Technology Council May 2020
May 12, 2020

Action Item #SC01

TITLE: Zoom Security Settings – Video Conferencing Standard Operating Procedure

BACKGROUND:

The VCCS is required by VCCS Information Security Standard 13.2 to protect information by implementing formal policies, procedures, and controls for the exchange of information through the use of all types of communication media and resources including voice communications and video.

The VCCS has developed a Standard Operating Procedure (SOP) for securing video conference meetings and recorded meeting data in response to the recent demands placed on the use of Zoom video conferencing tools for both business and instructional use to prevent incidents where student privacy has been or may be compromised. The phenomena known as “Zoom Bombing” resulted in numerous incidents of disruption to classroom instruction and personal attacks on students by persons unknown who gained access to unsecure Zoom Video Conference Meetings.

This new Standard Operating Procedure SOP 13.2.1 - Securing Information Exchange Using Video Conferencing Services has been developed to require that video conference meetings be secured by default. Any changes to the security settings of a video conference meeting must only be made after careful evaluation by the meeting host. This new Standard has been reviewed and approved by the Technology Leadership Council, the College Information Security Officers, the Campus Technology Committee, the Security and Compliance Committee, and reviewed by eLet.

RECOMMENDATION:

The Technology Council Security and Compliance Committee recommends that the new Standard Operating Procedure SOP 13.2.1 - Securing Information Exchange Using Video Conferencing Services be adopted by the Technology Council as the minimum standard for securely hosting video conference meetings.

MOTION:

That the Technology Council endorse the new Standard Operating Procedure SOP 13.2.1 - Securing Information Exchange Using Video Conferencing Services and approve its adoption as the minimum requirements for hosting secure video meetings by voting in the affirmative to approve this Standard Operating Procedure.

RESOURCE PERSON:

Chair – Security and Compliance Committee
Bob Young, VP Instruction & Student Services
Blue Ridge Community College
(540) 453-2500
youngb@brcc.edu

Information Security
Standard Operating Procedure

13.2.1 – Communications Security

Securing Information Exchange Using Conferencing Services

Version: 1.4
Status: Published - 2012/05/05
Contact: Chief Information Security Officer

Purpose

This procedure details the minimum controls that must be implemented in conferencing applications in order to ensure the confidentiality, integrity, and privacy of communication services used to facilitate meetings, conferences, of provide a platform for classroom lecture, training or instruction. This includes audio, video, and text messaging services.

Implementation Guidance

Special instructions or conditions for using this procedure:

Information Security Standard 13.2 – Communications Security requires under sub-section 13.2.1 that the VCCS will protect information by implementing formal policies, procedures, and controls for the exchange of information through the use of all types of communication media and resources. Information exchange may occur through the use of a number of different types of communication media and resources, including electronic mail, voice, facsimile, text messaging, and video.

This document provides the procedures and controls that must be implemented as minimum controls to ensure the security of conferencing services such as Google Meet, Microsoft Teams Video Chat, and Zoom. Where controls are specific to one platform they will be so noted. This document will be updated as necessary to reflect the services provided by authorized services such as Microsoft Teams Video Chat, Google Meet, and Zoom Video Conferencing.

Any changes made to the default security settings should be carefully evaluated by the host to ensure that the safety and security of any video meeting participants will not be adversely impacted by changes being made. The meeting host assumes all responsibility for the safety and security of participants when the host makes changes to the default security settings.

Contents

Securing Information Exchanges Using Conferencing Services

Conferencing Services must be secured to ensure the confidentiality and privacy of communications between parties and to insure the integrity of the information exchanged. At a minimum the following requirements must be met when using various conferencing services to exchange information between persons both within the VCCS and external to the VCCS.

1) **Conferencing Services originating from within the VCCS, its colleges and agencies must be authorized for such uses by the VCCS CISO prior to implementation.**

   The VCCS Chief Information Officer must review security controls and provide approval for use of any conferencing services to initiate information exchange by persons employed by the VCCS prior to their use. This does not limit the participation of employees in conferences originated by persons outside of the VCCS but when participating in such conferences hosted by outside entities caution should be taken to avoid sharing any sensitive information during the conference.

2) **For all conferencing services the meeting Host or Organizer must:**
   - Secure all meeting access with a password
   - Use a restrictive invitation distribution mechanism for participants to control meeting access information. Hosts must not publish meeting invitations on public forums. Restrictive distribution mechanisms would include:
     - Canvas
     - Email
     - Short Message Service (SMS) text message
     - Instant Message (IM)
     - Direct phone call
   - Not include sensitive information in the meeting invitation
   - Control screen sharing by permitting the Host or a Co-Host to manage screen sharing
   - Not record confidential or PII information via Zoom screen share, chat or file transfer
   - Disable participant recording capability
   - Disable recorded meeting downloads by viewers
   - The Host must control the download and distribution of recorded meetings

Securing Microsoft Teams Video Chat

There are no specific recommendations at this time.

Securing Google Meet

There are no specific recommendations at this time.

