ASLP-IC Zoom Policies and Procedures

Effective Date: August 20, 2025
Last Reviewed: August 20, 2025
Next Review Date: February 20, 2026, or as indicated by the Commission Secretary, Executive Director, or Legal Counsel

1. Purpose

The purpose of this policy is to establish security and privacy protocols for all Zoom meetings, webinars, and virtual engagements conducted under the authority of the ASLP-IC Commission. This ensures the confidentiality, integrity, and protection of information shared in virtual environments, as well as compliance with best practices.

2. Scope

This policy applies to all ASLP-IC Commission Executive Committee members, ASLP-IC Committee members, contractors, and external participants who attend and host Zoom-based meetings or events hosted by the ASLP-IC Zoom account.

3. Zoom Policy

3.1 Zoom Account Use

- All Commission-hosted meetings must use official, Commission-issued Zoom accounts.
- Personal or third-party Zoom accounts may not be used for official Commission business.

3.2 Meeting Settings

All Zoom meetings must be configured with the following settings by default:

- **Registration:** Enabled for all official Commission meetings.
- **Waiting Room**: Enabled for all meetings.
- **Meeting Passwords**: Required for all scheduled meetings.
- **Screen Sharing**: Restricted to hosts/co-hosts unless explicitly allowed.
- **File Transfer**: Disabled by default.
- **Join Before Host**: Disabled.
- **Mute Participants Upon Entry**: Enabled.
- **Chat Controls**: In-meeting chat may be limited or disabled for sensitive or closed meetings.
- **Participant Renaming**: Disabled to ensure identity integrity unless explicitly allowed or requested by the Host.
- **Participant First Name and Last Name**: Required for registered meetings.

3.3 Meeting Roles and Access

- Designate a **Host** and at least one **Co-Host** for each meeting to assist with minutes and participant entry/exit.
- Only authorized personnel may schedule or manage Zoom meetings on behalf of the Commission.

3.4 Privacy Protections

- Video/audio recordings must only be made with consent from all participants and stored in a secure Commission-approved cloud or local storage.
- No meeting may be recorded without informing all attendees at the start of the session.

3.5 Security Protocols

- Zoom software must be kept updated on all Commission-managed devices.
- Links to Zoom meetings should never be posted on public websites or social media without appropriate access restrictions (e.g., registration, authentication).

3.6 Use of AI Features in Zoom

- The Commission prohibits the use of AI-powered features within Zoom (such as AI Companion, meeting summarization, smart recording, or real-time transcription powered by AI) unless explicitly approved by the Commission Chair, Executive Director, or the Commission Secretary.
- AI-generated content (e.g., meeting summaries or action items) must be reviewed before being shared or stored.

4. Responsibilities

Role	Responsibility
ED/NCSB Host	Configure and manage Zoom security settings.
Meeting Organizers	Schedule and manage Zoom sessions in compliance with this policy.
All Participants	Follow the Commission's Zoom security and privacy protocols.

5. Review and Revisions

This policy will be reviewed annually or as necessary to accommodate changes in technology, regulations, or organizational needs.

6. References

- Elmer, G., Neville, S. J., Burton, A., & WardKimola, S. (2021). Zoombombing during a global pandemic. *Social Media + Society, 7*(3). https://doi.org/10.1177/20563051211035356
- Meena, B. S., Ranjan, R., and Anand, S.K. (2023). Virtual Meetings Under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era. *Journal of Visual and Performing Arts, 4*(2), 1256–1263. https://doi.org/10.29121/shodhkosh.v4.i2.2023.3047
- Zoom Resources for Virtual Meetings