Privacy Impact Assessment

PIA# 24-0021

INSTRUCTIONS/INFORMATION:

Why do I need to do a PIA?
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 FOIPPA.

Do I have to answer all the questions?
Sections marked as "required" must have an answer. Specify *N/A (not applicable)* if appropriate. Other sections not marked mandatory should STILL be answered if the information is known. You will be contacted to answer any questions that are deemed relevant to this assessment so it's best to be complete.

What if my initiative does not include personal information?
You still need to complete some parts of the PIA to ensure compliance with regulation. Under question "4. Elements of Information or Data", specify "*no personal information collected*". Sections that are marked as "*required*" still need to be answered.

What if I have questions?
If you have any questions about FOIPPA generally, you may contact the "*Privacy and Access Officer*" (privacy@tru.ca). For questions specific to this PIA, contact the "*Information Security Director*" (jcuzzola@tru.ca).

Please note: Depending on the dollar amount or length of the agreement you intend to enter into with a third party, you may need to engage the Procurement Services Department. Please see the TRU Purchasing Policy (BRD 02-2) for more information.

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	**Microsoft Copilot for Microsoft 365 and Copilot for Microsoft 365 Education**		
Name of TRU Department/Branch:	Information Security and Privacy Office.		
PIA Drafter (you):	John Cuzzola, Marina Sparks.		
Your Email:	jcuzzola@tru.ca, msparks@tru.ca	Phone:	
Service/Vendor:	Microsoft (Jenn Greene)		
Vendor Email:	jengreene@microsoft.com	Phone:	289-208-2916

Have you consulted IT Department for this Initiative/Project/Program?
_Yes_____ **No**_____ **N/A**____X_____
(*If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.*)

Part 1 – General

1. Description of the Initiative (required)

Copilot is an AI powered tool that is designed to assist with various tasks and increase productivity. Copilot can assist with searching for information, generating new content based on user prompts, answering questions, preparing presentations, transcribing meetings, etc. Copilot is a Microsoft product, and is integrated into the M365 environment. Copilot uses machine learning algorithms to make sense of user prompts and provide relevant content.

There are two version of Copilot currently in use at TRU: Microsoft Co-Pilot for Microsoft 365, and Copilot for Microsoft 365 Education.

Microsoft Copilot for Microsoft 365

- designed for general business and enterprise users, providing tools to enhance productivity and collaboration across various Microsoft 365 applications
- is available to business and enterprise customers with appropriate Microsoft 365 licenses.
- focuses on enhancing productivity, collaboration, and efficiency in a business environment. It includes features like document drafting, meeting preparation, and data analysis.

Copilot for Microsoft 365 Education

- specifically tailored for educational institutions, including faculty and students, to support teaching, learning, and administrative tasks.
- is available to education customers with Microsoft 365 A3 or A5 faculty licenses.
- includes features that cater to the unique needs of educational institutions, such as tools for personalized learning, academic research assistance, and administrative process improvements.

2. Scope of this PIA (required)

This section should explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

This PIA addresses security provisions in place to ensure that TRU can adequately protect the personal information in its custody and control that is entered into either version of Copilot.

This PIA focuses on the flow of data that is entered into Copilot, and how TRU will ensure personal information that may be entered into Copilot will be adequately protected s.13, s.14 [redacted]

2-1. Is this initiative recurring in a regular interval, e.g., yearly, or biennially? (required)

TRU's use of Microsoft Copilot will be ongoing.

3. Related Privacy Impact Assessments

s.13, s.14

4. Elements of Information or Data (required)

Due to the expansive nature of Co-Pilot's functionality, any information may be involved, including:

- Personal information about TRU students, faculty and staff;
- Information about TRU projects/initiatives;
- Confidential information;
- Information that is subject to solicitor client privilege;
- General communications, including content of meetings.

This PIA is being carried out based on an assumption that the most sensitive classes of information will be involved (information in the "Confidential" class per the TRU Information Classification Standard, which attracts the highest requirements for access restrictions, transmission, storage and disposal).

