

Guidelines for students using Zoom in research interviews

These guidelines apply to all use of Zoom in research interviews with the collection of data classified as red according to [VID's classification of data and information](#).

This routine applies to all use of Zoom in VID where VID is data controller (“behandlingsansvarlig”) or responsible for the research project ([Procedure for processing personal data in research and student projects at VID Specialized University](#)).

[Provided by Uninett AS](#), Zoom complies with GDPR and Norwegian privacy legislation. Uninett's Zoom service is completely separate from the American public service and runs on a separate Nordic platform, which is safely designed for all its users in the knowledge sector.

VID has a separate [privacy policy for Zoom](#).

Requirements and recommendations

Planning and preparations

- Do not use the free or web version of Zoom. For security reasons, VID users must install Zoom and log in with their VID username and password.
- The equipment must be approved for processing red data according to [VID's storage guide](#).
- The person responsible for the conversation must familiarize themselves with and follow these guidelines.
- The person responsible for the call must ensure that all approvals are in place and follow VID's procedure for processing personal data in research and student projects.
- Note: If the conversation is carried out as a substitute for a physical meeting in a research project, it may be necessary to notify Sikt (formerly NSD) of the change.
- When planning the interview, make a careful assessment of the kind of data you will be dealing with. See [Classification of data](#) and the [storage guide](#).
- Check that you have downloaded the latest version of Zoom well before the meeting starts. In case of problems, contact the [IT Helpdesk](#).
- Familiarize yourself with Zoom as a tool and test that everything works without sensitive content. See the guidance for Zoom in [Canvas for students](#) (in Norwegian).
- Obtain consent and send good information to the participants in advance.

Zoom meeting creation and invitation

Always use the following settings when creating the meeting:

- For the meeting ID, select **Generate Automatically**, not Personal Meeting.
- Do not reuse passcodes for meetings.
- Under Security, activate the **Waiting Room** function.
- Activate **End-to-end encryption**. This provides the highest degree of security and must be activated when collecting red data.

Meeting ID

☒ Generate Automatically

☐ Personal Meeting ID 897 725 7510

Security

☒ Passcode 

Only users who have the invite link or passcode can join the meeting

☒ Waiting Room

Only users admitted by the host can join the meeting

☐ Only authenticated users can join: Sign in to Zoom

Encryption

☐ Enhanced encryption 

☒ End-to-end encryption 

Several features will be automatically disabled when using end-to-end encryption, including cloud recording and phone/SIP/H.323 dial-in. [Learn More](#)

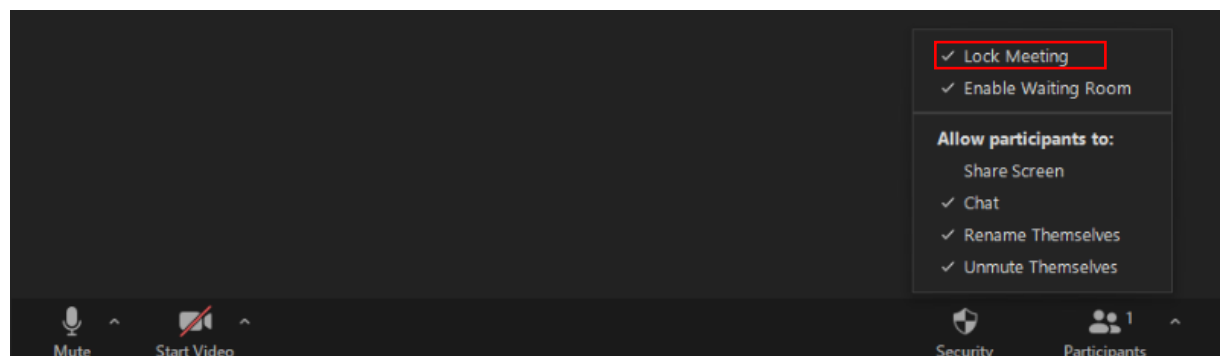
Save

Cancel

- Remove the option for participants to enter the meeting before the host. (Under **Advanced Options**, ensure that **Allow participants to join anytime** is unchecked.)
- Never post the link to the Zoom meeting with the meeting ID openly. Instead, convey it through e-mail, SMS or similar. If you send the link in Outlook, you must set the invitation as private.

Conducting a Zoom meeting

- Always ensure that no unauthorized person has access to the screen during the call or can overhear audio from the call. Use headphones where possible.
- If the interview concerns red data, you must always lock the meeting when all participants have entered. Click on **Security** and select **Lock Meeting**.

