PIA02712 – MS Teams Transcription

PIA REVIEW – EXECUTIVE REPORT

PREFACE

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

This segment serves to provide and record document control capabilities for this document.

Controlled Document

The template and final report documents are controlled documents. The master electronic versions of each reside on the SRS TeamShare S-drive. Any copies or versions not provided directly by the SRS PrISM team, or which have a broken chain of custody, are not to be considered as official copies.

Document Control

The following sub-sections provide a record of the base document template revision history and control.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Taylor Bohn	Safety and Risk Services	Privacy and Information Security Risk Advisor

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
1.0	2023-06-23	Taylor Bohn	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2023-06-23	Gordon Chan	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

TABLE OF FIGURES

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

UBC's central IT intends to enable the live transcription a feature within Microsoft Teams. Transcriptions and captions, the written output of what is said during a Teams meeting, identifies each speaker, it captures automatically in near real time, and is available during and after the meeting. Live transcription can act as meeting minutes or notes and ensure more inclusive experiences for participants. This change would be made available to all Microsoft Teams end users within the UBC domain.

A PIA was conducted on Microsoft Teams in 2020. The scope of the review at that time did not include the use of live transcription

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

UBC is planning to enable the Live Transcription feature in MS Teams. This functionality will be available to all departments as part of the MS Teams suite.

Live transcription is a written record of the spoken text that occurs during a meeting.
It identifies each speaker, it captures automatically in near real time, and is available during and after the meeting. The text appears alongside the meeting video, including the speaker's name (unless they choose to hide it) with a time stamp. Post meeting, a transcription of the entire meeting can be downloaded. This new feature is related to the existing PIA01675 - Microsoft 365: MS OneDrive, MS Teams, and Related MS Azure Services.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is 4 - **High.**
The residual risk classification level of this PIA submission at closure is 3 - **Medium**.

1.3 Scope

The scope of this PIA will focus on transcription feature in MS Teams. Scope of this PIA will not review aspects which were covered in PIA01675.

1.4 Related PIAs

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

1.5 Elements of Information or Data

All spoken content in a MS Teams meeting will be transcribed if the organizer turns on transcriptions during the meeting. By default, speakers will be identified in the transcription text, but the meeting attendees can hide their identity. in addition, attendees will receive a warning message when transcription is enabled.

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

Any saved/recorded transcripts will remain stored within Canada in meeting organizer's Exchange account, according to Microsoft's documentation.

1.7 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under s.(36) of FIPPA.

1.8 Is this a Common or Integrated Program or Activity?

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

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

- Teams meeting organizer or attendee enables transcription feature at the opening of a meeting.
- Attendees receive a warning message alerting them that the transcription has been enabled and can hide it from their meeting view.
    - If they choose not to be identified, attendees can also turn off speaker attribution in their profile setting.
- Attendees have access to live transcription during the meeting and conversation (including speaker's first and last name).
- The transcript is immediately available in the transcript tile in the chat or event on the calendar at the closing of the meeting.
- Teams live transcription files are stored in the meeting organizer's Exchange Online account and only the organizer has permissions to delete it.
- Attendees can download Teams transcription file as either a .ytt or .docx file
    - Download is restricted to attendees within the UBC domain.

The table below outlines the actions various meeting attendees can take as it relates to live transcription.

Type of meeting participant	Start and stop transcription	View real-time transcription	View transcript after meeting	Download transcript after meeting
Organizer	Yes	Yes	Yes	Yes
Person from same domain	Yes	Yes	Yes	Yes
Person from another domain	No	Yes	No	No
Anonymous	No	No	No	

2.2 Risk Mitigation Table

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

Category: Privacy					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Disclosing to or allowing unauthorized users access	RK0021558	4 - High	3 - Significant	Mitigate	3 - Medium
	The transcription will contain personal information including the first and last names of the individuals involved in the meeting. **Mitigation Plan:** Only those within the UBC domain can enable the transcription feature and/or view it after the meeting. Those outside the UBC domain will only be able to view the transcription while it takes place and will not have access to the file unless the organizer provides them with a copy after the meeting. It is the responsibility of all participants who have access to a transcription to ensure any transcription is handled with the same care as any other UBC Electronic Information and not shared with parties who are not authorized for that information.				
Inadequate controls for volume of personal information	RK0021559	4 - High	3 - Significant	Mitigate	3 - Medium
	Currently UBC IT System administrators are unable to enforce retention schedules for Teams transcription files. **Mitigation Plan:** Teams' live transcription files will need to be retained in compliance with applicable retention schedules by meeting organizers. As per Records Management Office, retention schedules and considerations will differ based on the meeting's contents. These files would be perceived as transitory records and not used to record business decisions and therefore, should be deleted after they have served their purpose. An example of this would be if the transcript were enabled to assist in the creation of meeting minutes, such that the associated transcript file should be deleted once the meeting minutes have been created. As per FIPPA, deletion after 1 year, manually or a retention label set for a year, manually, is the recommended best practice. Records management will be updating their existing documentation for end users regarding the creation of records from collaboration tools.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

