and role-based membership which simplifies management of changes over time. People's eligibility/ability to use the software is managed in general by applying rules such as "current staff members may access the applications in one configuration, and people with a student role are assigned a different set of rights." Individual licenses to use a given service or application in the M365 suite is managed by assigning a license to use a piece of software based on the person's role or group membership. Role changes in the SFU identity system will trigger changes in the license(s) provided to a given account as the account owner transitions between roles at the University (e.g., from student, to staff member, to retiree).

Access to content may be explicitly granted to external users (i.e., non-SFU users who do not have a staff/faculty/student/retiree SFU Computing ID). External users accessing content "shared" with them by SFU users will need to log in using a valid Microsoft account. Business contact information for SFU faculty and staff is available to all SFU Microsoft 365 users.

Access to any content in SFU's Microsoft 365 content must be by an authenticated member of the SFU organization via the SSO integration or, where content is shared to an external user, an account that has been verified by Microsoft authentication services.

Use: The data will be used for the following purposes:

Microsoft 365 Technical Operations

- Creation of user account in Azure Active Directory.

- Synchronization of account information, including passwords, between SFU Active Directory and Azure Active Directory.
- Authentication of SFU faculty, staff, and students accessing Microsoft 365 services.

Microsoft 365 Functional Operations:

- Creation and authoring of Office documents.
- Collaboration between SFU faculty, staff, students, and authenticated external users of Microsoft 365 using documents/files.
- Online meetings (chat, optionally streaming video, optionally streaming audio) held between SFU faculty, staff, students, and authenticated external users of Microsoft 365.
- Messaging communication (chat) between SFU faculty, staff, students, and authenticated external users of Microsoft 365.

Disclosure: Information about SFU Microsoft 365 users and content may be disclosed to

- SFU Enterprise IT and Local IT staff members providing operational support of the service.
- Microsoft support staff on a per-case basis where permission has been explicitly granted by the owners of the data concerned.
- Users and account owners (only their own information).

For SFU employees, the University is relying on the exclusion of business contact information from the FIPPA definition of personal information. Business contact information is defined as *information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual*. The question is whether this definition is broad enough to encompass the usage data described above. Some of the usage data is business contact information (unique id, IP address and geolocation) while the remainder is addressed by Microsoft's Terms of Service and its certification against ISO 27018 (an international security standard). Microsoft is the first major cloud provider to be independently verified as complying with ISO 27018. These Terms of Service and the ISO standard state Microsoft will not disclose a customer's data outside of Microsoft except in limited and defined circumstances. Therefore, FIPPA s. 33.1(1)(p.2)(vi) may apply and permit the out of Canada disclosure.

Retention: Multiple departments and faculties are expected to use Microsoft 365. Customer Content will be retained and disposed in accordance with governing RRSDAs for the department or faculty owning that data. In the event that conflicting opinions about applicable RRSDAs arise, the Archives and Records Management Department will provide guidance about proper record disposition.

2.4. Scope of this PIA

Explain exactly what the PIA covers and conversely what it does not.

The scope for this PIA is for SFU's implementation of the following components of Microsoft 365, a software-as-a-service cloud platform:

- OneDrive – supports personal file and document storage from a user's desktop, mobile device, and the web.
- Teams – tool that enables users to actively connect and collaborate in real time on documents, files and shared apps.
- SharePoint Online – collaboration platform allowing an enterprise to store, retrieve, search, archive, track, manage, and report on digitized documents and other content.
- The administration of Microsoft 365 by administrators at SFU in the SFU Microsoft 365 tenant. A tenant is the instance of M365 to which SFU controls access as an organization and governs usage of the tools within its organizational scope at a technical level (e.g., by assigning licenses to certain groups), or driven by SFU policy (e.g., data retention practices).
- The access, storage, retention, and management of SFU users' personal information by Microsoft as part of providing services required by Microsoft 365.
- The integration between Microsoft Active Directory used on premise by SFU and Azure Active Directory.
- Microsoft 365 "Apps" that are wholly supported and/or developed by Microsoft for use within the Microsoft 365 platform.

This PIA does not cover:

- The content or use of the *content* of files created, stored, or shared by users via Microsoft 365 products.
- Existing on-premise implementations of Microsoft Office products and services such as Exchange 2016 and SharePoint.
- The independent implementation and/or use of any other Microsoft services by students, faculty, or staff.
- Physical security and other controls associated with devices used to access services.
- Integration of Microsoft 365 and related Microsoft Azure services with other third-party applications or services.
- Microsoft 365 "Apps" available to users that are not supported and/or developed by Microsoft.
- Management of devices using Microsoft Azure.
- Exchange Online
- Any new MS products to be implemented in the future will require either a new PIA or amendments to this PIA.

2.5. Related PIAs

Identify PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative.

No current related PIAs exist; however, future PIAs and/or amendments will be developed as SFU increases the scope of Microsoft 365 usage.

2.6. Elements of Information or Data

List the types of personal information involved in the initiative (if applicable). This could include the individual's name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments, or opinions about third parties. See Schedule A for a partial list of types of personal information.

2.6.1. Data Elements

Microsoft will have custody of three basic categories of data, defined as follows:

a) **Service or System Data**
System or Service Data is data about, and generated by, an information system or cloud service. Typical examples of service data include remaining storage capacity, system health indicators, network traffic volume, and bandwidth consumption, all of which are examined or used solely for the purpose of providing the cloud service.
   i. System data is generally not personal information, but can contain usernames, and is distinct from user generated content. System data is used solely for the purpose of providing, operating and maintaining the service, or diagnosing and/or troubleshooting in the event of problems or system outages.
   ii. This data is accessed by authenticated Microsoft system administrators, service technicians and operators with the appropriate and minimized levels of access. As a rule, technicians are granted just-in-time[1] minimum privileges necessary to troubleshoot the system on an exceptional basis, and only for a fixed period of time. Upon completion of any maintenance task, administrative privileges and access to service data are revoked, and all associated data around these activities are logged. SFU is notified when this kind of access is required or occurs.
   iii. System Data for Teams, OneDrive, and SharePoint Online is stored at rest inside Canada.

b) **Account Data** Account Data is basic information used to identify and differentiate users within the cloud service. Examples include Name, User ID, Organizational ID and basic user contact information such as email address. This information may be accessed by Microsoft staff in specific cases where SFU IT Service desk or SFU escalated support staff are unable to resolve an access issue. Microsoft is never provided with a user's password.

   Account Data for SFU employees, when used for the purpose of authenticating, identifying, differentiating, and otherwise contacting employees using Microsoft 365 in the course of their employment is being used to facilitate contact with and between

these employees at their place of business. It is therefore "contact information" and not "personal information" as defined by Schedule 1 of FIPPA.

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

Account Data for Microsoft 365 is stored internationally in the Azure Active Directory (AAD) cloud service for identity and access management. It should be noted that Azure Active Directory data is stored internationally because of the replication requirements in place to facility access to Microsoft 365 across a broad range of locales. This is a business choice made by Microsoft.

Account Data is also aggregated with system logging and analyzed as part of "Usage Data". Usage Data is used to provide information about service usage and licensing. Microsoft 365 includes a feature called a "Productivity Score", which provides an arbitrary productivity rating based on analysis of usage data and may be aggregated based on several factors including (but not limited to) departments, groups, locations, roles and individuals. SFU does not have the Productivity Score feature enabled, and usage data is anonymized.

c) Customer Content

Customer (in this case, SFU) content consists of data, information (including personal information of staff, students, alumni, and faculty), documents, spreadsheets and other artifacts that are authored, edited, communicated, maintained and eventually disposed of by SFU users.

i. Content is considered sensitive in nature and is likely to include personal information. In Microsoft Cloud Services, customers control their own content data. Microsoft's role is limited to that of data processor, a position that is further reinforced in the Microsoft Online Privacy Statement and their security audits, third party attestations and certifications.
ii. Specific content will range in type, volume and sensitivity according to the SFU users that are making use of Microsoft Cloud Services.
iii. Customer content is not accessible or visible to Microsoft administrators, except in non-routine maintenance scenarios. In these cases, Microsoft, with explicit consent from SFU, would be able to investigate and/or fix an ongoing problem with a cloud service.
iv. Customer Content for Teams, OneDrive and SharePoint Online is stored at rest inside Canada and includes:
    i. Teams: Files, chat (opinions), history
    ii. OneDrive: Files
    iii. SharePoint Online: Files, wiki, blogs, lists
v. Customer Content may be temporarily processed outside of Canada for automated analytical services such as spell check, translation, meeting transcription, and text analysis, but results are stored at rest in Canada.

All customer content is owned by a designated individual or group, which in turn has designated individuals as owners. SFU users/owners control their user-created content and the content which they receive from others, including the deletion of such content, and adherence to SFU data retention guidelines. By default, all customer content is

private to the individual or group to which it belongs, unless it is explicitly shared by the individual or a group member. Group owners are notified when group content is shared by members.

d) Other data considerations

The Azure platform records additional information about users, including user metadata (IP Address, browser, operating system). This information is used by SFU Microsoft 365 administrators for security purposes and troubleshooting. The information may be disclosed to Microsoft support on a case-by-case basis.

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 Azure AAD.

2.7. Storage or Access outside Canada

Provide a brief description of whether the personal information can be accessed from outside Canada. For example, by a service provider that is repairing a system, or if the information is being stored outside Canada, for example, in the "cloud"'. If the data is stored within Canada and accessible only within Canada, please indicate this and describe with whom and where it is stored.

With respect to storage and access of data, each of the three basic categories of data (System or Service Data, Employee Contact Data and Customer Content) in Microsoft Cloud Services are treated individually as follows:

System or Service Data comes from the ongoing operation of Microsoft 365 and Microsoft Azure cloud services. System data, which does not contain personal information, is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. All service and maintenance data are accessed and contained within Microsoft's global, private network. System or Service Data for SFU's instances of Teams, OneDrive, and SharePoint Online is stored at rest in Microsoft's Canadian facilities located in Toronto (primary Microsoft Data centre for SFU) and Québec City (secondary Data centre).