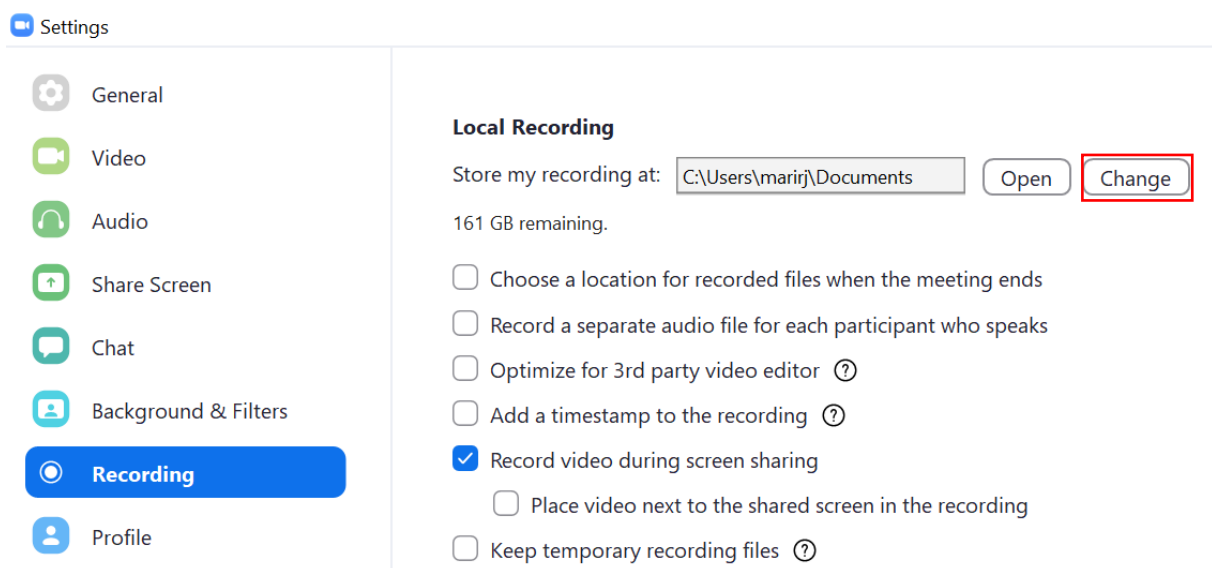


- Repeat information sent ahead of the meeting.

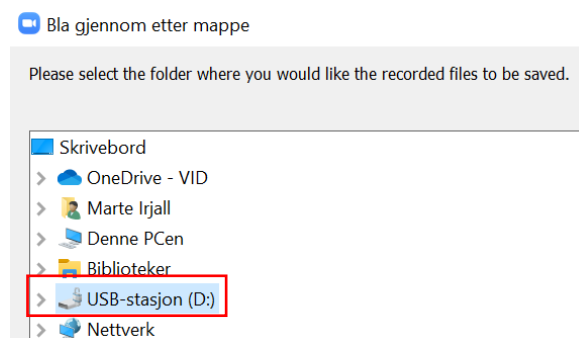
- If there are unauthorized persons inside the meeting, immediately end the meeting and notify your advisor.

Recording Zoom meetings

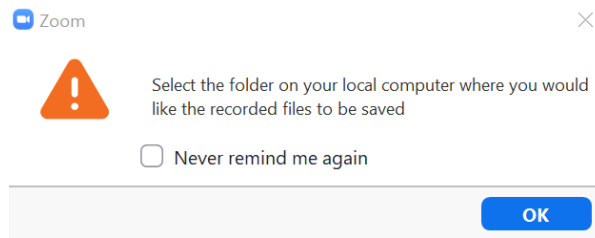
- Note that recording of red data in Zoom can only be done if a separate written risk assessment is made. VID's storage guide must be followed when saving recordings.
- If necessary, update any recording settings before the meeting starts.
- Red data must be stored on an encrypted memory stick or hard drive. See [instructions for encryption from IT](#).
- To save directly on an encrypted memory stick or hard drive:
- Go to your Zoom client and select settings.
- Under **Recording**, Select **Change** for **Store my recording at**.



- Select the desired storage device.



- Click OK on the message window that appears.



- You can record a separate audio file for each participant (**Record a separate audio file of each participant**).
- You can check the box for timestamping the recording (**Add a timestamp to the recording**), so that you can more easily edit later.
- Make sure that the temporary recording file is not saved (**Keep temporary recording files** should **not** be checked).
- If something happens or is said during the meeting that needs to be removed afterwards, note the time so that you can remove it more easily.