Security Guidelines for ZOOM Users

ZOOM has been well received by many Universities and schools worldwide, given its features, stability, and low technical threshold. Hence, during the class suspension period, SPCS has adopted ZOOM as the platform to support synchronous teaching and learning as teachers find this an easy to use tool. However, because of the recent concern on its security issues, we recommend the following suggestions to both teachers and students.

1) All teachers are advised to follow the best practices suggested by ZOOM for online classes:
   - Set up a Waiting Room
   - Remove uninvited participants
   - Disable join before host
   - Manage annotation. Prevent participants from screen sharing during teacher's presentation
   - Close the meeting immediately and eject all participants if there are intruders or hacker activities.

Details: https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/

2) Never share sensitive information @ online meetings.

3) Never disclose the Meeting ID or meeting link on social media or publicly.

4) Never open any malicious links and files.

5) ZOOM clients/app must be updated to the latest version.

6) Cover the webcam when not in use.

7) Protect computers and devices using anti-virus and anti-malware software. Keep the software and the virus pattern updated.

8) Keep a close watch of any unusual activity on ZOOM client/app, the account and the device which you use to join ZOOM meetings. Document and report to the IT technician / co-ordinator ASAP for further follow up with the company.

9) The school will continue to support teachers on the use of ZOOM with its set up in the 1st, 2nd, 4th & 5th floors of the classrooms for those who wish to use ZOOM from school.

10) Further development and new recommendations will be provided when necessary.