Account Data in Microsoft Cloud Services will be stored in Microsoft Azure Active Directory. All replication of such data around the globe happens within Microsoft's global, private network. Account Data for SFU instances of Teams, OneDrive, and SharePoint Online is stored in the AAD in North America, but outside of Canada.

Data from SFU's on premises Active Directory (AD) domain synchronizes with Azure AD upon account creation and thereafter approximately every 30 minutes; there are also push triggers that may be activated. Azure AD is a component of the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Microsoft Cloud Service and is included here because it is used to provide identity and access management services for Microsoft 365. It combines core directory services, advanced identity governance, and security and application access management. All replication of Azure AD data around the globe happens within Microsoft's secure global, private network. The information is not disclosed to the public or to other Microsoft customers, rather it remains accessible only to the

authorized users in the same customer tenant. The elements of the AD that would sync to Azure AD are limited to data that is considered business contact information for employees but would be considered personal information for students. Azure AD attributes are listed in Appendix A.

Once authenticated, data transactions occur directly between the user and Microsoft. The important differences between how SFU currently manages the Microsoft services and features on campus versus Microsoft 365 in the cloud is that user data will be stored (at rest) on Microsoft's servers, as opposed to SFU servers.

SFU has provided an option to students to mask their identity by anonymizing their user name and email account (usually in the form of a combination of initials and numbers (e.g., JED587@sfu.ca) so that their first and last names are not visible in the directory. SFU also has included a notice in its Academic Calendar about the use of M365 and the need to store minimal account data globally. Students are also presented a consent form before downloading M365 products.

Customer Content for SFU instances of Teams, OneDrive, and SharePoint Online, which is likely to contain personal information, is encrypted at rest and stored in Microsoft's Canadian facilities located in Toronto (primary Microsoft Data centre for SFU) and Québec City (secondary Data centre). These facilities are designed to run 24x7x365 and employ a variety of measures to minimize the possibility of power failures, physical intrusions and network outages. Data is replicated three times within the primary Data centre, with a fourth copy retained in the secondary Data centre. Under exceptional or catastrophic conditions to a broad geo-location, Microsoft may, with SFU consent, effect temporary movement to another data centre location to ensure customer services and data are not lost.

Data transmitted to users from Microsoft 365, or between users within the Microsoft 365 platform is encrypted using TLS (or mTLS or SRTP in the case of certain MS Teams data).

Data transmitted between the Microsoft 365 Canadian data centre and SFU campuses will generally be routed through the CANARIE backbone.

Access to SFU Microsoft 365 will be generally done from within Canada, where the majority of staff, students and faculty are located, and access from within Canada will be encouraged; however, Microsoft 365 will also be accessed from outside of Canada by traveling users.

Assurances from Microsoft that SFU data is stored within Canada (with the exception of the data in AAD)

SFU's discussions with Microsoft representatives clearly indicated that customer content would be stored in Canada. Microsoft's Online Services Terms (https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all) state that Microsoft will store customer data at rest within Canada for files uploaded to OneDrive. In addition, assurances from Microsoft websites (https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?ms.officeurl=datamaps&view=o365-worldwide#canada) state customer content for Teams will be located in Canada.

Another means for SFU to ensure compliance is accomplished through technical settings such as the configuration controls. The selection of tenanting of online services within a specific geographic

region is achieved through configuration controls. It is not certain at this stage that there is a process in place at SFU to ensure the correct tenanting is selected and that there is periodic review to ensure there have not been unauthorized changes in the configuration.

Microsoft Technical Support

As a global organization offering an extremely broad range of services, Microsoft Technical Support includes an extraordinarily broad range of help channels that a customer may pursue. For example, if a customer is experiencing problems with SharePoint Online, they may be directed by the SFU Help Desk to engage with a specific Microsoft support desk, and, if the same customer experiences problems with Microsoft Teams, they may be routed to a completely different Microsoft support desk in another location, in another country, permitted under FIPPA 33.1 (1)(p)(i)(a). Microsoft support desks, and escalated Microsoft support, may not be based in a specific, fixed location.

For the support purposes, data may be disclosed to Microsoft Technical Support personnel. Disclosure happens on a case-by-case basis and is monitored by SFU administrators.

2.8. Data-linking Initiative

In FIPPA, "data linking" and a "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. If so, you must comply with requirements under the Act for a data-linking initiative.	
1. Personal information from one database is linked or combined with personal information from another database	☒ **Yes** ☐ **No**
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled	☐ **Yes** ☒ **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	☐ **Yes** ☒ **No**
If you answered "yes" to all three questions, please contact the Information and Privacy Coordinator or Officer to discuss the requirements of a data-linking initiative.	

2.9. 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 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** ☐ **No**
2. Those services are provided through: 1) a public body and at least one other public body or agency working collaboratively to provide that service; or 2) one public body working on behalf of one or more	☐ **Yes** ☒ **No**

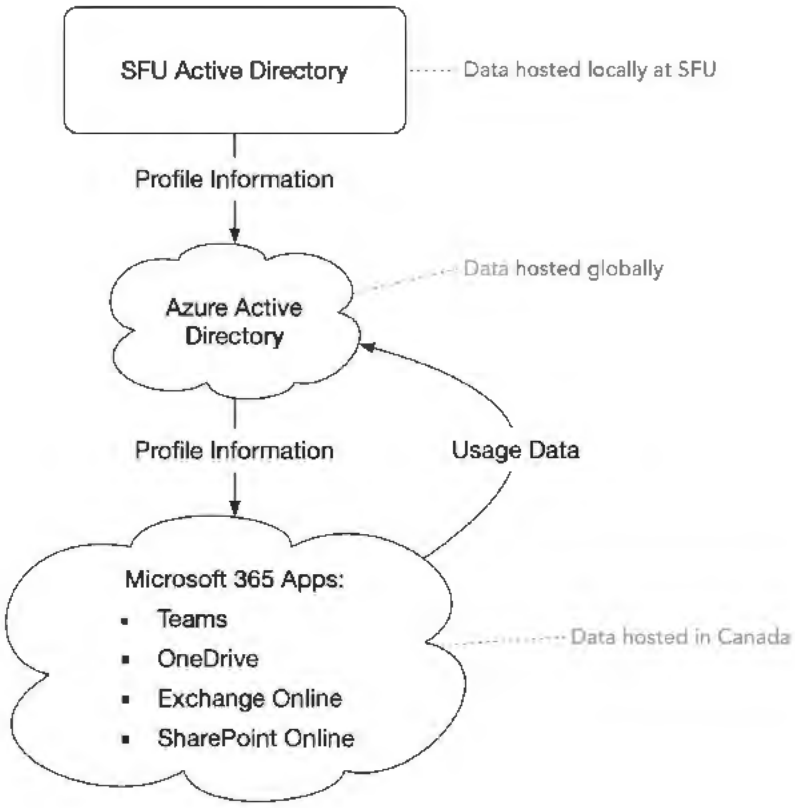
other public bodies or agencies	
3. The common or integrated program or activity is confirmed by a written agreement that meets the requirements set out in section 12 of the FIPPA Regulation (link to the Regulation and read section 12)	☐ Yes ☒ No
If you answered "yes" to all three questions, please contact the Information and Privacy Coordinator or Officer to discuss the requirements of a common or integrated program or activity.	

3. Collection, Use and Disclosure of Personal Information

3.1. Personal Information Flow Diagram / Table

Complete the table(s) below (if applicable). Include a personal data flow diagram (if one exists) as well as completing the table(s). See Schedule B for a list of the privacy rules. Use the hyperlink to the Act in Schedule B to identify the specific rule and cite the appropriate section number in the "Legal Authority" column.

3.1.1. Data Flow



Personal Information Flow Table – Typical Use Cases			
	Description/Purpose	**Type**	**Authority**

1.	Account data for SFU users (name, sfu.ca email address, and SFU affiliation) is disclosed to Azure Active Directory through automated integration on a recurring period.	Collection, Disclosure and storage outside Canada	30.1 (b) 33.1(1)(b)
2.	System or service data is stored on Microsoft servers inside Canada.	Disclosure	33.2(a)/(c)
3.	Customer Content is processed by Microsoft outside of Canada to enable features of Microsoft 365 (e.g. spell check) without being stored.	Disclosure outside of Canada	33.1(1)(p.1)
4.	Customer Content stored in Microsoft Canadian data centre	Disclosure	33.2(a)/(c)
5.	Site or Teams owner searches for and adds other users to their site. Users are visible to other users of that site.	Collection, Disclosure	26(c), 33.2(a)/(c)
6.	Sites/Teams are used by members to share information and collaborate on work related projects and initiatives.	Disclosure	33.2(a)/(c)
7.	Microsoft administrators may monitor sessions, at SFU's request, to install, implement, maintain, repair, troubleshoot or upgrade the system. No session data is recorded or stored.	Disclosure outside of Canada	33.1(1)(p)

