# ZOOM SECURITY FOR DFV SERVICES

techsafety.org.au

*Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of June 2025.*

## Why this guide?

Zoom is a commonly used tool for video calls in many organisations, including domestic/family violencevictim services for survivors. It is often used within the organisation and when hosting calls with external parties (and may be used for features other than video calls). Sometimes, it is used to discuss confidential information, such as that pertaining to survivors. Zoom has changed a great deal since 2020, when many organisations began using it. This resource provides guidance, that is current as of June 2025, regarding data collection, data retention, and data security in Zoom.

In its desktop version (which includes laptops), Zoom saves chat logs and recordings in multiple locations:

- The meeting host's Zoom cloud account.
- Attendees' desktop Zoom apps. In this case, the data is being stored on users' actual computers, as opposed to the cloud.
    - Some of this data may also be stored in the Zoom or Zoom Apps C:\Users\[Username]\AppData\ folder (or macOS equivalent), but appears to be encrypted.
- A Zoom folder within your Documents folder. This is the case whether you use Windows or a Mac.

On mobile devices such as phones, Zoom only stores logs and recordings in the Zoom cloud account, in order to avoid taking up too much storage space on the device.

While many users are familiar with Zoom chat logs, users don't necessarily realise that logs and (if applicable) recordings are being saved in multiple locations, including both the cloud and their own devices. It may not occur to them to delete these once they no

longer need them. And even if they do delete them, they may be saved by other attendees.

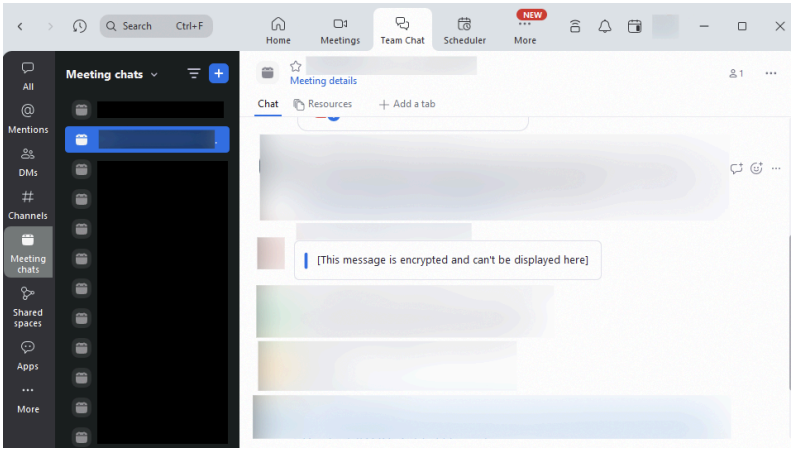
**Note:** If you're hosting a meeting, let attendees know beforehand if the chat or meeting will be recorded. This helps attendees make an informed decision about whether and how to participate.

## Settings Suggestions

### Encrypting comments by default

Encryption protects data so that only authorised people can view it. It scrambles the data so that only people who have the right electronic key can unscramble it. If you need an introduction to or refresher on encryption before reading this section, please see our Encryption Basics for Programs resource.

Zoom can be set to encrypt comments ("Advanced Chat Encryption"). Encrypted comments are viewable in the chat at the time, but are not viewable in later logs. The screenshot below (with sections blurred for privacy) shows an example of this. In this screenshot of a Zoom meeting's chat bar, taken by the meeting host after the meeting had ended, one comment is not viewable because it is encrypted. This comment was viewable by attendees during the meeting, but not in the logs afterward.




Encrypting your organisation's Zoom chat comments prevents them from later being

accessible through the files and Zoom accounts of other external and internal attendees. This measure is quick and easy to implement across your organisation. Only those with Zoom administrator privileges can turn this setting on (or off), and only those who implement organisational information security policies should have Zoom administrator privileges.

Enabling Advanced Chat Encryption will also disable the "continuous chat" feature, as discussed below.

## Disabling continuous chat

Most users think of Zoom chat as something that lasts for a meeting. Anyone who has hosted a Zoom meeting knows that Zoom does record chat logs in some way, because Zoom provides the logs to the host. However, Zoom has a feature called "Continuous Chat" or "Team Chat," whose name may be confusing. This feature allows attendees (including attendees from outside the hosting organisation) to continue to chat in the meeting chat and access the logs after the meeting has concluded. If someone unauthorised were to access the Zoom account of any attendee still in the continuous chat, that person would be able to read the logs, including ones from the meeting itself.

Users can leave these chats when they wish. Many users, though, do not realise that continuous chat exists. Given this, they may not realise they can leave the chat after the meeting. In addition, while any user can leave a continuous chat, only a host can *delete* the chat.

If staff are not using the continuous chat feature, it creates an unnecessary vulnerability, and it would be more secure to disable it. This requires administrator privileges. Enabling Advanced Chat Encryption, as described in this post by NNEDV, will also disable continuous chat.

