

Running Secure Microsoft Teams Meetings

Ash Nathaniel
NCDIT – Enterprise Collaboration Services

Oct 06, 2026

Secure Any Teams Meeting with 3 Key Option Setting

- **Selection of Lobby (virtual door) based on Meeting Type**
- **Role of Organizer/ Co-Organizer (Presenter)**
- **Content**

Setting these three options in Meeting Options prevents 95% of accidental disruptions and provide better security.

Match Your Settings to Your Audience

- **Daily Team Standup** - Open for teammates within the organization
- **Vendor & Partner Meeting** - Lobby (virtual door) for outside guests
- **Executive Strategy Session** - Strict access for leadership sessions.



Who Waits at the Virtual Door?



People in My Org

Colleagues join instantly.



People I Invite

External guests wait for admittance.



Only Me

Complete entry control for organizers.

Presenters' vs Attendees

ROLES & PERMISSIONS



Presenter Powers

Screen Broadcast: Share slides, apps, or whiteboard

Lobby Admittance: Let guests into the call

Recording Start: Trigger cloud meeting capture



Attendee Experience

Screen Guard: Cannot accidentally hijack the presentation

Organized Audio: Muted until recognized by host

Focused View: Can chat and raise hand politely

Recommended Settings by Meeting Type

ORGANIZER CHEAT SHEET

Meeting Type	Lobby Bypass	Presenters	Recommended Setting
Ad-Hoc ("Meet Now")	People in my org	Everyone	Never share confidential files in quick chat
Standard Team Sync	People in my org	Specific people	General / Internal sensitivity label
External Partner / Client	People I invite	Specific people	Disable attendee mic until Q&A
Town Hall / Broadcast	Attendees bypass	Co-organizers only	Moderated Q&A

Mastering Ad-Hoc Calls & Town Halls

Ad-Hoc ("Meet Now")

Link Discipline: Never reuse old links for sensitive topics

Guest Inspection: Glance at attendee tray upon starting

Chat Leak Trap: Files dropped stay in persistent chat

Town Hall Format

Green Room: Rehearse privately before going live

Moderated Q&A: Review questions before publishing

Hard Shield: Attendee mic and camera locked off

Running Meetings Inside a Teams Channel

✓ Key Advantages

Centralized Records: Chat, files, & notes stay in the channel

No Lost Invites: Team members join straight from the posts feed

Async Catchup: Absent members easily watch the recording

⚠ Security Drawbacks

No Topic Privacy: All channel members can freely drop in

Future Members: New team hires see past meeting chat and files

Unsuitable for 1-1: Never hold confidential reviews in open channels

Where Does Your Meeting Data Actually Live?

DATA STORAGE ARCHITECTURE



Chat & 1:1 Meetings

Sender's OneDrive: Files upload to your "Teams Chat Files" folder.

Recordings save to recorder's personal OneDrive.



Channel Meetings

Team SharePoint: Files save directly in the Team site library.

Recordings save to Channel's "Recordings" folder.



PowerPoint Live

Streamed in Memory: Slide deck renders through Teams securely.

Attendees cannot download local deck copies.

Meeting Data Hygiene Best Practices

DIGITAL HYGIENE



Recording Sharing: Ensure cloud recordings share permission are removed



Prune Guest Links: Check OneDrive shared links to revoke expired external project access



No Unmanaged Chat Drops: Share SharePoint links with view-only instead of raw file attachments

How to Share Slides

SCREEN SHARING BEST PRACTICE



Comparing Sharing Modes & Bandwidth

PERFORMANCE & PRIVACY



PowerPoint Live

Lowest Bandwidth (~85% Less)

Vector Stream: Sends slide text without heavy video encoding

Private Notes: Presenter notes stay hidden from audience

Crisp Display: Zero blurriness on poor Wi-Fi connections



Single App Window

Moderate Bandwidth

Targeted Frame: Transmits only the selected application

Toast Blocker: Outlook reminders remain invisible

Multitask Safe: Host can review private notes behind app



Full Desktop Screen

Highest Bandwidth Load

Heavy Stream: Constantly encodes full monitor resolution

Notification Trap: Personal messages pop up live

Lag Vulnerability: Freezes easily on constrained mobile data

POWERPOINT LIVE: ADVANCED PRESENTER CONTROLS

HOST SUPERPOWERS



Private Notes

Discreet speaker prompts on screen.



Navigation Lock

Prevent attendees skipping ahead.



Slide Grid View

Jump to any slide instantly.



Live Inking

Real-time virtual laser guidance.

Best Way to Present Video in Large Meetings

MEDIA OPTIMIZATION

Audio Setup

Include Sound Toggle: Enable computer audio before sharing

Direct Stream: Avoid mic picking up laptop speakers

Green Room Test: Verify audio volume with co-hosts

Bandwidth & Smoothness

PowerPoint Embed: Slides buffer video locally for smooth play

Turn Off Incoming Video: Conserve host bandwidth on large calls

Wired Ethernet: Prevents Wi-Fi packet jitter during clips

Handling Disruptions in Under 10 Seconds

IN-MEETING CONTROLS

STEP 01

Mute All

Silence background noise instantly.

STEP 02

Stop Video

Turn off participant cameras.

STEP 03

Remove User

Eject uninvited attendees immediately.

STEP 04

Lock Meeting

Prevent new participants from joining.

Preventing AI Bots & Unauthorized Notetakers

AI GOVERNANCE & PRIVACY



Lobby Gatekeeping

Never click "Admit All".

External bots always stop in the lobby queue.



Lock Recording

Organizers only.

In Meeting Options, restrict recording & transcription to co-hosts.



Spot & Eject

Scan attendee tray.

Look for "Notetaker" or "Assistant" handles; click "Remove from meeting".



Protect Content

Review Content / Apps

block unapproved apps and untrusted audio scrapers.

You vs. Vendor: Why Host the Meeting

MEETING OWNERSHIP

You Host (OurTenant)

Data Sovereignty: Our organization owns all recordings and transcripts

Lobby Gate Control: You decide which external guests enter

Host Override: Power to mute, eject, or end call for everyone

Vendor Hosts (Their Tenant)

Lost Data Rights: Vendor retains and governs recording files

Open Lobby Door: Vendor decides who joins the session

Uncontrolled Bots: Vendor may allow third-party transcription AI

"Leaving" vs "Ending" the Meeting



Clicking "Leave" (Risky)

Only removes you. The call bridge remains alive.

- External guests can linger unmoderated
- Cloud recording continues if active
- Participants can continue sharing files



Clicking "End Meeting" (Best Practice)

Red button arrow > "End meeting for everyone".

- Immediately disconnects all participants
- Instantly stops and compiles the recording
- Prevents unsupervised post-meeting banter

SECURE COLLABORATION

Keep Every Meeting Trusted & Protected

Questions, scenario walkthroughs, or specialized meeting support.



Thank You

Ash Nathaniel

Enterprise Collaboration Services