3.2. Risk Mitigation Table

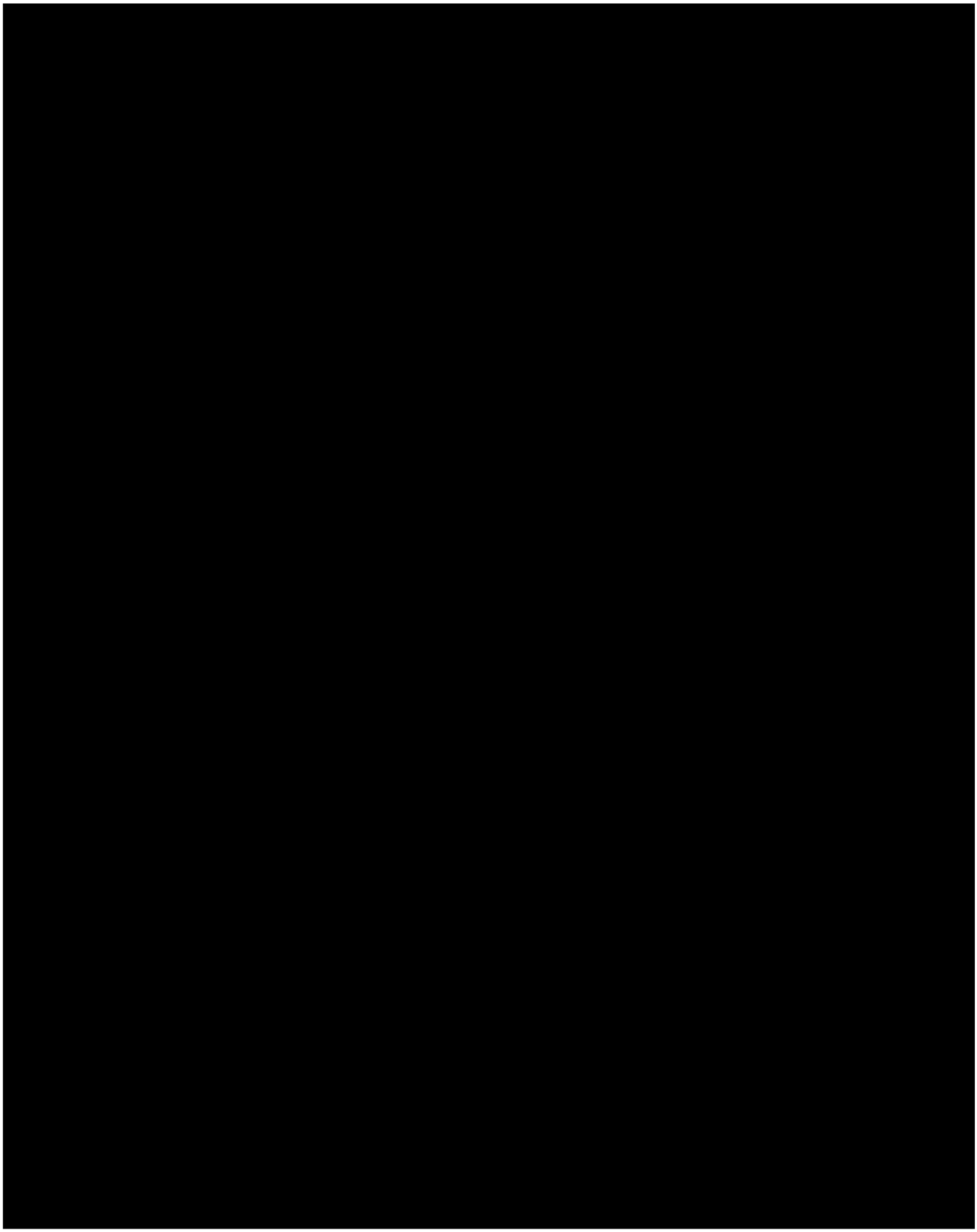
Complete the table(s) below. Describe the risk and the mitigation strategy. Use the terms "High", "Medium" or "Low" to rate the "Likelihood" and "Impact" of each risk. In cases where the risks are substantially different for the individuals whose personal information is

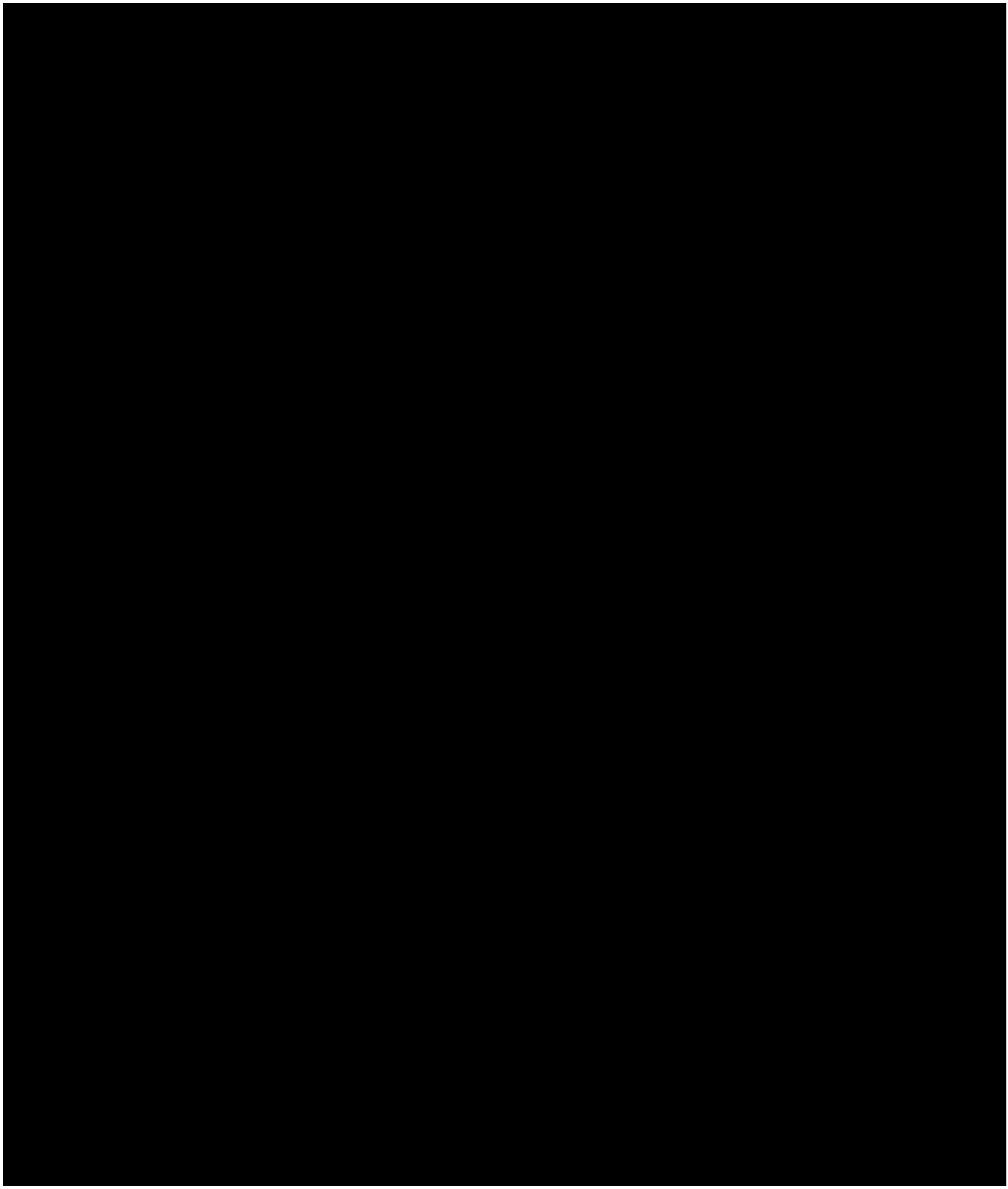
in SFU's custody or under its control, complete a table for each group. In cases where the risks are substantially similar or the same, complete only one table.

3.2.1. Risks to Data

Risk Mitigation Table

[redacted]





3.3. Collection Notice/Consent

In order to allow individuals the ability to exercise their information rights with knowledge of how their information will be used, they must be notified at or prior to the time of collection. Section 27(2) of the Act requires that the individual from whom personal information is collected be told: a) the purpose for collecting it, b) the legal authority for collecting it, and c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Describe below how and when notice will be given to individuals. Include the specific collection notice(s) that will be used. Link to SFU's collection notice templates.

3.3.1. Collection Notice

The only personal information that is stored outside of Canada when using M365 is Account Data of non-employees, primarily students and usage data. In SFU's implementation of M365 this personal information will be comprised of **name, email address, and affiliation (e.g. department)** which will be disclosed to Microsoft in Azure AD. As noted above, Azure AD is stored outside of Canada within Microsoft's global private network. In order to authorize the disclosure of this limited personal information SFU will require consent from non-employee users of M365. This consent will be collected from all users when they first register for an M365 account, by presenting such users with the following consent notice and requiring them to consent in order to proceed with registering their account:

Privacy Notice

As an SFU student you are eligible for access to Microsoft 365 services. The following notice applies to all Microsoft 365 services offered by SFU.

Microsoft 365 is a cloud-based service that includes communication and collaboration tools such as persistent chat, file storage, video conferencing capabilities, productivity apps and much more.

All user-created content (files, messages and site content) related to Microsoft 365 services is stored in Canada. However, some information about your account may be stored outside Canada in Microsoft's global network - specifically your name, SFU computing ID, SFU email address, SFU affiliation, and device information. Microsoft employees and subcontractors will have access to this information for the purposes of operating the service. Complete information on Microsoft's use, protection, and access to personal data can be found on their website: https://privacy.microsoft.com/en-ca

Users logged into SFU's Microsoft 365 service will be able to search for and collaborate with you using your SFU email address. Other users will be able to see your name, SFU computing ID, and SFU email address. If you wish to anonymize your identity, please click on "XXX" before activating your Microsoft 365 account.
By using the Service, your information is made available to SFU service administrators who are located in Canada and Microsoft service administrators who are located worldwide for the purpose of support and system administration.

For further information about this notice, please contact XXX.
I HAVE READ AND UNDERSTOOD THE ABOVE INFORMATION

In addition, the following notice will be added to the University's Academic Calendar:

Microsoft 365: Disclosure of student contact information advisory

As an SFU student you are eligible for access to Microsoft 365 services. The following notice applies to all Microsoft 365 services offered by SFU.

Microsoft 365 is a cloud-based service that includes communication and collaboration tools such as persistent chat, file storage, video conferencing capabilities, productivity apps and much more.

Disclosure of personal information to vendors, systems or services storing or accessing that information outside of Canada without consent is restricted by s. 30.1 of FIPPA. Students are required to consent to the disclosure of student contact information for the purpose of enabling the student to access and be contacted on an electronic system. "Student contact information" may include your name, SFU computing ID, SFU email address, SFU affiliation, and device information, if used solely for the purpose of providing access to or use of an electronic system. Registration at SFU means you give your consent for the University to disclose your student contact information to Microsoft as a SFU service provider. Specific notice will be given when you sign up for a Microsoft 365 service through SFU.