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

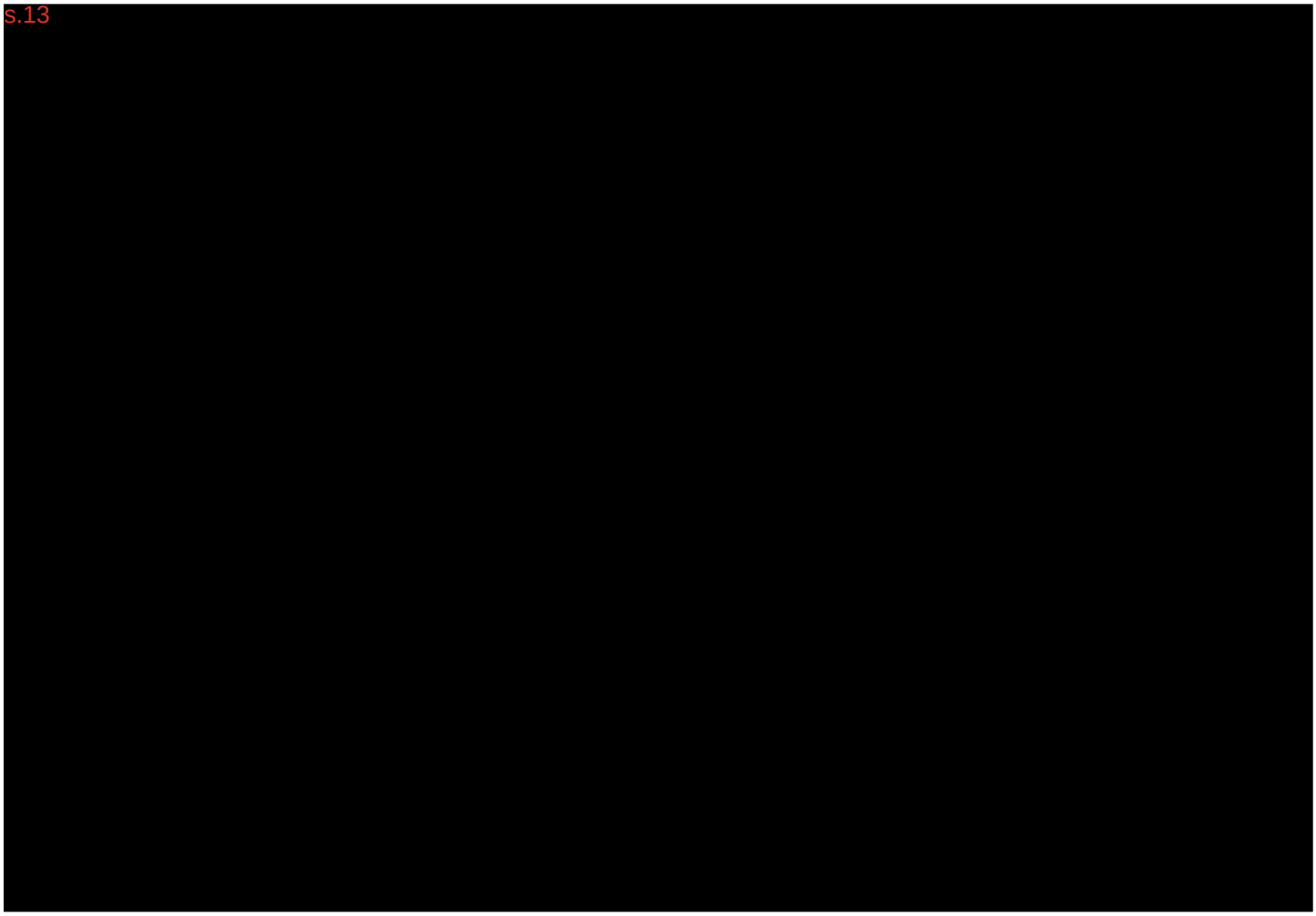
5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)

Microsoft has contracted with TRU to provide software products to TRU. FIPPA defines a service provider as "a person retained under a contract to perform services for a public body." A service provider is involved here.

Microsoft's arrangement with TRU involves storing Customer Data for their Core Online Services, including Microsoft Copilot, within major geographic areas referred to as Geos. The specific locations of these storage data centers are determined by the regions outlined in the Product Terms.

