Dear Colleagues,

With the unfortunate actions taken by some to hijack Zoom sessions, Zoom has made global security changes to their application, which will affect how meetings will occur in the future.

Zoom has enabled the **Waiting Room** feature and some **additional password settings** for all Basic user accounts. They also now **require a password for Personal Meeting ID (PMI)** use. These settings are designed to prevent unwanted participants from joining your meeting or course.

To further block against attacks, it is highly suggested that meeting hosts:

- Set a password for every Zoom session.
- Use meeting settings to prohibit screen-sharing by anyone other than the individual hosting the meeting.
- Do not share a link to a teleconference or classroom on a publicly available social media post. Provide the link directly to invited participants.
- Turn off video for participants upon entry.
- Lock the meeting right after it starts to ensure that only authorized participants are in the meeting and remain in.

Daemen IT has created a How Do I? article on How to Secure a Zoom Meeting in regards to these concerns.

With the Waiting Room feature enabled by default now, the host of the meeting will need to Admit or Remove entry to each participant. Our How Do I? article on How to Host a Zoom Meeting has been updated to include these steps.