All user-created content (files, messages and site content) related to Microsoft 365 services is stored in Canada. However, your student contact information may be stored outside Canada in Microsoft's global network. Microsoft employees and subcontractors will have access to this information for the purposes of operating the service. Complete information on Microsoft's use, protection, and access to personal data can be found on their website: https://privacy.microsoft.com/en-ca

Users logged into SFU's Microsoft 365 service will be able to search for and collaborate with you using your SFU email address. Other users will be able to see your name, SFU computing ID, and SFU email address.

If you wish to anonymize your identity, please click on "XXX" before activating your Microsoft 365 account.

By using the Service, your information is made available to SFU service administrators who are located in Canada and Microsoft service administrators who are located worldwide for the purpose of support and system administration.

For further information about this notice, please contact XXX.

4. Security of Personal Information

Describe below the specific measures that will be used to protect the personal information from unauthorized collection, access, use, disclosure, retention and disposal. See Schedule C for a list of common types of security measures.

4.1. Physical Security Measures

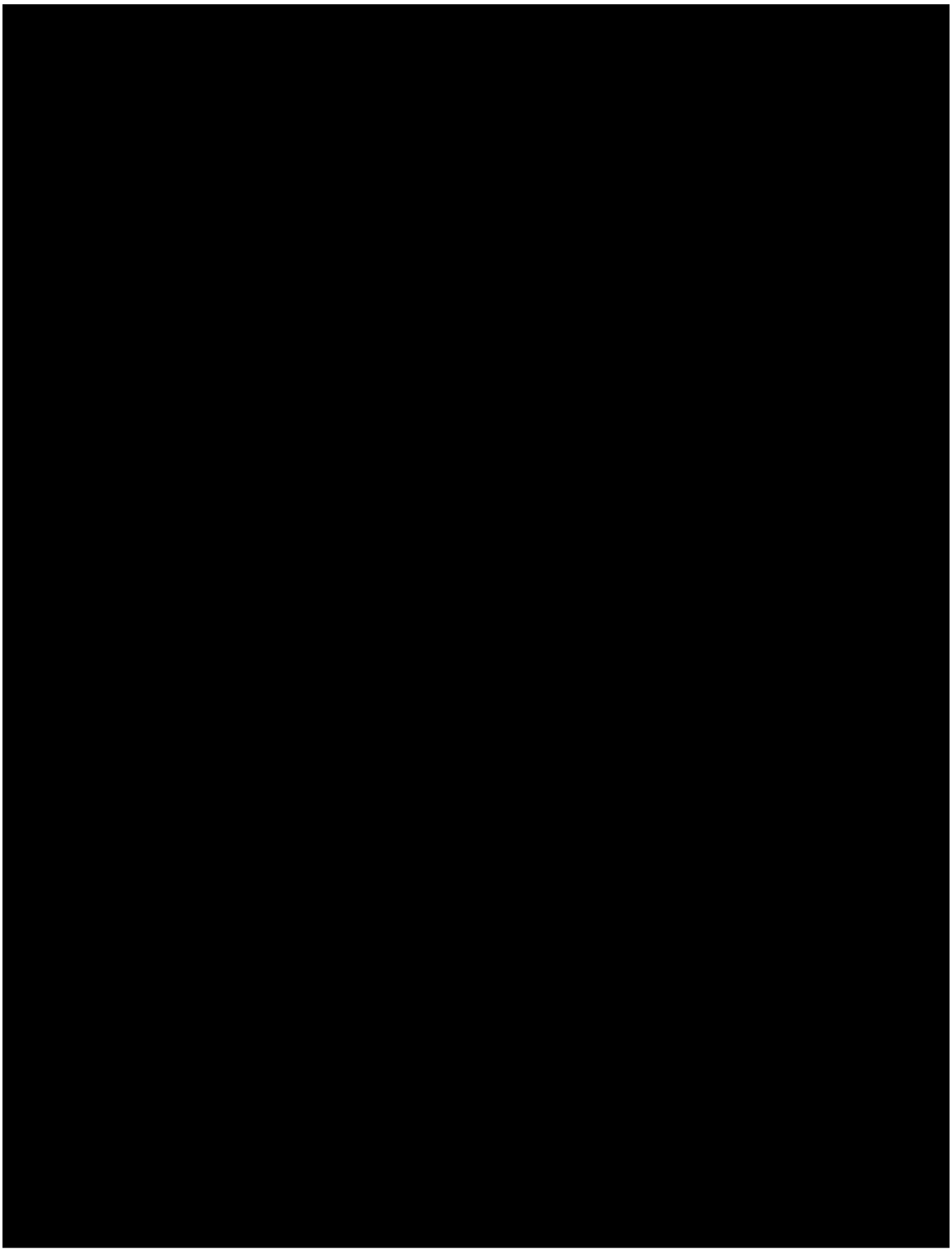
[redacted]