## Disabling non-host recording

A Zoom meeting's host can disable the ability of other attendees to record a meeting without the host's permission. This could be a useful setting to check. Zoom administrators can change this setting for the entire organisation. It can be especially relevant for meetings with attendees from outside your organisation, to minimise the amount of

information they store from the meeting – remember that you have no control over the information security practices of outside organisations.

Live transcripts of meetings can be a vital accessibility measure. However, since transcripts are similar to recordings, Zoom meeting hosts and/or administrators may want to disable the ability of non-hosts to *download* transcripts without permission.

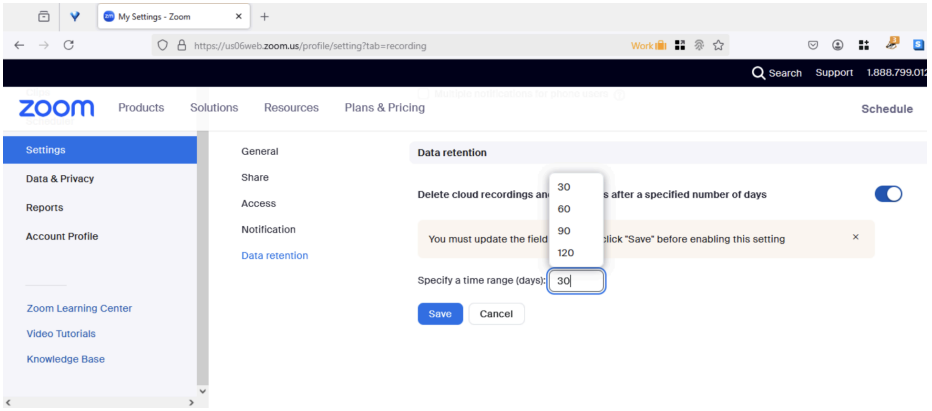
## Shortening the chat and recording retention periods

Account owners and administrators can set policies for how long Zoom chats are stored. This includes both:

- Storage on attendees' own computers (local storage). This is part of the Zoom app's data.
- Storage in the cloud. This is the data that you can access through the web portal.

The default retention period for Zoom cloud accounts is 2 years, and there is no default retention period for local storage. Both can be set by the administrator to any period between 1 day and 10 years. While being able to refer back to chat logs can be useful, this should be balanced with other concerns when deciding on the retention period.

The possibility of sensitive data being stored by Zoom is not an issue that can be addressed by Advanced Chat Encryption. Advanced Chat Encryption makes the messages themselves unreadable. It does not make metadata (data about the data) unreadable. The name of the meeting, the display names of attendees who post in the chat, and the timestamps of their messages, are still visible.



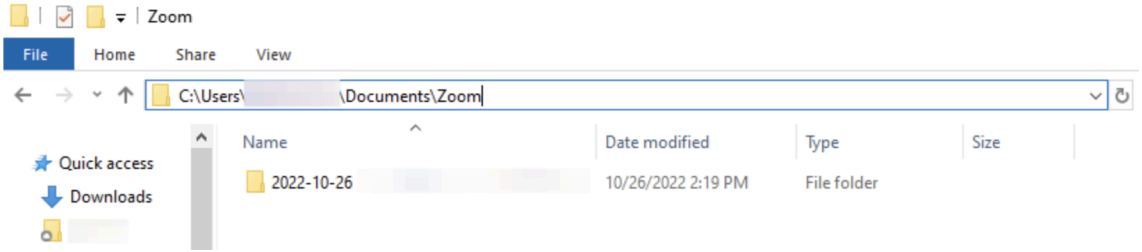

Shortening the retention period is especially useful because while any user can leave a chat or delete messages from a chat *on their own device*, chats can only be *deleted* by the owner.

Zoom does not delete recordings by default, as shown below, but it is possible to set a retention/deletion interval. This could be useful if a meeting that is not a webinar or similar is being recorded.

Changing this setting does not require an administrator account. However, an administrator can set a retention/deletion interval for all organisation accounts. This may be more straightforward and reliable than requiring each staff member to remember to change it.

## Automating the deletion of chat logs and recordings from organisation computers

When a Zoom meeting concludes, Zoom saves chat logs in folders on the meeting host's computer. These are saved in C:\Users\[Username]\Documents\Zoom on both Windows computers and Macs. The screenshot shown below illustrates what this looks like on a Windows computer. In addition, if an attendee records a meeting, this folder on that attendee's computer is where Zoom saves the recording.




Individual attendees can delete these logs from their computers. However, it may be more reliable and more time-efficient for administrators to do this in an automated way for all the organisation's computers. There are tools that IT providers can use to do this on both Windows-using and MacOS-using computers.

## Reviewing options for local backups

Some organisations automatically back up staff computers, so that the files can be restored if something happens to the computer. This includes any Zoom data, including logs, stored on staff members' computers. Your IT provider may consider how backups are stored, which information is stored, and for how long.

## Reviewing organisational Zoom settings periodically

Zoom changes its features and options regularly. Organisations may want to review their settings every so often to prevent excessive retention of potentially confidential/sensitive data. Your organisation does not control the information policies of other organisations. Therefore, you may want to consider whether non-host attendees at meetings that you host should be allowed to record or not.

## Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.