Where possible, as a courtesy, all participants should be notified in advance if a scheduled Teams meeting, or Webinar will be transcribed. A warning notice will be displayed to all attendees at the time live transcription is enabled. Notice is as follows: "By attending this meeting, you consent to being included in the transcript. Privacy Policy."

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

Not applicable.

2.5 Consent Withheld Procedure

Not applicable.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards). See PIA01675 for details regarding Microsoft's physical security measures.

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards). See PIA01675 for details regarding Microsoft's technical security measures.

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy), Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems and the associated Information Security Standards.

In addition, UBC's requirements related to respectful communication, including Policy SC7 - Discrimination, the UBC Statement on Respectful Environment for Students, Faculty and Staff, and the UBC Student Code of Conduct.

For details regarding UBC's instance of Microsoft 365 reference Terms of Service: https://it.ubc.ca/services/email-voice-internet/microsoft-teams/microsoft-365-terms-service#:~:text=If%20you%20are%20a%20student,the%20Service%20by%20Other%20Users.

3.4 Tracking Access / Access Controls

Teams' live transcripts are stored in the meeting organizer's Exchange account. The transcript can be accessed through the meeting chat and Recording & Transcripts tab in Teams until a meeting organizer deletes the transcript. For details around what access each meeting attendee has, please see section 2.1 Personal Information Flow.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable.

4.2 Decisions That Directly Affect an Individual

Not applicable.

4.3 Records Retention and Disposal

The meeting organizer will be responsible for retaining transcript files. If the transcript is to create another record, such as meeting minutes, it would be transitory and deleted once the record has been created. Below is the associated schedule.

https://rmo.sites.olt.ubc.ca/files/2022/06/TR0000%E2%80%AF_TransitoryRecords_Rev2.pdf

UBC employees are given guidance from the records management department on how to handle meeting recordings, which would also apply to meeting transcripts. This documentation in its current form can be found using the link below.

https://rmo.sites.olt.ubc.ca/files/2023/06/RM_Guideline_WhenToCreateARecord_Rev0.pdf

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

Not applicable.

5.2 Access for Research or Statistical Purposes

Not applicable.

5.3 Other Applicable Legislation and Regulations

Not applicable.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

According to Microsoft, meeting's content and the models are automatically deleted immediately after each meeting. This data is not used or stored for improving its own.

AI Reference: https://techcommunity.microsoft.com/t5/microsoft-teams-blog/live-transcription-with-speaker-attribution-now-available-in/ba-p/2228817
MS Teams uses Azure Cognitive Services to optimize the speech recognition models using the NVIDIA Triton open-source inference serving software. Cognitive Services is available in the Canada Central region.

6.2 Analysis and Findings

This project is compliant with FIPPA and UBC's Information Security Policies.

6.3 Conditions of Approval

Risk Mitigation Plans should be followed. If, in future any changes are made to the scope of this PIA, a PIA update will be required.

6.4 Review and Distribution

This refers to the report approval process. The Owner is accepting the accuracy of the data provided to PrISM for this review and the risk responses. The Owner is responsible for the on-going operational activities and must ensure that this project continues to meet legislative and legal requirements, along with Information Systems Policy (SC14) requirements. Any change in PI collection or use will require new PIA.

Assessment Acceptance
Mark Belsito

This refers to the report distribution, including Requestor, Project Manager, Owner, and assigned Risk Advisor.

Distributed To
Requestor: Gordon Chan, Senior Systems Administrator
Project Manager: Gordon Chan, Senior Systems Administrator
Owner: Mark Belsito, Manager
Risk Advisor: Taylor Bohn, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2023-05-26 11:52:48	2023-06-23 15:16:12