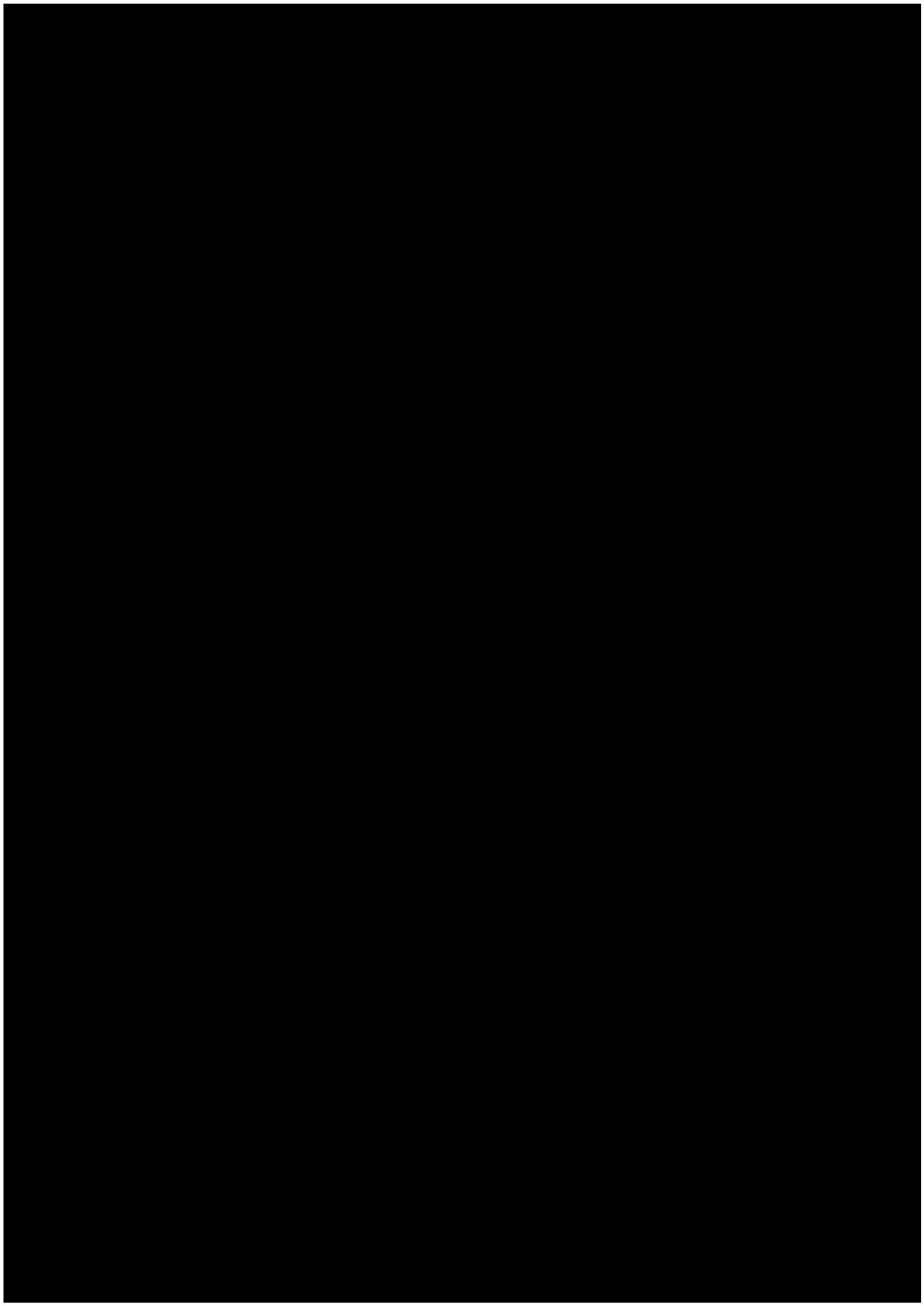
4.2. Technical Security Measures

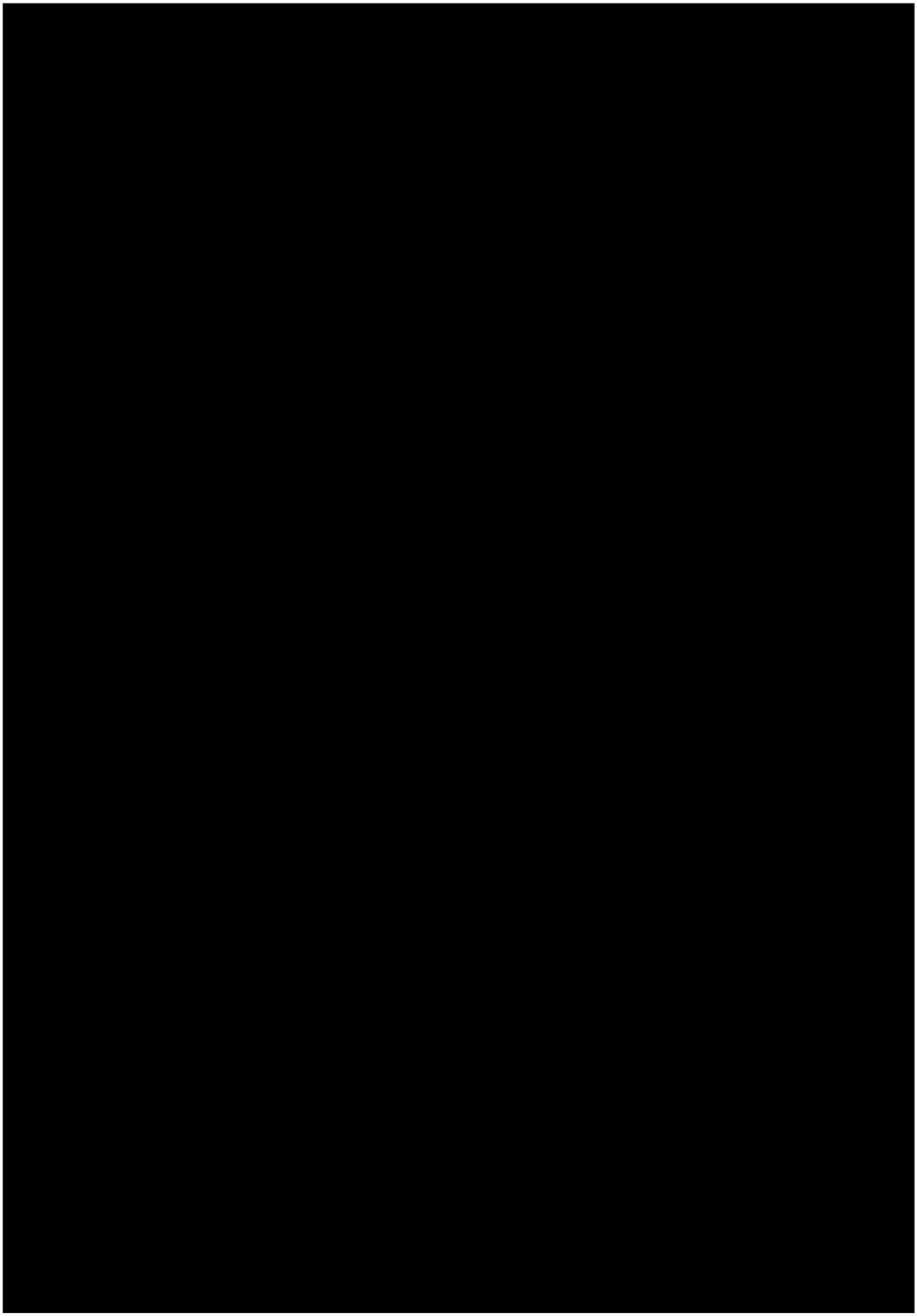
[redacted]

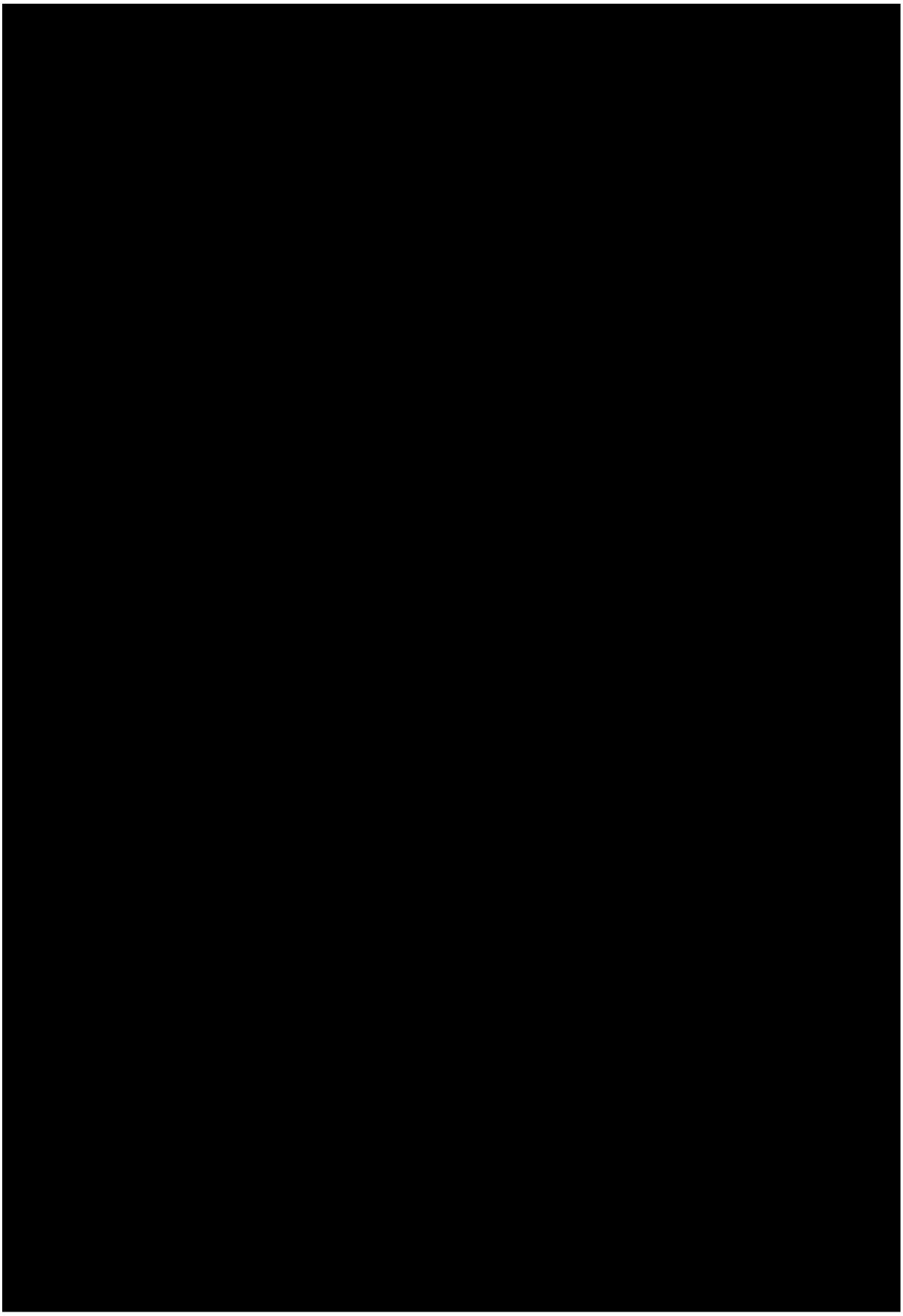
[redacted]

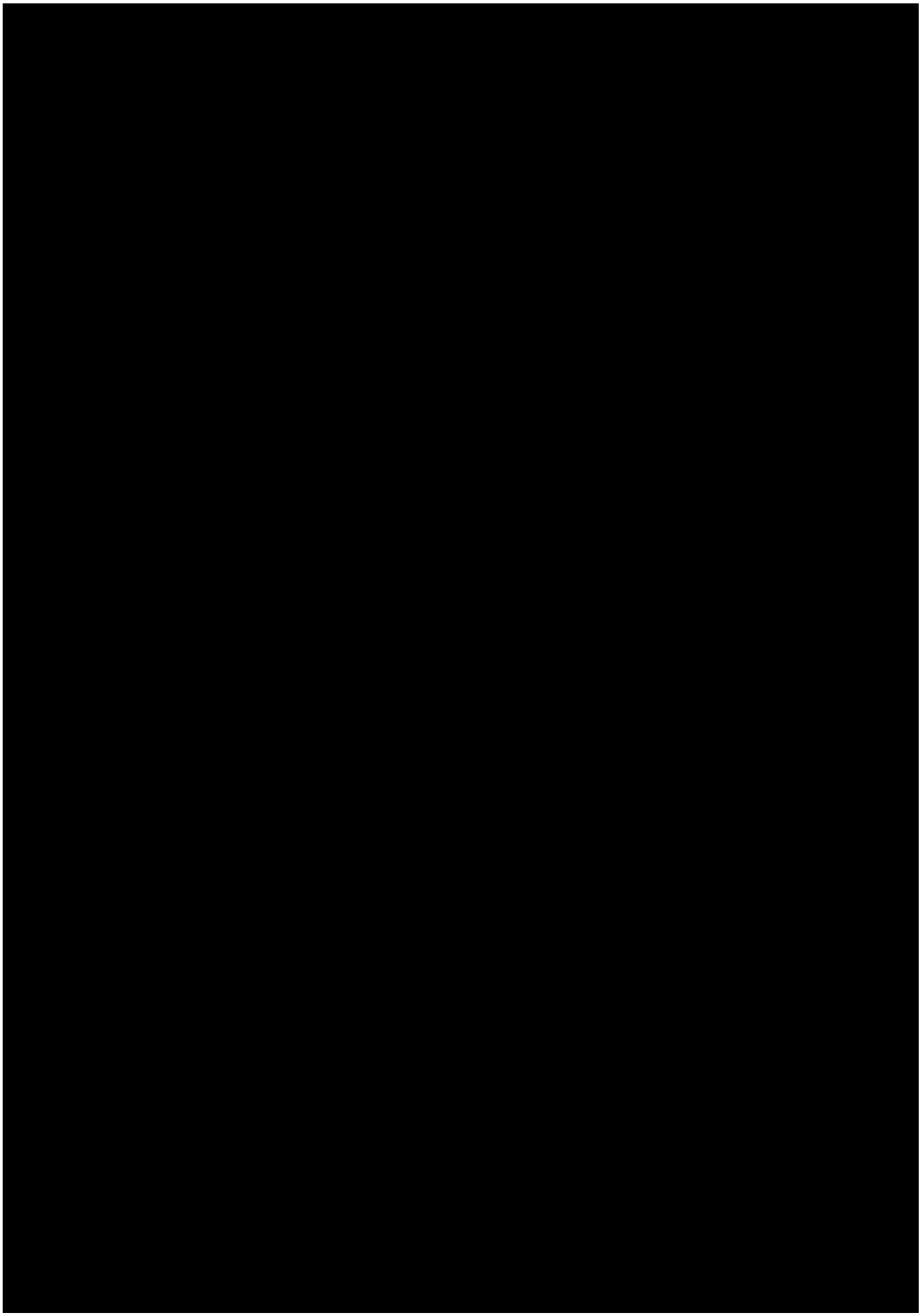
Data Privacy
[redacted]

