Security Guide for First Church Zoom Meetings

During “safer at home” time, First Church has implemented a video conferencing meeting application called Zoom to help our community connect with our church programs and groups. This guide outlines security settings that provide reliable and secure Zoom meetings.

YOUR HOME COMPUTER. Before you host or join a meeting, you should first review your home and computer setup and perform the following:

- Upgrade your computer operating system.
- Install or upgrade a computer security program (a virus and malware program.)
- Install the Zoom application from zoom.us/download.
- If you connect on WiFi verify your WiFi device requires a password or connect with an ethernet cable (the cable is a faster connection.)

ADVERTISING YOUR ZOOM MEETING. Meeting participants can join a meeting with either a URL link specific to your meeting on a Web browser, on their Zoom application using the specific Meeting ID, or on their phone. Inform your participants of your specific meeting information by email or on our closed First Church Facebook GROUP site. Do not advertise the Zoom meeting information in public places.

ZOOM MEETING PASSWORDS. Your meeting will be assigned a password if your group wants to allow visitors to join. When you share the participant joining information by email, the URL link includes the password (encrypted.) You can advertise this event on public sites with an RSVP to receive their email to share the password.

AUDIO & VIDEO TURN OFF. All meetings are set up with audio and video turned off. This will ensure that a participant is a real person operating with the connection.

WAITING ROOMS. Larger public meetings will be set up with a waiting room. A participant will join the meeting in a waiting room. The host will verify their identification and invite them into the meeting. The host can change the name of the person, turn on their video, and remove them if they are not welcome.

CO-HOST. For a larger public meeting, a co-host should be assigned before the meeting begins. A host can also assign a co-host during a Zoom meeting. This person can let people in from a waiting room, remove unwanted people, turn off their audio/video and manage other settings such as chat or sharing during the meeting.

LOCK YOUR MEETING. Once your participants are in the Zoom meeting, the host can lock the meeting so no one else will try to access the meeting. If a person needs to leave and come back, you should arrange to unlock when they return.

SCREEN SHARING. Meeting are set up with screen sharing available to HOST only. The host or co-host can turn this on but be wary if your meeting is public. Locking your meeting is a good policy before allowing people to share.

REGISTRATION. Any meeting can request registration to obtain their email and name. The participant needs to pre-register to receive the joining information with either the link or a phone number to attend the meeting.

This table indicated by X what security controls are the best practice for these types of meetings. The passwords, waiting room, and registration needs to be set up before the meeting begins. Co-host, lock, and participant controls are available during the meeting.

	Passwords	Waiting Room	Co-Host	Registration	Control Participants (e.g. share, chat, rename)	Lock Meeting
Small closed meeting					X	X
Small open meeting	X				X	After you start the meeting
Public meeting	X	X	X		X	
Webinar		X	X	X	X	