Security and data protection for web conferencing

06 May 2020

Contact:
digitale-lehre@uni-konstanz.de

www.uni-konstanz.de/elearning
1. General recommendations for secure web conferencing

The University of Konstanz recommends four different web conferencing tools for various application scenarios. As is customary with these tools, none of these tools uses end-to-end encryption (E2EE). The university holds licenses for the commercial systems Zoom and Cisco WebEx, for which data protection policies are currently being finalized for approval.

**Big Blue Button**
- An open-source application, the server is hosted locally at the University of Konstanz
- Recommended for teaching and meetings with confidential information, including personal data
- Can be directly integrated into ILIAS
- Permanent KIM service
- Runs directly in the browser of your choice; there is no app
- Login with your university account

**Cisco WebEx**
- A commercial system with servers in the European Union
- Recommended for teaching and meetings, especially when using a large amount of video content
- Licensed for one year
- Runs directly in the browser or in the WebEx app (the latter has better functionality)
- Login with your university account

**DFNconf**
- Service of the German National Research and Education Network (DFN), server in Germany
- Recommended for teaching and meetings
- Permanent DFN service
- Runs in the browser of your choice
- Login with your university account

**Zoom**
- Commercial system; the university uses servers in Germany, Austria and Switzerland for spoken content; servers in the US for meta data
- Recommended for teaching and meetings, especially when using a large amount of video content; please read the privacy policy carefully beforehand
- Licensed for one year
- Runs in the browser of your choice. Based on information currently available, use of the Zoom app is not recommended for IT security reasons
– All licences are provided centrally by the KIM (one licence per chair).

Generally, we recommend using either Firefox or Chrome. [https://www.kim.uni-konstanz.de/en/services/research-and-teaching/video-conferences/](https://www.kim.uni-konstanz.de/en/services/research-and-teaching/video-conferences/)

### 1.1. Recommendations for teaching staff

1. Please use video conferencing systems only on trusted devices. Only install additional software if absolutely necessary. If possible, use a device dedicated only for this purpose and that is not used to process critical data.

2. Make sure that all software applications are up to date: operating system, browser, and app. Please also note current information about security loopholes (information security management). If critical security warnings are issued, you should not use Zoom, even if this poses a limitation to your planned meetings.

3. Please also use a specific, secure password for each conference (see password guidelines of our IT team).

4. Do not use conference rooms twice. There should be a specific link for each course/meeting.

5. You may share access data only via secure and known channels (e.g. as information in your ILIAS course).

6. Before starting the videoconference, check the visible background in the camera view and make sure no personal items can be seen.

7. Make sure the data protection information as per article 13 GDPR is available and, if applicable, get the consent of your participants.

8. During the videoconference, audio and video recording must be disabled. Recording is only permitted if there is the corresponding legal basis. The explicit and documented consent of all participants might be required. You have to inform all participants about the planned recording. Please be aware that unauthorized eavesdropping or recording of the privately spoken word is a punishable offence (§ 201 StGB (German criminal code)).

9. By default, the microphone, camera and screensharing features of your participants should be disabled. The participants must explicitly and voluntarily agree to use these features. Ask your participants if they want to participate in the videoconference with their cameras activated and point out possible alternatives.

10. Please make sure that there are no unauthorized observers in the room.

11. Use a LAN internet connection for the videoconference, if possible.
1.2. **Recommendations for students.**

1. Please use videoconferencing systems only on trusted devices. Only install additional software if absolutely necessary. If possible, use a device dedicated only for this purpose and that is not used to process critical data.

2. Never share access data; it is for your personal use only.

3. If you receive links to conferences or software/apps, please carefully check the origin and linked content (phishing, scamming, hijacking).

4. Only install software/apps from trusted sources. Preferably you should use the browser instead of an app-version. This may lead to limitations in the functionality of the tool. Use the WebEx app only if you absolutely need certain features (such as “raise hand”, the whiteboard in the Cisco desktop app or in the mobile WebEx app, or the “grid view”).

5. When joining a meeting, make sure that your microphone, camera, and screen sharing are turned off. Activate these features only when necessary. Do not feel compelled to share anything.

6. Before starting the videoconference, check the visible background in the camera view and make sure no personal items can be seen.

7. If you do not want to disclose any personal information at all, we recommend you use a disposable email address created in our system void.uni-konstanz.de. This will identify you as a member of the university, but you can use a pseudonym. Create a new disposable email address for each new conference.

8. Do not make audio recordings, video recordings or screenshots (unauthorized eavesdropping or recording of the privately spoken word is a punishable offence (§ 201 StGB - German criminal code)).

