

Standard Operating Procedure (SOP): Security Equipment Usage (CCTV, Alarms) Instructions

This SOP provides detailed **security equipment usage** instructions, covering the proper operation and maintenance of CCTV systems, alarm systems, and related security devices. It includes guidelines for installation, monitoring, troubleshooting, and regular testing to ensure optimal performance, as well as protocols for data privacy and incident response to enhance overall facility security.

1. Purpose

To establish standardized procedures for the effective use, management, and maintenance of security equipment, including CCTV and alarm systems, to ensure the safety and security of the facility and its occupants.

2. Scope

This SOP applies to all security personnel, facility managers, and authorized operators responsible for handling security equipment on premises.

3. Roles and Responsibilities

Role	Responsibilities
Security Personnel	Operate and monitor equipment; conduct regular checks; report malfunctions or incidents.
Facility Manager	Supervise equipment installation, approve maintenance, and ensure compliance with SOP.
IT/Admin Support	Provide technical assistance, conduct troubleshooting, and manage data storage.

4. Equipment Installation Guidelines

- Install CCTVs and alarms at designated security-sensitive locations as per facility risk assessment.
- Ensure all devices are properly mounted, powered, and connected to control units/servers.
- Label each device for easy identification and maintenance tracking.
- Test the equipment post-installation for operational verification.

5. Operation Instructions

5.1 CCTV Systems

- Monitor live feeds regularly and in real time from control room monitors.
- Review and export recorded footage as required for investigations following data privacy protocols.
- Report equipment faults or suspicious activity immediately according to incident response procedures.

5.2 Alarm Systems

- Arm/disarm alarms according to access schedules and operational needs.
- Respond promptly to alarm activations; investigate root cause and document the incident.
- Reset alarms only after the source of activation has been verified and resolved.

5.3 Related Security Devices

- Ensure all sensors, access control systems, and related devices are functional.
- Follow manufacturer guidelines for device-specific operations.

6. Maintenance and Troubleshooting

- Perform visual inspection and cleaning of cameras/lenses at least monthly.
- Test alarm sounders and triggers weekly as part of routine checks.

- 3. Document and report any malfunctions to facility manager and request repairs as needed.
- 4. Keep a maintenance log for each device, detailing tests, faults, and corrective actions.

7. Data Privacy and Retention

- Restrict access to recorded footage and logs to authorized personnel only.
- Store all video/data securely in encrypted formats.
- Retain recorded data for the specified period as per legal or organizational requirements; delete securely thereafter.
- Do not share footage externally without written authorization from management and compliance with privacy laws.

8. Incident Response Protocol

1. Immediately report and escalate any equipment tampering, outages, or security incidents to management.
2. Preserve all relevant footage and logs for investigations.
3. Complete and submit an incident report within 24 hours of occurrence.
4. Support any reviews/investigations initiated as a result of the incident.

9. Regular Testing and Review

- Schedule bi-annual system audits and review SOP for relevance and effectiveness.
- Update training records to ensure personnel are current on equipment operation and protocol updates.

Note: Non-compliance with this SOP may result in disciplinary action and increases facility vulnerability. All personnel must report SOP deviations immediately.

10. Revision History

Date	Revision	Description
2024-06-01	1.0	Initial SOP Document Creation