SOP: Confidentiality and Privacy Management During Meetings

> **Objective:** To maintain trust, comply with legal requirements, and safeguard organizational data by ensuring proper confidentiality and privacy management practices throughout all meeting processes.

1. Scope

This SOP applies to all organizational meetings, both virtual and in-person, where sensitive or confidential information may be discussed, shared, or recorded.

2. Responsibilities

- **Meeting Organizer:** Implements and enforces this SOP during all meetings.
- **IT Department:** Ensures secure communication tools and access controls.
- **Participants:** Adhere to confidentiality guidelines and agreements.

3. Pre-Meeting Preparation

1. Identify confidential or sensitive topics to be discussed.
2. Select secure communication platforms (e.g., encrypted conferencing tools).
3. Issue invitations only to authorized participants.
4. Distribute confidentiality agreements (NDAs) to all attendees as necessary and verify their completion.
5. Prepare and label confidential meeting materials; restrict access to authorized participants only.

4. Meeting Conduct

1. Begin with a confidentiality reminder, referencing relevant policies and agreements.
2. Prohibit unauthorized audio, video, or screen recording. If recording is required:
    - Obtain written consent from all participants prior to recording.
    - Store recordings securely with restricted access.
3. Prevent unauthorized access by using waiting rooms, passwords, or attendance lists in virtual meetings.
4. Monitor the discussion for unintended disclosures of sensitive information; address breaches immediately.

5. Access Control to Meeting Materials

- Distribute meeting documents via secure channels (e.g., encrypted email, secure drives).
- Restrict document access to necessary personnel only; implement role-based permissions.
- Label all materials with appropriate confidentiality notices.

6. Post-Meeting Protocols

- Collect all physical copies of confidential materials or ensure proper destruction (e.g., shredding).
- Limit distribution of minutes and recordings to authorized individuals only.
- Store all digital records on secure, access-controlled platforms.
- Remind participants of ongoing confidentiality obligations.

7. Information Sharing & Breach Response

1. Prohibit sharing of sensitive information outside the group without management approval.
2. Report any actual or suspected confidentiality breaches immediately to the designated authority.
3. Investigate breaches according to organizational policies and take corrective action.

8. Compliance and Review

- Regularly review this SOP for alignment with legal, regulatory, and organizational requirements.
- Provide ongoing training to staff regarding confidentiality and privacy expectations.

9. References

- Data Protection Laws (e.g., GDPR, HIPAA)
- Organizational Privacy and Security Policies
- Confidentiality & Non-Disclosure Agreements