VANDERBILT UNIVERSITY
Office of Cybersecurity

Vanderbilt Video Conference Recording and Sharing Guidance

The Office of Cybersecurity

Introduction

This guide provides clear and concise instructions for recording, transcribing, and sharing video conference sessions within Vanderbilt University.

It aims to protect participants' privacy rights, comply with legal and ethical standards, and foster a respectful and inclusive environment for learning and collaboration.

These guidelines apply to all Vanderbilt students, faculty, staff, and other participants involved in video conferencing sessions as a host or participant.

Ensuring the privacy, security, and integrity of recorded information is critical to safeguarding the trust and efforts of all concerned parties. You secure your and others' work by adhering to the guidelines.

Currently, the Vanderbilt-licensed solutions for video conferencing and transcription applications are:

- **Microsoft Teams**
- **Zoom**

Unique Use Cases

Other videoconferencing or transcription tools can be used in exceptional situations. However, Vanderbilt's Office of Cybersecurity must evaluate and approve them through the Vendor Risk Assessment (VRA) Process.

Additional Options

Alternative approved options are available for specific situations. Please contact the Office of Cybersecurity for more information.

Guidelines

1. Ethical and Legal Considerations

a. Purpose and Use of Recordings/Transcribing: Recordings and transcribing must only be used for legitimate academic or administrative purposes.
The intended purpose and use of the recordings and transcribing must be communicated to all participants.

b. Consent for Recording and Transcribing: All recordings and transcribing must be conducted with the explicit consent of all participants.
Consent may require verbal or written consent, depending on the context and sensitivity of the session. In cases where recording or transcribing is necessary (e.g., lectures for later review), participants must be informed beforehand.

c. Avoid Sensitive Information: Personal, financial, or confidential information should not be documented unless necessary.

d. End-to-end Encryption: Use end-to-end encryption platforms for video and transcript uploads and sharing. **Vanderbilt-licensed Zoom and MS Teams accounts have data encryptions by default for all recordings and transcripts stored online.**

e. Anonymize Content: Where appropriate, anonymize identifiable information within the video and transcripts.

f. Use Pseudonyms: Consider using pseudonyms instead of real names if the content is sensitive.

g. Compliance: Ensure compliance with laws and regulations regarding digital content where applicable. Please note that local authorities in some countries may not allow the communication tools approved by VU (such as Zoom and Teams) when traveling abroad.

h. Report Abuse: Know how to report privacy violations or security breaches on the platform.

    i. Report privacy violations or security breaches to VU Office of Cybersecurity by contacting cybersecurity@vanderbilt.edu. If the violation or breach is with Vanderbilt's Institutional Review Board approved research, please also report to the Vanderbilt Human Research Protections Program at (615) 322-2918 or Toll Free 1 (866) 224-8273.

2. **Transparency and Communication**
    a. Notification of Recording and Transcribing: At the start of the session, participants must be notified that the meeting will be recorded or transcribed. This notice should be verbal and displayed in the video conference chat or notification area—Vanderbilt-managed solutions. **Vanderbilt-licensed Zoom and MS Teams accounts have technical controls that comply with these requirements.**
    b. Inform Viewers: If you share educational or instructional content, inform your viewers about maintaining their privacy and security.
        i. When sharing educational or instructional material, it's crucial to advise your viewers on how to safeguard their privacy and security. It's important to ensure that your content includes recommendations on safe practices for engaging with online materials. Please remind your audience to protect their personal information and follow best practices for online security. This guidance aims to enhance the safety and security of your viewers as they interact with your content.
3. **Data Protection and Security**
    a. Storage of Recordings and Transcripts: Recordings and transcript files must be stored securely per Vanderbilt University's Data Classification Guidance. Access to saved files should be limited to authorized personnel and participants. **Vanderbilt-licensed Zoom and MS Teams accounts have technical controls that comply with these requirements.**
    b. Restricted Sharing: Only intended recipients should receive access to shared records or transcripts. Use features like passcode protection or shareable links with limited access.
    c. AI Assistance: Only use Vanderbilt-licensed MS Teams and Zoom-provided meeting recording and transcription AI assistance. For all other AI assistance with virtual meeting recording and transcribing, please go through the Vendor Risk Assessment (VRA) process.
    d. Verify Recipient Identity: Ensure you know who receives the video or transcripts.
    e. Secure Backup: Keep secure backups of your videos or transcripts. Note: Both VU-licensed Zoom and MS Teams accounts have auto backup enabled.
    f. Data Lifespan: Be aware of how long the video or transcript will be stored on the platform and what happens afterward. Note that the default length for Zoom cloud recordings is 112 days. All MS Teams and local recordings will remain saved until deleted.

g. Remove Metadata: Videos and transcripts often contain metadata like location, time, and device information. The use of tools to remove this metadata would be required to go through the Vendor Risk Assessment (VRA) process.