Microsoft is a US based company.

s.13



6. Common or Integrated Program or Activity (required)
If you answer yes, please contact the *Privacy and Access Officer*

If you answer "yes" to all 3 of these questions, your initiative qualifies as "a common or integrated program or activity," and you must comply with requirements under FOIPPA.	
1. This initiative involves a program or activity that provides a service (or services);	yes/no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes/no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes/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.	yes/no

7. Data-linking Initiative* (required)
If you answer yes, please contact *Privacy and Access Officer*

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
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

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**

1.	Users generate prompts for Copilot, which creates a response. This may be in the form of a question, a request for Copilot to create minutes from a meeting, request to convert a document into a presentation, etc.	Use	s.32(a), s.32(c).
2			
3			
4			

9. Risk Mitigation Table (required)

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please identify the likelihood (rare, unlikely, possible, likely, almost certain) and the degree of impact (insignificant, minor, moderate, major, catastrophic).

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact	Exposure
1	s.13	[redacted]			
2					

s.13

3

[redacted]

s.13 [redacted]

→ Exposure rating of *high* or *critical* is of concern. Please contact Director, Information Security to discuss possible solutions.

s.13 [redacted]

Risk Exposure Matrix

Risk Exposure Matrix		IMPACT				
		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	Low	Medium	High	Critical	Critical
	Likely	Low	Medium	High	Critical	Critical
	Possible	Insignificant	Low	Medium	High	High
	Unlikely	Insignificant	Low	Low	Medium	Medium
	Rare	Insignificant	Insignificant	Insignificant	Low	Low

10. Collection Notice

TRU will not be using Copilot to collect personal information, but to process information we already have in our custody/under our control or that is freely available online. s.13, s.14 [redacted]

s.13, s.14 [redacted]

Part 3 – Security of Personal Information

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

Rigorous Physical Security Controls
Microsoft enforces stringent physical security controls to protect its infrastructure, including data centers where Microsoft 365 Copilot operates. These controls include:

- *Restricted Physical Access: Data centers are equipped with multi-layered access restrictions such as biometric scanners, key cards, and security guards to ensure that only authorized personnel can enter.*
- *Surveillance and Monitoring: Continuous video surveillance, intrusion detection systems, and alarm systems monitor the premises to prevent unauthorized physical access.*
- *Environmental Controls: Safeguards, such as fire suppression systems, temperature monitoring, and backup power supplies, ensure operational continuity and physical protection of hardware.*

Compliance Certifications
Microsoft data centers adhere to industry-recognized compliance standards and certifications:

- *ISO/IEC 27001: This international standard specifies requirements for establishing, implementing, and maintaining robust information security management systems, including physical security.*
- *ISO/IEC 27018: A code of practice for protecting personal data in the cloud, specifically ensuring physical controls align with international privacy expectations.*
- *SOC 1, SOC 2, and SOC 3: These Service Organization Control reports validate the effectiveness of controls, including physical security measures, to protect customer data in data centers.*
- *FIPS 140-2 Compliance: Microsoft ensures the use of cryptographic technologies for data encryption and protection at rest and in transit.*

Microsoft Data Center Safeguards
Microsoft data centers are designed with multiple layers of security to ensure the protection of customer data processed by Microsoft 365 Copilot. Includes:

- *Geographically Dispersed Facilities: Microsoft operates data centers across various regions, ensuring redundancy and reducing risk from localized incidents.*
- *Data Isolation Between Tenants: ensures that customer data remains logically and physically segregated*[1]
- *Backup Systems: Data centers include backup power supplies and failover systems to ensure uptime and data availability even during physical disruptions.*
- *Personnel Screening: Microsoft uses background screening for individuals with physical access to the data centers, ensuring that only trusted personnel can access sensitive environments*[2]*.*

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

[1] Enterprise data protection in Microsoft 365 Copilot and Microsoft Copilot | Microsoft Learn
[2] AI security for Microsoft 365 Copilot | Microsoft Learn

***Encryption**:*
All data sent for AI processing is encrypted both in transit and at rest. Microsoft 365 uses FIPS 140-2-compliant service-side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS) 1.2, and Internet Protocol Security (IPsec)[3]

***Access Control**:*
Microsoft 365 Copilot accesses resources on behalf of the user, so it can only access resources the user already has permission to access [3]*Copilot respects Microsoft 365, Microsoft Entra, and Microsoft Purview policies that further limit user access and permission, such as information barriers, Conditional Access, and sensitivity labels*[3]

***Data Isolation**:*
Copilot uses encryption at rest and in transit, physical security controls, and data isolation between tenants[4]

***Content Filtering and Prompt Injection Mitigation**:*
Copilot uses machine learning for content filtering at multiple layers with continuous monitoring. Indirect or cross-prompt injection classifiers to detect and block prompt injection at multiple layers[3].

