Information Security Guide

Zoom

COLUMBUS STATE COMMUNITY COLLEGE

Introduction

The following Zoom security protocols/practices are required for campuses, programs, academic departments, offices, faculty or staff that have or use a license to Zoom for any Columbus State related activities.

Note that Columbus State does not have an enterprise-wide license for this service. If you wish to use Zoom, check with your supervisor to determine that you have a license for its use.

Protocol	Required	Recommended
1. Don't share Zoom meetings on social media without additional security *	✓	
2. Set a password for all meetings	✓	
3. Don't use a Personal Meeting ID (PMI) to host a classroom or large event	✓	
4. Keep the Zoom app up-to-date	✓	
5. Use Waiting Room	✓	
6. Disable private chat		✓
7. Allow chat with host only		✓
8. Set Screen Sharing to Host Only		✓
9. Turn off annotation when not needed		✓
10. Turn off file transfer		✓

*Additional security settings: https://www.cscc.edu/employee/technology/it-security/zoom-security-and-privacy.shtml

Avoid Zoombombing

Zoombombing happens when uninvited guests join Zoom meetings with the intention of disrupting the meeting or sharing unwelcome content. Most of these are perpetrated through publicly available Zoom links, but that is not always the case.

Report Incidents

- **Report** zoombombings or other inappropriate activities to your **supervisor.**
- **Submit** an IT help request: **https://www.cscc.edu/ithelp. 614-287-5050.**
- For incidents that include suspicious activities:
  Contact Campus Police at **614-287-2525.**
- Report abusive behavior to zoom. **https://zoom.us/trust-form**