Dear all,

There has been more warning and replay of the concern and risk with using zoom and its reached levels where governments too have had to take notice and act. As a platform, the product owner has taken commendable steps to address the issues. But as a guideline for business use internally , please follow this –

A. Use the corporate accounts for sensitive business communication. We have enabled the possible security configurations at the account level itself.

B. As much as possible avoid using BASIC and Open account for critical business communications.

   a. In case you are using it, please make sure the steps outlined below are taken to secure the meeting.

Recommended security configurations:

1. *Setting new user ID and password for each meeting*
2. *Enabling waiting Room, so that every user can enter only when host conducting meeting admits him*
3. *Disabling join before host*
4. *Allowing Screen Sharing by host Only*
5. *Disabling "Allow removed participants to re-join"*
6. *Restricting/disabling file transfer option (if not required)*
7. *Locking meeting, once all attendees have joined*
8. *Restricting the recording feature*
9. *To end meeting (and not just leave, if you are administrator)*

For your reference here is the full [Link to the MHA Advisory on Secure use of ZOOM Meeting Platform](#).