***Responsible AI and Post-Processing**:*
Copilot performs post-processing after receiving responses from the LLM. This includes additional grounding calls to Microsoft Graph, AI checks such as content classifiers, security, compliance, and privacy checks[5]

***Threat Protection**:*
Microsoft Threat Intelligence, a global network of researchers, monitors threat actors and cyberattacks that might take advantage of AI applications[3]

***Data Loss Prevention (DLP)**:*
Copilot inherits data loss prevention (DLP) policies to prevent data exfiltration of Copilot-generated responses. Additionally, it enhances data security by applying sensitivity labels to these responses[3]

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

***Zero Trust Security Policies**:*
Zero Trust principles to ensure security across the Microsoft 365 environment:
'never trust, always verify.' enforcing the validation of user credentials, device requirements, and app permissions and behaviors[6]

[3] AI security for Microsoft 365 Copilot | Microsoft Learn
[4] Enterprise data protection in Microsoft 365 Copilot and Microsoft Copilot | Microsoft Learn
[5] Transparency Note for Microsoft 365 Copilot | Microsoft Learn
[6] How do I apply Zero Trust principles to Microsoft 365 Copilot? | Microsoft Learn

***Microsoft 365 Security Policies**:*
Copilot respects Microsoft 365, Microsoft Entra, and Microsoft Purview policies that further limit user access and permission, such as information barriers, Conditional Access, and sensitivity labels[3]

***Data Loss Prevention (DLP) Policies**:*
Copilot inherits data loss prevention (DLP) policies to prevent data exfiltration of Copilot-generated responses[3]

***Access Controls and Permissions**:*
Copilot accesses resources on behalf of the user, so it can only access resources the user already has permission to access[3]

***Security Development Lifecycle (SDL)**:*
Rigorous SDL integrates security considerations throughout the entire AI development process[3].

***Audit Logging and Retention Policies**:*
Copilot meets regulatory requirements for eDiscovery, audit logging, and retention[3]

***Responsible AI Policies**:*
Microsoft Responsible AI principles guide the development and use of Microsoft 365 Copilot[3]

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. (required)

***Access Permissions**:*
Copilot accesses resources on behalf of the user, so it can only access resources the user already has permission to access. If the user doesn't have access to a document, for example, then Microsoft 365 Copilot working on the user's behalf will also not have access either[3]

***Inheritance of Security Policies**:*
Copilot respects Microsoft 365, Microsoft Entra, and Microsoft Purview policies that further limit user access and permission, such as information barriers, Conditional Access, and sensitivity labels[3]

***Audit Logging and Retention**:*
Copilot meets regulatory requirements for eDiscovery, audit logging, and retention through several mechanisms... Audit logs generated by Microsoft 365 Copilot can be retained for up to 180 days for Audit (Standard) customers and up to one year for Audit (Premium) license holders, with the option to extend up to 10 years[3]

***Data Loss Prevention (DLP)**:*
Copilot inherits data loss prevention (DLP) policies to prevent data exfiltration of Copilot-generated responses[3]

***Role-Based Access Controls**:*
Grounding occurs within the context of your identity, and the semantic index and graph queries are trimmed based on your permissions for the underlying content. This process ensures that only authorized content is included in the grounding process[3]

***Administrative Controls**:*
Admins can use Microsoft Purview to view and manage stored data, set retention policies, and perform eDiscovery searches[3]

***Protection of Copilot Activity History**:*
Admins can also use Microsoft Purview to set retention policies for the data related to chat interactions with Copilot[7].

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

***Audit Logging**:*
Copilot meets regulatory requirements for eDiscovery, audit logging, and retention. Audit logs generated by Microsoft 365 Copilot can be retained for up to 180 days for Audit (Standard) customers and up to one year for Audit (Premium) license holders, with the option to extend up to 10 years[3]*. The details are as follows:*

- ***eDiscovery**:*
  Copilot supports eDiscovery, which allows administrators to search, access, and manage data related to Copilot interactions for legal and compliance purposes.

  Admins can use Microsoft Purview to view and manage stored data, set retention policies, and perform eDiscovery searches[3]

  eDiscovery tools enable compliance administrators to retrieve user prompts and Copilot responses that are stored in a hidden folder within the user's mailbox.