Securing Zoom Video Conferencing

Zoom Video Conferencing is a preferred solution used to facilitate communications between VCCS faculty, staff, and students. The following security settings should be configured as indicated *when setting up a Zoom Meeting to insure the security and safety for all participants. "Enabled by default" and "Disabled by default" settings are configurable by the meeting Host. "Locked by admin" settings cannot be changed.*

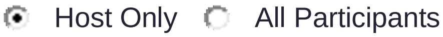
When Scheduling a Zoom Meeting

- Use authorized VCCS Zoom Accounts to schedule and host meetings
- Disable - Join before host (Disabled by default, also disabled when using a Waiting Room)
- Require a password when scheduling new meetings (Enabled by default)
- Require a password for instant meetings (Enabled by default)
- Embed password in meeting link for one-click join (Enabled by default)
- Mute participants upon entry (Enabled by default)

In Meeting (Basic)

- Require Encryption for 3rd Party Endpoints (H323/SIP) (Enabled by default)
- Chat (Enabled by default)
- Private chat (Disabled by default)
- File transfer (Disabled, Locked by admin)
- Screen sharing (Enabled by default, Host can allow others to share)

  Who can share?

  ● Host Only ○ All Participants

  Who can start sharing when someone else is sharing?

  ● Host Only ○ All Participants
- Disable desktop/screen share for users (Disabled by default)

In Meeting (Advanced)

- Give hosts option to report participants to Zoom (Enabled by default)
- Disable - Far end camera control (Disabled by default)
- Identify guest participants in the meeting/webinar (Enabled by default)
- Use Waiting room (Enabled by default)

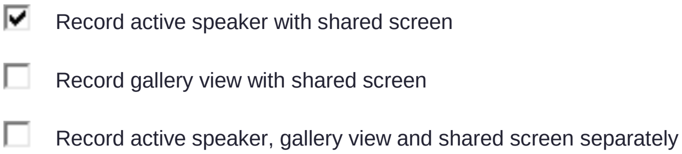
  Choose which participants to place in the waiting room:

  ○ All participants ● Guest participants only

  Do Not Allow internal participants to admit guests from the waiting room if the host is not present
- Show a "Join from your browser" link (Enabled by default)
- Disable - Allow live streaming meetings (Disabled by default)

Recording (Your Meeting)

- Disable - Local recording (Disabled by default)
- Cloud recording (Enabled by default)

  ☑ Record active speaker with shared screen

  □ Record gallery view with shared screen

  □ Record active speaker, gallery view and shared screen separately

  - ☐ Record an audio only file
  - ☑ Save chat messages from the meeting / webinar

- Advanced cloud recording settings
  - ☐ Add a timestamp to the recording
  - ☑ Display participants' names in the recording
  - ☐ Record thumbnails when sharing
  - ☐ Optimize the recording for 3rd party video editor
  - ☐ Audio transcript
  - ☐ Save panelist chat to the recording
- Disable - Automatic recording (Disabled by default)
- Disable - IP Address Access Control (Disabled by default)
- Only authenticated users can view cloud recordings (Disabled by default)
- Disable - Require password to access shared cloud recordings (Disabled by default)
- Disable - Auto delete cloud recordings after days (Disabled by default)
- The host can delete cloud recordings (Enabled by default, Locked by admin)
- Recording disclaimer (Enabled by default)
  - ☐ Ask participants for consent when a recording starts
  - ☑ Ask host to confirm before starting a recording
- Multiple audio notifications of recorded meeting (Enabled by default)

Share This Cloud Recording

- All settings determined by the host

Implementation Guidelines

- Encourage students, faculty, and staff to authenticate by logging into their VCCS Zoom or Canvas account prior to joining a meeting session. Authenticated users do not have to wait in the meeting room but will be immediately joined to the meeting when started by the Host
- The Host will control the admission of all Guest participants (all unauthenticated users)

Open Zoom Meeting Rooms

- The use of open Zoom Meeting Rooms for purposes such as student recruitment or advising is restricted to uses where the Zoom Waiting Room is monitored by the Host during specific hours only. All such uses must be approved in writing as an exception to this standard by the Agency Head and the CIO. Links to open Zoom Meeting Rooms must use an embedded password in the meeting link, the Host must require the Zoom Waiting Room for all participants, screen sharing must be controlled by the Host, and the meeting must not be recorded.

REVISION HISTORY

Date	Version	Reviewer	List of Changes
2020-04-08	1.0	J. Skinker	Initial Draft
2020-04-14	1.1	J. Skinker	Incorporated VITA recommendations for Zoom Meetings
2020-04-29	1.2	J. Skinker	Incorporate eLet, Campus Technology, and Security and Compliance Committee revisions into draft document for Zoom Meetings
2020-04-30	1.3	J. Skinker	Format requirements to correspond to screen settings in the Zoom Application
2020-05--5	1.4	J. Skinker	Added setting status definitions, Open Zoom Meeting exception to the standard.
2020-05--12	1.5	J. Skinker	Reworded to indicate downloads by viewers must be disabled, clarified that authenticated users accounts include Canvas accounts, clarified that Open Zoom Rooms can occur during specific hours monitored by a host. Removed all caps lettering from the word Zoom.

Final Approval

Date	Name	Position