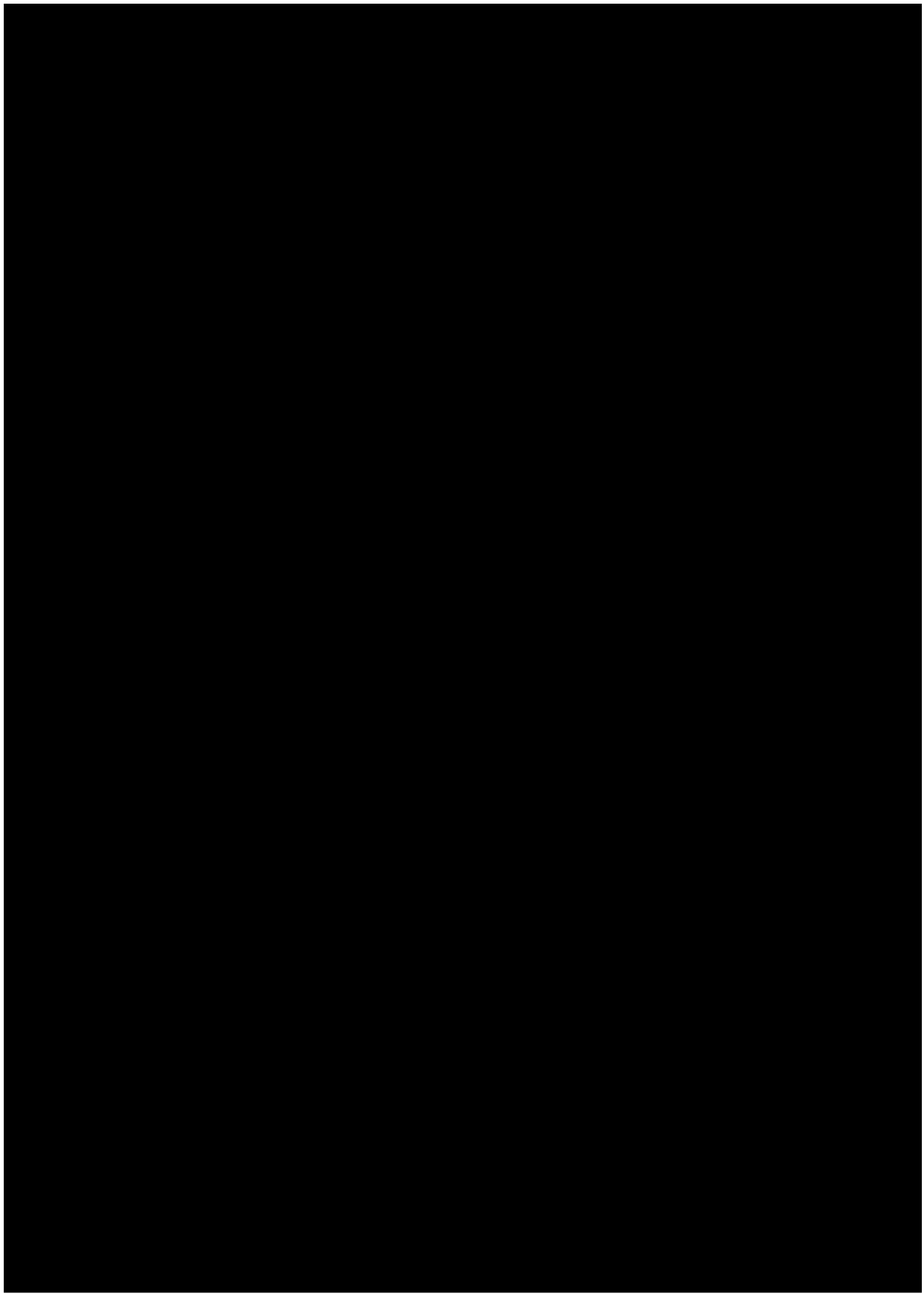


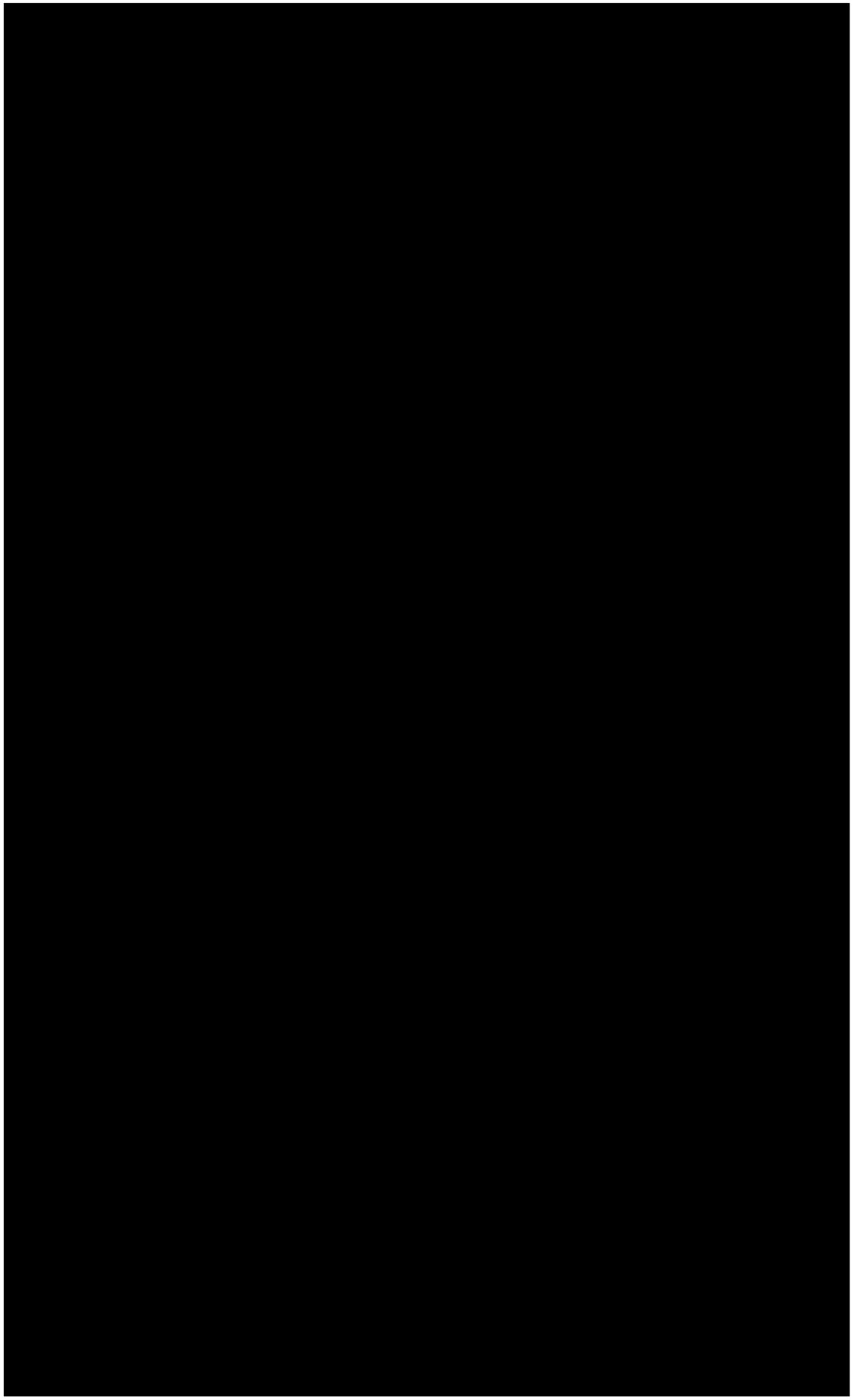












[redacted]

4.3. Security Policies, Procedures and Standards

Overall usage of Microsoft 365 by SFU staff, faculty and students is governed by the SFU Fair Use of Information and Communication policy (GP 24)
https://www.sfu.ca/policies/gazette/general/gp24.html

Specific functional use cases and configuration settings are defined in the Microsoft 365 governance documentation created by SFU, based on contributions from a broad range of SFU stakeholders.

4.4. Tracking Access / Access Controls

Describe the controls used to track access by authorized users of the personal information.

[redacted]

4.5. Information Classification Standard

(Note: this standard is under development – please leave this section blank). Using Information Technology Services' standard for classifying the sensitivity, access

restrictions and minimum-security requirements for information, identify the specific classification level that applies to this initiative.

[redacted]

5. Accuracy, Correction and Retention of Personal Information

5.1. Updating and Correcting Personal Information

Describe here (if applicable) the procedure to allow individuals to routinely update or correct their personal information using regular channels (e.g., a student uses the SIS to update a home address or telephone number, an employee uses the HAP system to update emergency contact information, etc.).

In the absence of a routine process, this requirement would default to SFU's formal procedure Requesting a Correction to Personal Information in University Records.

Account information in Microsoft 365 is based on information in the on-premise Active Directory managed by SFU. This directory is, in turn, populated upstream from several SFU identity management systems working in concert.

To correct personal information, constituents may contact IT Services, Human Resources, Alumni Relations, or Student Services, depending on their role within the university.

5.2. Decisions That Directly Affect an Individual

Describe here (if applicable) how the information will be used to make decisions that directly affect an individual.

Because Microsoft 365 is expected to be a widely used collaboration and communications workspace, it is likely that Customer Content may be used to make decisions about individuals.

Given the functions that Microsoft 365 System Data and Account Data serves, it is unlikely and not expected that decisions about an individual will be made on this platform or with its information, however, if decisions are made, records will be retained in accordance with records management obligations.

5.3. Records Retention and Disposal

Cite the approved SFU Records Retention and Disposal Authority (RRSDA) that apply to the records series generated through this initiative. Link to SFU's Directory of University Records to determine if an approved RRSDA exists for these records.

If no approved RRSDA exists, describe how the records will be kept in the meantime. Note that if an individual's personal information is used by or on behalf of SFU to make a decision that directly affects the individual, SFU must retain the personal information for at least one year after being used. This is to ensure that the affected individual has a reasonable opportunity to obtain access to that personal information.

Multiple departments and faculties are expected to use Microsoft 365. Customer Content will be retained and disposed of in accordance with governing RRSDAs for the department or faculty owning that data. In the event that conflicting opinions about applicable RRSDAs arise, the Archives and/or SFU Legal will provide guidance about proper record disposition.

