KEEP YOUR MEETINGS SECURE

By default, Zoom uses a 256-bit Advanced Encryption Standard (AES-256) for protect data and comply with FERPA requirements. In addition, educational institutions must further restrict entrance to all Zoom meetings.

Update the Zoom Desktop App

The first step to ensure secure meetings is to make sure that your Zoom desktop app is up to date and that you are using the app or the web portal to start meetings.

Use Unique Meeting IDs

Next, create meetings for every section of every course. For example, if you are teaching ENGL 110 at 9:00 am and at 10:00 am, each class time should have its own meeting ID.

Protect meetings by restricting entrance

To restrict entrance to meetings, two methods can be used separately or together. You can assign a password to each meeting and/or you can enable waiting rooms in every meeting.

Please Note: Mayville State University **requires** that you have **one** meeting ID **per class section** AND that you employ **password protection *or* enable the waiting room**. Also, do not post meeting information in public web spaces.

Pros and Cons of Passwords and Waiting Rooms

Use a Password

Pros: The password can be customized for each meeting. Do not use the same password for all your meetings as this reduces the security that the password provides.
Passwords can be safely shared in the Bb course with the Meeting ID.
Cons: As with all scenarios in which passwords are used, people can forget them, or people can give them out to others. Password management can be cumbersome.

Use a Waiting Room

Pros: Waiting rooms can be customized for each meeting so that students will know they are in the right place. If you are unsure about a user, you can place them in a waiting room.
Cons: Wireless connection issues can cause a lot of logging in and out of meetings. Often this is imperceptible with Zoom. However, it will become burdensome when the host has to admit people who lose connection during the meeting as they are logged out and back in again.

Respond to Inappropriate Behaviors

If, for some reason, your meeting is occupied by an inappropriate participant, you have at least two ways (described below) to minimize the potential damage.

Revoke sharing rights

Hosts have the option to allow screen sharing for only the host or for all participants. If someone is sharing inappropriate material, switch the setting to **Host Only**. This will immediately shut down the screen share.

Remove the participant from the meeting

In the Manage Participants area, hosts can hover over a participant name, click More… and chose Remove. The participant is notified that he or she has been removed from the meeting. The removed participant will not be able to enter that meeting while it is still running. If the meeting stops and starts back up again another time, that person will not be restricted from joining.