4. Education and Awareness

a. Take Training: Engage with the annual Cybersecurity training provided by Vanderbilt University.
b. Educate Yourself: Stay informed about potential risks and the latest best practices for online privacy.
c. Stay Vigilant: Protecting recorded information is crucial to shelter trust, privacy, security, and integrity.

----Please see the Best Practices below for additional instructions----

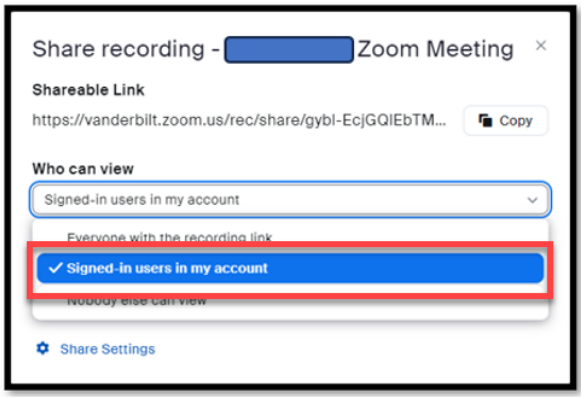
Zoom Recording Sharing

As mentioned in the General Guidelines, Vanderbilt-licensed Zoom has many technical security controls embedded in its configurations, such as encryption, access controls, and notifications. However, users are responsible for managing the access and sharing of recordings and transcripts (Note: when sharing recordings, transcripts are included in the sharing package).

Please follow the best practices listed below when sharing recordings.

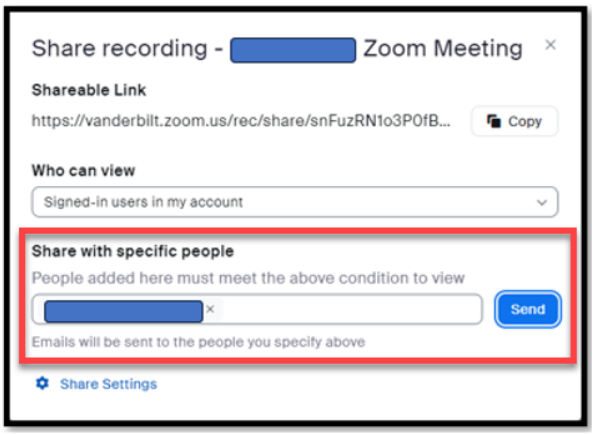
Change the default sharing settings to "***Signed-in users in my account***" from "***Everyone with the recording link.***" (Go to "***Recordings***"; when "***Share***" is selected, the selection box below will populate. Once this is changed, it will be the default setting from now on.)

As a default, this setting prevents links from being shared with people outside of VU.



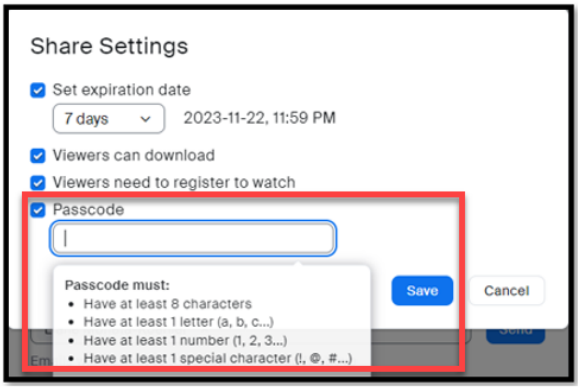
Always use the "***Share with specific people***" function when possible.

For people within VU, typing names will trigger a directory search. An email address will be required to share with people outside of VU.



Configure the "***Share Settings***" (expiration, download, passcode, etc.) with all desired settings.

When setting the passcode, consider complex and lengthy passcode.



