SOP: Physical Security and Workstation Privacy Requirements

This SOP defines the **physical security and workstation privacy requirements** necessary to protect sensitive information and maintain a secure working environment. It covers secure access controls, proper workstation organization, privacy measures to prevent unauthorized data exposure, guidelines for locking devices and screens, and protocols for handling confidential materials. The goal is to minimize security risks and ensure compliance with data protection policies within the workplace.

1. Scope

This SOP applies to all employees, contractors, and visitors who access or use workstations or handle confidential information within company facilities.

2. Responsibilities

- **All Staff:** Follow the procedures outlined to protect information and equipment.
- **IT & Facilities:** Ensure physical security systems are maintained and operational.
- **Management:** Enforce compliance and provide regular training.

3. Physical Security Controls

- Restrict access to authorized personnel using electronic badges, keys, or PIN systems.
- Escort visitors at all times within secure areas.
- Report lost or stolen access devices immediately.
- Ensure doors, windows, and entry points remain secured after-hours.

4. Workstation Organization

- Maintain a clean desk policy-store documents securely when not in use.
- Do not leave sensitive information or devices unattended.
- Lock drawers and filing cabinets containing confidential materials.

5. Privacy Measures

- Position screens away from public view or use privacy filters.
- Refrain from discussing sensitive information in public or shared spaces.
- Use secure printers and promptly retrieve printouts with confidential data.

6. Device and Screen Locking

- Activate automatic screen lock after 5 minutes of inactivity.
- Manually lock devices when leaving the workstation, even briefly.
- Use strong passwords or authentication mechanisms to unlock devices.

7. Handling Confidential Materials

- Shred confidential paper documents before disposal.
- Label confidential materials appropriately.
- Use locked containers for disposal of sensitive documents awaiting shredding.

8. Incident Reporting

- Report any suspected breaches or suspicious activities to the Security or IT department immediately.
- Document incidents as per the company's incident management policy.

9. Compliance & Review

- Regularly review and update the SOP to reflect evolving risks and best practices.
- Non-compliance may result in disciplinary actions as per company policy.

10. Quick Reference Table

Requirement	Responsible	Frequency
Access Control Verification	Facilities/IT	Daily/Entry
Clean Desk Checks	All Staff/Supervisors	Daily/End of Day
Screen Lock Enforcement	All Staff	Whenever Away
Confidential Material Disposal	All Staff	As Needed
Incident Reporting	All Staff	Immediately Upon Discovery

11. Revision History

- **Version 1.0:** Initial draft - 2024-06-20