- ***Audit Logging**:*
  All activities within Copilot are tracked and recorded for transparency and accountability. Logs include details about user prompts and Copilot-generated responses, ensuring visibility into actions performed using Copilot and aiding in audits and investigations.

- ***Retention Policies**:*
  Retention policies help organizations define how long data related to Copilot interactions, such as prompts and responses, is retained or deleted to comply with regulatory requirements.

[7] Data, Privacy, and Security for Microsoft 365 Copilot | Microsoft Learn

Messages from Microsoft 365 Copilot are automatically included in the retention policy location named Teams chats and Copilot interactions. This means that user prompts and Copilot responses can be retained and deleted for compliance reasons[3]

Retention policies ensure that organizational data remains available as long as necessary and is deleted when no longer required, supporting compliance with data governance frameworks.

***Admin Controls and eDiscovery**:*
Admins can use Microsoft Purview to view and manage stored data, set retention policies, and perform eDiscovery searches[3]

***Access Permissions and Security Trimming**:*
Grounding occurs within the context of your identity, and the semantic index and graph queries are trimmed based on your permissions for the underlying content to ensure that only authorized content is included in the grounding process.[3]

***Retention Policies**:*
Messages from Copilot are automatically included in the retention policy location named Teams chats and Copilot interactions. User prompts and Copilot responses can be retained and deleted for compliance reasons[3].

***Administrative Visibility**:*
Admins can review feedback submitted in the Microsoft 365 admin center[5].

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's personal information updated or corrected? If it is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated.

TRU will retain access to information processed using Copilot, our existing procedures for updating personal information as needed will apply.

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

Copilot will be used for various purposes, existing requirements to retain personal information used to make a decision that directly affects an individual for one year after the decision is made to allow the individual a reasonable opportunity to access that personal information (requirement under s.31 of FIPPA) will apply.

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

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

N/A

Part 5 – Further Information

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

No

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact Legal Services.	No

21. Does the program involve access to personal 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 *Privacy and Access Officer*.	No

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

A personal information bank means 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.

Certain uses of Copilot may result in the creation of a PIB, but those will need to be assessed on a case-by-case basis. There is nothing inherent to Copilot that would result in a PIB.

Part 6 – Canada's Anti-Spam Legislation (CASL) Compliance

23. Please confirm if you plan on emailing, texting, or instant messaging as part of your project. (required)

Certain uses of Copilot may involve sending CEMs, but those will need to be assessed on a case-by-case basis. General use of Copilot will not involve sending CEMs.

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM[8])?

N/A

25. If your communication message does fall under CEM rules, you must comply with the unsubscribe mechanism and identification requirements under CASL. Please confirm your method of unsubscribe mechanism that must be processed within 10 business days and how you will meet the identification requirements?

N/A

26. If you do meet the definition of CEM, please confirm that you have a records retention schedule that will ensure that consent communications, both paper and electronic, are stored appropriately and retained for three years after the last communication?

N/A

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

(This section to be completed by the **Information Security Office**). If your initiative involves the transmission of personal data between TRU and the vendor, or from the vendor to 3rd parties, then TRU may ask for the name of the software used to determine if there are applicable CVEs.

[8] If your initiative or program sends commercial electronic messages (CEMs), such as emails promoting a product or service, you must comply with CASL's requirements to: (1) obtain consent, (2) provide identification information, and (3) include an unsubscribe mechanism in each message. Please note that an electronic message that contains a request for express consent is also considered to be a CEM under CASL.

Part 8a – Information Security Director Comments

s.13 .

John Cuzzola	s.22	2025-01-15
Information Security Director	Signature	Date

Part 8b – Privacy Officer Comments

s.13, s.14

Marina Sparks	s.22	2025-01-16
Privacy and Access Officer	Signature	Date

Part 9 – Program Area Signatures

Program/Department Manager	Signature	Date
John Cuzzola	s.22 [redacted]	2025-01-15
Information Security Director	Signature	Date
Senior Manager, Program Area/Division	Signature	Date
General Manager	Signature	Date
General Manager	Signature	Date

A Final Copy of this PIA (with all signatures) shall be kept on record by the program area responsible for this project. The signed original record will be retained by the FOI and Privacy Office. ***If you have any questions about FOIPPA generally, you may contact the "Privacy and Access Officer" (privacy@tru.ca). For questions specific to this PIA, contact the "Information Security Director" (jcuzzola@tru.ca).***