FIELD REFERENCE — 2026 EDITION

Pre-Meeting Security Checklist

Twenty checks to run before any meeting where the conversation itself is the asset worth protecting — a board session, a negotiation, a disclosure of financial or legal strategy. Work through each section in order: room selection first, then electronics policy, then the sweep itself, then discipline once the meeting is under way.

Room selection

- [ ] Choose a room your organization controls rather than a shared or public space wherever possible.
- [ ] If off-site, confirm who booked the room before you and who has had access since.
- [ ] Check adjoining rooms and shared walls — a neighbouring space can carry a conversation as effectively as a device inside the room.
- [ ] Avoid rooms with unexplained recent renovation, repair visits or "maintenance" work.
- [ ] Confirm the room was not left unattended and unlocked in the hours before the meeting.

Electronics policy

- [ ] Set a policy on personal phones, smartwatches and recording devices for the duration of the meeting.
- [ ] Inspect any AV equipment, conferencing hardware or "smart" devices already in the room.
- [ ] Check phones, radios or Wi-Fi devices for unusually fast battery drain or unexplained warmth.
- [ ] Remove or account for gifts, promotional items or unfamiliar electronics on desks or shelves.
- [ ] Confirm laptops and devices brought into the room are known and authorized.

Pre-Meeting Security Checklist

Pre-meeting sweep

- [ ] Schedule an RF sweep to baseline the environment and surface active or intermittent transmitters.
- [ ] Physically inspect ceilings, walls, furniture and fixtures — dormant devices emit nothing for equipment alone to find.
- [ ] Check outlets, wiring and any recently moved or reset furniture, ceiling tiles or wall fixtures.
- [ ] Test phone lines, PBX or VoIP infrastructure for taps or unauthorized call-routing.
- [ ] Document what was inspected and cleared, with a timestamp, before principals arrive.

During-meeting discipline

- [ ] Keep the circle of people aware of the meeting's sensitivity as small as possible.
- [ ] Do not discuss the fact that a sweep took place inside the room itself.
- [ ] For high-stakes sessions, arrange live monitoring so a device introduced mid-meeting is not missed.
- [ ] Watch for new interference on calls, unfamiliar Wi-Fi or Bluetooth signals, or unexplained devices drawing power.
- [ ] If anything is found or suspected: do not touch it, do not announce it in the room — leave and call a TSCM specialist from elsewhere.

Print this checklist and keep it with your meeting-planning materials. For a full sweep, live monitoring, or executive travel support, call +233 20 778 9103 or email info@forensictscm.com — every enquiry is handled in strict confidence.