Microsoft Teams Recording Sharing Best Practices

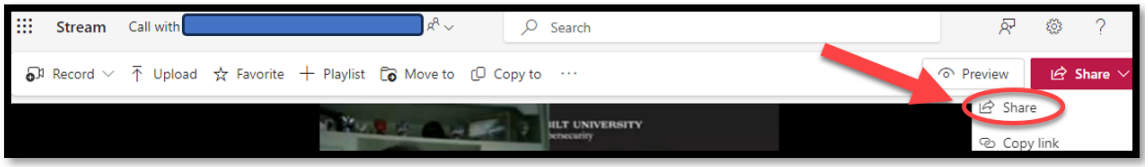
Like Vanderbilt-licensed Zoom accounts, MS Teams also has many technical security controls embedded in its configurations, such as encryption, access controls, and notifications. However, users are responsible for managing access and sharing recordings and transcripts. Please follow the best practices listed below when sharing recording accesses.

All MS Teams recording files are stored within the actual space where the meeting occurred (Individual, Meeting, or Channel chats). Recording files are stored either in the individual's **OneDrive** space under the "**Recordings**" folder of the person who clicks **'Record'** or in a **Teams channel** under Files > Recordings.

<u>It is not recommended</u> to share a recording file by copying the link (with the "Get link" option) since the default setting for meeting space copied link is "**Sharing with People in Vanderbilt**," which means all VU members would have access.

It is suggested that the "Share" function be used to share recordings in MS Teams.

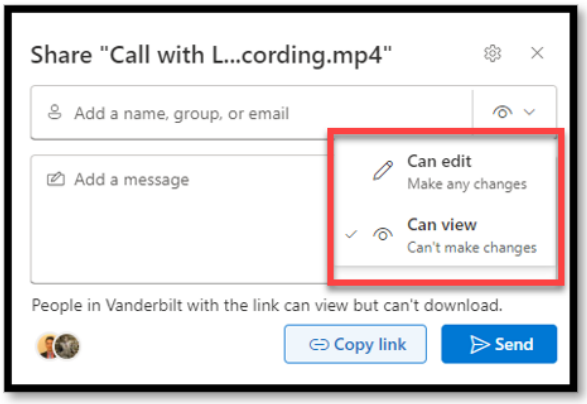
a. The "***Share***" function can be found in the upper right-hand corner of the "***Open in Stream***" window.



Sharing Recording - Permissions

When sharing your recordings with the "***Share***" function, ensure the "***Can edit***" or "***Can view***" option is set appropriately.

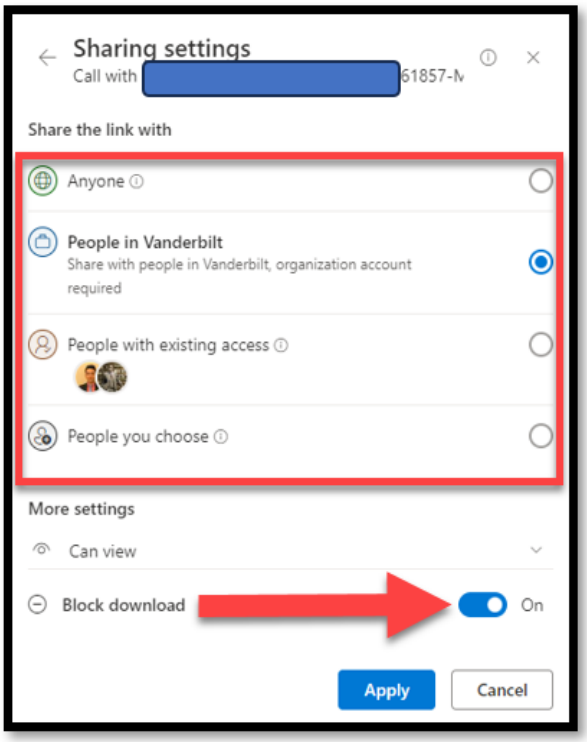
Note: "***Can view***" is the default in MS Teams.



In "**Sharing settings**," select the most appropriate option. Avoid selecting "**Anyone**" or "**People in Vanderbilt**" if unnecessary.

Ensure that "**Block download**" is set to "**On**" when you don't want others to download the recording.

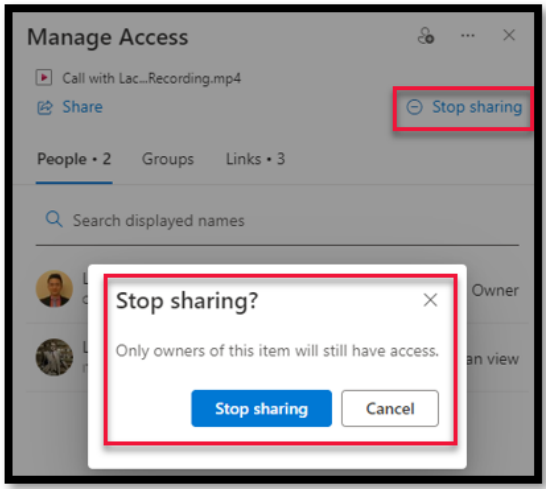
Note: This setting is set at "**On**" by default.