9. The videoconference may only be recorded if you have been informed accordingly and given your consent. Otherwise the university will not record any conferences. However, always carefully consider what you say, write and show to others.

10. If possible, use a LAN internet connection for the video conference.

11. If you are coerced against your will to share personal data or share audio/video/screen, or if you have reasonable suspicion that you have been recorded without your consent, please contact the university’s Data Protection Officer immediately (datenschutzbeauftragter@uni-konstanz.de).

2. Recording of videoconferences

From a legal standpoint, unauthorized audio or video recordings of videoconferences are prohibited (unauthorized eavesdropping or recording of the privately spoken word is a punishable offence (§ 201 StGB - German criminal code)). Unauthorized audio or video recordings violate both personal rights and the right to one’s own image. As the moderator of a web meeting, please make your participants aware of this before starting the meeting.

For data protection purposes, the option of recording video conferences on BBB has been deactivated by default on the university’s servers. However, as Cisco WebEx and Zoom are commercial systems, audio recording/video recording cannot be turned off or prevented. Therefore, if you plan on recording a session, you must receive the consent of each individual participant beforehand – it does not matter whether the moderator or one of the participants does the recording. The same applies to screencasts.

3. Recommendations for the Zoom system

We would like to draw your attention to the special features when using Zoom.

Due to the high demand for a stable alternative system, the University of Konstanz decided to purchase licenses for Zoom for one year. However, additional security instructions must be followed which apply in addition to the information for the other systems:

– Zoom is a commercial software programme offered by a company based in the United States. The metadata (i.e., who meets with whom and when) is stored on worldwide servers without taking into account the GDPR in force in the EU.

– All content that is communicated using Zoom via text, image and video is transmitted within the scope of the University of Konstanz’s license with the provider C4V on servers in Germany, Austria, and Switzerland. The provider does not have GDPR certification but is subject to the provisions of the GDPR.

– In plain language, this means: Do not use Zoom for conversations that contain sensitive and/or personal information, such as exams, confidential conversations, or office hours. Thus, only use Zoom for public conversations.
3.1. **Notes for teachers / moderators**

1. Please use videoconferencing systems only on trusted devices. Only install additional software if absolutely necessary. If possible, use a device dedicated only for this purpose and that is not used to process critical data.

2. Make sure that all software applications are up to date: operating system, browser, and app. Please also note current information about security loopholes (information security management). If critical security warnings are issued, you should not use Zoom, even if this poses a limitation to your planned meetings.

3. Select or generate your own individual password for each meeting (→ see the university’s password instructions)

4. Create a new meeting for each time slot or at least for each course (new ID, new access data) and do not reuse a previous meeting link.

5. Provide the link to the meeting/meeting ID with the password via secure channels previously announced to a closed group. For example, in an ILIAS course. Do NOT share access data via public channels (social media, public website)

6. Clearly and unambiguously urge students to not pass on access data to others.

7. By default, the following settings must be activated for all Zoom meetings:
   - Participants’ microphones are disabled
   - Participants’ cameras are disabled
   - Far-end camera control is disabled
   - Screen sharing by the participants is disabled
   - Remote control of screen sharing is disabled
   - Remote support is disabled
   - Attendee attention tracking is disabled
   - Recordings are disabled
   - Notification of the host when participants join before the host is disabled
   - Automatic notification of participants in the event of cancellation of a meeting is disabled
   - Sending emails via the ZOOM website is disabled
   - Sending feedback to ZOOM at the end of a meeting is disabled

8. Participants may not be forced against their will to share personal data or share their audio/video/screen. The meeting may only be recorded if the explicit consent of all participants has been received and documented beforehand. If the number of participants who grant consent is less than the overall number of participants, the meeting may not be recorded.
9. Dealing with subsequent access to the meeting room:
   - The “waiting room” feature can be used for latecomers.
   - The “block meeting” feature can be used to prevent further access if this is desired.

10. Participants should only be asked to give their name if this is necessary for the course/event.

11. If participants are disruptive or cause disturbances, you can mute their microphone.

12. When the link to the room is sent, we recommend that you adjust the URL as to encourage participants to access the room via a web browser. (https://zoom.us/j/{id} to https://zoom.us/wc/join/{id}). If the link is not sent manually (i.e. via an automated invitation email), we recommend activating the corresponding option so that connecting via web browser is at least suggested.

13. Consider whether you need certain features such as “file transfer” and configure the settings accordingly.

14. Disable “join before host”.

### 3.2. Notes for students / participants

- If prompted to install the client, reject this and click “Join from your browser” instead.