Guidelines to strengthen security with VidyoConnect platforms used for Desktop VC solution.

VidyoConnect technology can be used in the following ways by users:

a. **Private meeting room links**- The private meeting room links are owned by individual registered users. The meeting links and access code (pin no) can be changed by the owner of the room.

b. **Public meeting room links** - The public meeting room can be associated with registered users, who will have permission to change public meeting links and access code.

c. **Schedule meeting room links** - This kind of meeting can be scheduled by registered users. Multiple meeting links can be created for different meetings with correspondent access code. The meeting link expired after some period, once meeting is over.

The following are the mandatory actions to follow to strengthen the security with VidyoConnect platform:

- Every scheduled meeting link will have a mandatory access code.
- The meeting of any kind individual/public meeting should not be published on the internet or any website.
- The meeting link should be created with a mandatory access code and shared with the meeting link.
- The meeting link should be changed by the user for every meeting and on regular basis. It is advised that the meeting room link should be changed after the completion of the meeting to avoid any possibility of misuse of the room link in the future.
- Once the meeting is started, it is suggested to lock the room so that no one can further enter during the meeting.
- Before the start of any discussion, Admin/Moderator must ensure that only intended/ authenticated participants have joined the meeting.
- It is requested to avoid clicking on the links shared during virtual meetings/classes without confirming the source(s) as they might be phishing links.

Note: The static web room links of reserve portal will be withdrawn soon by dynamic link with mandatory access code option.