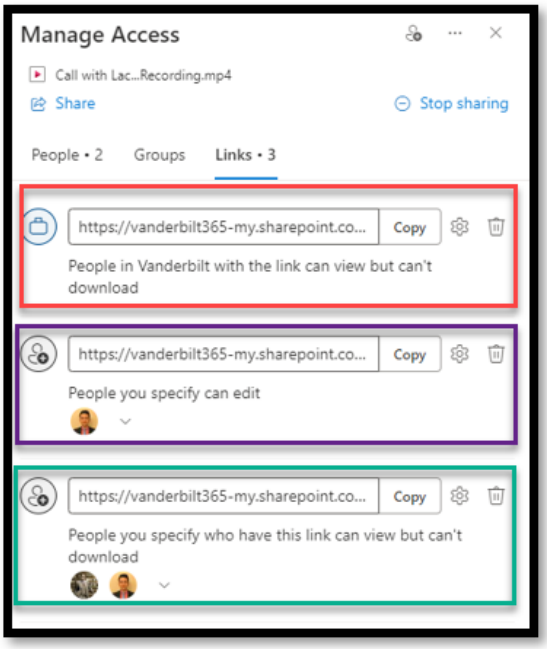
Managing Shared Access

We encourage all VU users to regularly use the "Manage access" function to confirm and manage MS Teams recording sharing details, especially when sensitive information is included or recordings are under regulatory requirements.

Within the **"Manage Access"** function, you can use **"Stop sharing"** to stop sharing with all parties you had previously shared with.



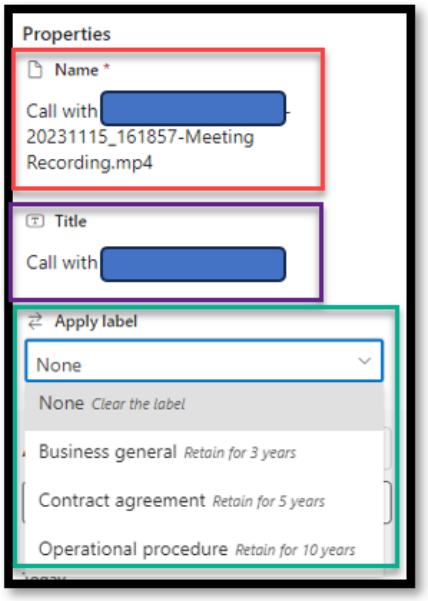
Also, the "**Manage Access**" function shows all "**Links**" created and shared with any parties. These settings can be viewed and configured in detail by selecting the setting function next to the links.



Accessing Recording Details

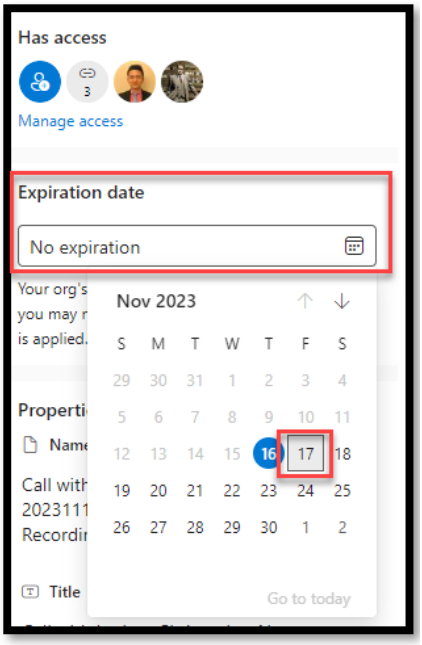
Recording details can be accessed and managed in an individual's VU OneDrive "***Recordings***" folder by selecting the ellipsis "**…**" icon. Information on the recording file will be shown on the right-hand banner of the OneDrive window.

The **Recording Name** and Title can be modified in "**Details**."



Labels can be applied to recordings as well. The default label is "**None**," and three other options exist.

The Expiration Date can be set or modified in the "**Details**" section.



For additional questions or comments, please get in touch with the Office of Cybersecurity

Last updated [3/26/2024]