6. Further Information

6.1. Systematic Disclosures of Personal Information

Describe here (if applicable) any usual disclosures inside the University between the office with primary responsibility for the personal information and other SFU departments and programs. Also describe any usual disclosures outside the University between SFU and another public or private body (e.g., provincial, territorial or federal government ministry, department or agency; university or college; transit authority; law enforcement agency).

If SFU and one or more other parties have signed an Information Sharing Agreement, include a copy with this completed PIA. An Information Sharing Agreement sets terms and conditions on the collection, use, disclosure and protection of personal information by the parties to the agreement.

None known. See 6.3

6.2. Access for Research or Statistical Purposes

Describe here (if applicable) any usual disclosures of the personal information made by your department for a research purpose, including statistical research, and how you comply with section 35 of the Act.

None known. See 6.3

6.3. Personal Information Directory (PID) and Personal Information Banks (PIB)

The Personal Information Directory (PID) contains descriptions of the Personal Information Banks (PIBs) created and maintained by Simon Fraser University. A PIB is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. PIB entries are added to the Directory as PIB records series are identified and scheduled.

Cite the PIB that apply to the records series generated through this initiative. Link to SFU's Directory of University Records and search the Personal Information Directory to determine if a PIB description exists for these records.

If no PIB description exists, create one below using the outline described in the Personal Information Directory.

Not applicable. However, any SFU program or department using the data resting on Microsoft's services will be responsible for the required Information Sharing Agreements or Research Agreements in the event that personal information is disclosed regularly and systematically or for research or statistical purposes as well as providing the Privacy Office with information on any Personal Information Banks.

7. Coordinator of Information and Privacy Comments

7.1. Information or Materials Reviewed

The Coordinator will describe here any additional resources and authorities consulted when reviewing and commenting on the completed PIA.

Bill Trott, Information and Privacy Officer reviewed and considered:

1. UBC PIA01675 Microsoft 365: MS OneDrive, MS Teams, and Related MS Azure Services;
2. UVic Microsoft 365 PIA, April 30, 2020;
3. BCNET PIA Microsoft Azure;
4. BC Government PIA for Microsoft SharePoint Online and OneDrive for Business, PIA#CITZ20078, November 19, 2020;
5. BC Government PIA for Microsoft Teams, PIA#CITZ20028, September 2, 2020;
6. Langara PIA Microsoft Office 365, PIA2019-0005;
7. Interview with BC Corporate Information and Records Management Office, March, 2021;
8. Interview with Microsoft representative, March, 2021;
9. Meetings with SFU IT Services staff, 2021;
10. Microsoft's Law Enforcement Requests Report (https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report)
11. Microsoft's Online Services Terms (https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all);
12. https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?ms.officeurl=datamaps&view=o365-worldwide#canada; and
13. Campus and School Agreement Amendment ID CTM-X20-11363", (updated October 2013)

7.2. Conditions of Approval

The Coordinator will describe here any recommended conditions to be considered by the University officer with delegated decision-making authority under the Act, who approves the completed PIA.

Recommended conditions are:

1. **Submit contemplated system changes for FIPPA compliance review**: Any contemplated changes to or use of this system that differs from the description provided in this PIA (e.g., in the collection, use, disclosure or storage of personal information) must be reviewed by the Archives for compliance with FIPPA. IT Services must consult with the Archives and Records Management Department prior to implementing any proposed changes to the implementation or use of the system.
2. **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. ITS should have a 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 SFU. ITS must take steps to ensure that SFU's implementation of Microsoft Teams is tenanted in Canada.
3. **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. As discussed above students will be presented with a consent notice when they sign up for the service.

4. **Implementation of Retention and Disposition Process for Azure Active Directory Data:** It appears 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. ITS 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. ITS should work with the Archives and Records Management Department on drafting a Records Retention Schedule and Disposal Authority for this purpose.

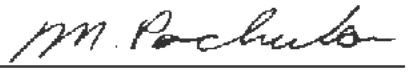
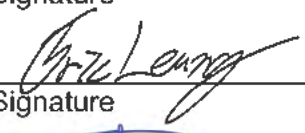
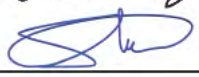
5. **Implementation of Retention and Disposition Process for MS Teams Customer Data:** The intended structure and use of MS Teams in learning settings has not yet been fully established or documented. It is unclear if a team established for a course session will be re-used for subsequent course sessions 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. ITS and appropriate SFU stakeholders must establish and implement processes to address excessive retention of Customer Data and deletion or archiving 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. ITS should work with the Archives and Records Management Department on drafting a Records Retention Schedule and Disposal Authority for this purpose.

6. **Review and Assessment of Proposed / Agreed Configuration Settings** ITS must document 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. ITS 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 SFU change management processes. The Privacy Office 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.

7. **Review and Assessment of Implementation of Products, Services, or Integrations:** ITS 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.

8. Approval and Signatures

The undersigned confirm that they have taken reasonable steps to confirm that the contents of this PIA are accurate and complete.

Martin Pochurko		Sept 27, 2021
VP Finance and Administration	Signature	Date
Eric Leung		
Program Manager	Signature	Date
Stephen MacGregor		September 16, 2021
Information Compliance Architect	Signature	Date
Paul Hebbard		September 16, 2021
Coordinator of Information and Privacy	Signature	Date

Schedule A

Definition of terms	
Access	Disclosure of personal information by the provision of access to personal information.
Anonymize	Present the results of a process in such a way that individuals whose personal information is contained in the records cannot be identified, and no linkages can be made between any personal information found in the records and personal information that is publicly available from other sources.
Authorized access	Occurs when a person has access to personal information in the custody or control of the University that is authorized by the Act.
Consistent purpose	A use of personal information is consistent with the purpose for which the information was obtained or compiled if the use: 1. has a reasonable and direct connection to that purpose, and 2. is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.
Contact information	Information that enables an individual at a place of business to be contacted; includes name, position title, business telephone number, business address, business email or business fax number of the individual.
Data linking	The linking or combining of personal information in one source with personal information in one or more other sources if the purpose of the linking or combining is different from: 1. the purpose for which the information in each database was originally obtained or compiled, and 2. every purpose that is consistent with each purpose referred to in paragraph (a).
Disclose	Reveal, show, expose, provide copies of, sell, give or tell. SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3 of the Act.
Employee	A person employed for wages or salary by the University. In relation to SFU, includes: (a) a volunteer and (b) a service provider (see also the definitions for each of the latter terms).
Individual identifier	Information that would enable a third party to deduce the identity of the person concerned; examples include a person's name, Social Insurance

Number, student number, employee number, address, date of birth (usually used in combination with other identifiers).

Instructor	Individuals responsible for the teaching of credit and non-credit courses including professors, associate professors, assistant professors, professors emeritus, adjunct professors, visiting faculty, practitioner faculty, post-retirement appointees, lecturers, instructors, teaching assistants, tutors and markers, faculty associates, in-service associates, associate members and program coordinators.
Personal information	Recorded information about an identifiable individual, other than business contact information, including but not limited to: 1. names, home addresses and telephone numbers; 2. age; 3. sex; 4. marital or family status; 5. identifying number; 6. race, national or ethnic origin; 7. colour; 8. religious or political beliefs or associations; 9. educational history; 10. medical history; 11. disabilities; 12. blood type; 13. employment history; 14. financial history; 15. criminal history; 16. images; 17. anyone else's opinions about an individual; 18. an individual's personal views or opinions; and, 19. name, address and phone number of parent, guardian, spouse or next of kin.
Record	Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.
Service provider	A person retained under contract to perform services for SFU or a person with whom an employee automatically enters into an agreement by virtue of using their product or service and in so doing accepts the service provider's terms of use.
Unauthorized collection, use, disclosure and disposal	Occurs when a person who has access, whether authorized or unauthorized, to personal information in the custody or control of the University, collects, uses, discloses and disposes of that information and it is not authorized by the Act.
Use	Employ information to accomplish a specific purpose.
Volunteer	A person who provides a service to the University without being paid.

Schedule B

FIPPA table of contents

Collection, Accuracy, Correction, Protection and Retention of Personal Information

Collection	Section 26	Purpose for which personal information may be collected 1. Prescribes the only situations in which SFU is permitted to collect personal information 2. Collect only the minimum personal information related directly to and necessary for the particular purpose
	Section 27	How personal information is to be collected 3. Prescribes that SFU must collect personal information directly from the individual the information is about except in very limited and specified circumstances 4. Prescribes when a collection notice is required and not required to be given to individuals
	Section 27.1	When personal information is not collected 5. Describes the situation when personal information is received by SFU but not collected
Accuracy	Section 28	Accuracy of personal information 1. Prescribes that SFU must make every reasonable effort to ensure that the personal information it uses is accurate and complete 2. Information collected by the University is often used to make a decision that directly affects the individual. Ensure this information is accurate because using out-dated information may result in serious consequences for the individual and the University
Correction	Section 29	Right to request correction of personal information 1. Prescribes how SFU must handle a request made by an individual to correct her or his information 2. Where factual errors in personal information are identified, the University is responsible for making the appropriate corrections upon request. If the incorrect information was made available to a third

		party, the University is responsible for providing the corrected information to that third party
Protection	Section 30	Prescribes that SFU must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal 1. The media on which information is stored (paper or digital) must be considered when deciding what reasonable physical, technical and procedural security measures are necessary to adequately protect the personal information
	Section 30.1	Storage and access must be in Canada 2. Prescribes that SFU must ensure that personal information in its custody or under its control is stored and accessed only in Canada except in very limited and specified circumstances
Retention	Section 31	Retention of personal information 1. Prescribes that SFU must ensure that personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information

Use and Disclosure of Personal Information

Use	Section 32	Use of personal information 1. Prescribes the only situations in which SFU may use the personal information it collects 2. Consider the difference between “use” (within the University office that collected) and “disclosure” (making information available to anyone else inside or outside the University)
Disclosure	Section 33	SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3 1. Describes the situations in which personal information may be released to another person. The circumstances under which personal information may be disclosed are prescribed in very specific and limited terms, therefore, it is important to confirm that one has legal authority to disclose personal information before doing so

Section 33.1	Disclosure inside or outside Canada
	2. Prescribes the only situations in which SFU may disclose personal information inside or outside Canada
Section 33.2	Disclosure inside Canada only
	3. Prescribes the situations in which SFU may disclose personal information inside Canada only
Section 33.3	Disclosure of personal information in records available to public without request
	4. Prescribes the situation when SFU may disclose to the public a record that is within a category of records established under section 71(1)
Section 35	Disclosure for research or statistical purpose
	5. Prescribes the situation when SFU may disclose personal information in its custody or under its control for a research purpose, including statistical research

Schedule C

Types of security measures	
Physical	1. SFU data centre and backup data centre are both located on SFU campuses in Canada 2. Locked doors 3. Key card and electronic access control devices 4. Securely stored computing equipment 5. Receptionist supervision 6. Physical barrier to the public 7. Staff only access 8. Alarm systems 9. After hours security patrol checks
Technical	1. Firewalls 2. Encrypted network transmission 3. Tiered network infrastructure 4. Identity assurance provided by SFU's main Systems of Record 5. Role-based user access assigned on a need-to-know basis 6. Log-on user ID and password (single sign-on) provided by SFU's Central Authentication Service (CAS) 7. Timed out computer sessions
Security Policy, Procedure and Standards	1. University Policies e.g., GP-24 Fair Use of Information Systems, I 10.04 Access to Information and Protection of Privacy, I 10.05 Collection of Personal Information, I 10.09 Retention and Disposal of Student Exams or Assignments, and I 10.10 Confidentiality Policy 2. Designation and authentication of authorized users is managed through SFU's Identity and Access Management (IDAM) infrastructure, which is registered with the Canadian Access Federation (CAF) 3. SFU's IDAM infrastructure is benchmarked against the InCommon assurance program (http://incommn.org), which certifies campuses, non-profits and research organizations to determine the accuracy of a user's electronic identity and help mitigate risk for the service provider. While InCommon certification is not available outside the US, the assurance program serves as a benchmark for international standards and best practices 4. SFU's Privacy Protection Schedule is included as part of a signed agreement with a service provider of digital storage when purchased through Procurement, which includes provisions relating to data ownership, use, disclosure, security, retention and confidential/permanent deletion 5. SFU has signed an Information Sharing Agreement with the public body describing the terms and conditions of their data-linking initiative or common or integrated program or activity

	6. Authorized users of the IT system are made aware of protection of privacy rights and responsibilities by means of notices when logging onto the system; education by through the SFU website, workshops and advisory service; and/or signing SFU's Privacy and Confidentiality Agreement 7. Personal information is retained and disposed of according to an existing Records Retention Schedule and Disposal Authority approved by the University Archivist
Tracking Access / Access Controls	1. IDAM infrastructure assures identity 2. Role-based access management infrastructure authorizes access 3. Auditable log files

APPENDIX A - Data Elements

Data from SFU's on premise Active Directory services is pushed to Azure Active Directory on a recurring schedule.

The following table of data elements (Active Directory "Attributes") provides an overview of the data that may be collected, used, and disclosed with the Microsoft 365 applications being implemented. It is grouped to show data elements used for specific services, such as SharePoint Online and MS Teams (some data elements may be repeated).

Please note that **Intune** is included in this table as a service requiring AD elements; however, this service has not been assessed by SFU for risk to privacy.

Service Name	Attribute Name	Comment
M365 Apps	accountEnabled	Defines if an account is enabled.
M365 Apps	cn	
M365 Apps	displayName	
M365 Apps	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
M365 Apps	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password hash sync, pass-through authentication and federation.
M365 Apps	samAccountName	
M365 Apps	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
M365 Apps	usageLocation	mechanical property. The user's country/region. Used for license assignment.
M365 Apps	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
Intune	accountEnabled	Defines if an account is enabled.
Intune	c	
Intune	cn	

Service Name	Attribute Name	Comment
Intune	description	
Intune	displayName	
Intune	mail	
Intune	mailnickname	
Intune	member	
Intune	objectSID	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
Intune	proxyAddresses	
Intune	pwdLastSet	mechanical property. Used to know when to invalidate already issued tokens. Used by both password hash sync, pass-through authentication and federation.
Intune	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
Intune	usageLocation	mechanical property. The user's country/region. Used for license assignment.
Intune	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
SharePoint Online	accountEnabled	Defines if an account is enabled.
SharePoint Online	authOrig	indicates that the mailbox for the target object is authorized to send mail to the source object
SharePoint Online	c	Country abbreviation
SharePoint Online	cn	Common name or alias. Most often the prefix of [mail] value.
SharePoint Online	co	Country
SharePoint Online	company	The user's company name.
SharePoint Online	countryCode	Specifies the country/region code for the user's language of choice.
SharePoint Online	department	The name of the person's (user or contact) department.
SharePoint Online	description	Contains the description to display for an object.
SharePoint Online	displayName	A string that represents the name often shown as the friendly name (first name last name).
SharePoint Online	dLMemRejectPerms	Distribution reject permission list.
SharePoint Online	dLMemSubmitPerms	Distribution submit permission list.
SharePoint Online	extensionAttribute1	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute10	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute11	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.

Service Name	Attribute Name	Comment
SharePoint Online	extensionAttribute12	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute13	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute14	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute15	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute2	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute3	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute4	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute5	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute6	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute7	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute8	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	extensionAttribute9	Custom attribute that is defined in the customer on-premises directory.
SharePoint Online	facsimiletelephonenumb	Contains telephone number of the user's business fax machine.
SharePoint Online	givenName	Contains the given name (first name) of the user.
SharePoint Online	hideDLMembership	True/False. Hide distribution list.
SharePoint Online	homephone	The person's (user or contact) main home telephone number.
SharePoint Online	info "Notes" field on "Telephone" tab of ADUC.	
SharePoint Online	initials Strings of initials of some or all of an individual's names, except the surname(s).	
SharePoint Online	ipPhone TCP/IP Address of common area phone	
SharePoint Online	l City	
SharePoint Online	mail The list of email addresses for a contact.	
SharePoint Online	mailnickname Alias of the users mailbox.	
SharePoint Online	managedBy The distinguished name of the user that is assigned to manage this object.	
SharePoint Online	manager manager properties set to this distinguished name.	
SharePoint Online	member The list of users that belong to the group.	
SharePoint Online	mobile The primary mobile phone number.	
SharePoint Online	msExchTeamMailboxExpi Date attribute	

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

Service Name	Attribute Name	Comment
SharePoint Online	telephoneAssistant	Assistant Phone Number
SharePoint Online	telephoneNumber	The primary telephone number.
SharePoint Online	thumbnailphoto	Persons Photo - 10kb maximum size limit
SharePoint Online	title Contains the user's job title.	
SharePoint Online	unauthOrig Email addresses that cannot send messages to this email address	
SharePoint Online	url	The list of alternative web pages.
SharePoint Online	usageLocation mechanical property. The user's country. Used for license assignment.	
SharePoint Online	userPrincipalName UPN is the login ID for the user. Most often the same as [mail] value.	
SharePoint Online	wWWHomePage Web site	
MS Teams	**accountEnabled Defines if an account is enabled.**	
MS Teams	c Country abbreviation	
MS Teams	cn Common name or alias. Most often the prefix of [mail] value.	
MS Teams	co Country	
MS Teams	company The user's company name.	
MS Teams	manager manager properties set to this distinguished name.	
MS Teams	department The name of the person's (user or contact) department.	
MS Teams	description Contains the description to display for an object.	
MS Teams	displayName A string that represents the name often shown as the friendly name (first name last name).	
MS Teams	facsimiletelephonenumb Contains telephone number of the user's business fax machine.	
MS Teams	givenName Contains the given name (first name) of the user.	
MS Teams	homephone	The person's (user or contact) main home telephone number.
MS Teams	ipPhone TCP/IP Address of common area phone	
MS Teams	l City	
MS Teams	mail The list of email addresses for a contact.	
MS Teams	mailNickname Alias of the users mailbox.	
MS Teams	managedBy The distinguished name of the user that is assigned to manage this object.	

MS Teams	mechanical property. Used to know when to invalidate already issued tokens. Used by both pwd LastSet password sync and federation.	
MS Teams	member The list of users that belong to the group.	
MS Teams	mobile The primary mobile phone number.	
MS Teams	msExchHideFromAddress Indicator to control the visibility of a mail recipient for name resolution.	
MS Teams	msRTCSIP- Lync/SfB - Fully qualified DNS name of the Microsoft Lync Server 2010 deployment, as specified in DeploymentLocator the authoritative (customer, on-premises) directory.	
MS Teams	msRTCSIP- Lync/SfB - SIP URI for instant messaging, as specified in the authoritative (customer, on-premise) PrimaryUserAddress directory.	
MS Teams	msRTCSIP- Lync/SfB. Option for the application contact.	
MS Teams	msRTCSIP-OptionFlags Lync/SfB	
MS Teams	msRTCSIP-OwnerUrn Lync/SfB	
MS Teams	objectSID mechanical property. AD user identifier used to maintain sync between Azure AD and AD.	
MS Teams	otherTelephone A list of alternative office telephone numbers.	
MS Teams	physicalDeliveryOfficeNa Contains the office location in the user's place of business.	
MS Teams	postalCode The postal or zip code for mail delivery.	
MS Teams	preferredLanguage The preferred written or spoken language for a person.	
MS Teams	proxyAddresses Mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.	
MS Teams	securityEnabled	Derived from groupType
MS Teams	sn	Last Name
MS Teams	sourceAnchor	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
MS Teams	st	State/Province
MS Teams	streetAddress	Street Address
MS Teams	telephoneNumber	The primary telephone number.
MS Teams	thumbnailphoto	Persons Photo - 10kb maximum size limit
MS Teams	title	Contains the user's job title.
MS Teams	usageLocation	mechanical property. The user’s country. Used for license assignment.
MS Teams	userPrincipalName	UPN is the login ID for the user. Most often the same as [mail] value.
MS Teams	wWWHomePage	Web site

In addition to the above attributes, a password hash is also passed into Azure Active Directory.