

# SOP: CCTV Monitoring and Surveillance Operations

This SOP defines **CCTV monitoring and surveillance operations**, covering the installation, maintenance, and management of CCTV systems, real-time monitoring protocols, data storage and retrieval procedures, privacy and legal compliance, incident detection and reporting, and response strategies. The goal is to ensure effective security surveillance, protect assets, deter criminal activities, and maintain accurate records for investigation and analysis purposes.

## 1. Purpose

To provide a standardized procedure for the operation, monitoring, maintenance, and management of CCTV surveillance systems to enhance security, safeguard assets, ensure compliance, and support investigative processes.

## 2. Scope

This SOP applies to all staff responsible for the operation, monitoring, and management of CCTV systems within the organization's premises, including security personnel, IT staff, and management.

## 3. Responsibilities

Role	Responsibilities
Security Manager	Oversee CCTV operations, ensure SOP compliance, authorize access, coordinate incident responses.
CCTV Operators	Monitor live feeds, record incidents, follow notification procedures, ensure system functionality.
IT Department	Maintain CCTV hardware/software, manage data storage, assist in technical troubleshooting.
All Staff	Report suspicious activities, respect privacy guidelines, cooperate with investigations.

## 4. Procedure

### 4.1 Installation and Setup

- Install cameras at designated locations as per security risk assessment.
- Ensure all cameras are functional and positioned for optimal coverage.
- Record equipment serial numbers and locations in the CCTV inventory log.
- Test system functionality after setup and log results.

### 4.2 Real-Time Monitoring

- Operators must monitor feeds during designated shifts.
- Patrol and scan all camera views regularly for suspicious activities.
- Do not leave monitoring areas unattended during shift hours.

### 4.3 Incident Detection and Reporting

- Log and report any suspicious or criminal activity immediately to the Security Manager.
- Record the time, location, and details of the incident in the incident logbook.
- Preserve video footage relevant to the incident as evidence.

### 4.4 Data Storage and Retrieval

- Store footage on secure servers with restricted access.
- Retain video recordings for at least [specify period, e.g., 30 days] unless required for investigations.
- Process footage retrieval requests via formal authorization only.

### 4.5 Maintenance and Troubleshooting

- Conduct routine system checks (daily/weekly/monthly as per policy).
- Report malfunctions to the IT department for prompt resolution.

- Maintain maintenance logs for all hardware and software interventions.

## **4.6 Privacy and Legal Compliance**

- Display signage in all monitored areas informing about CCTV surveillance.
- Ensure data handling complies with applicable privacy laws and organizational policies.
- Do not use cameras in private areas such as restrooms or changing rooms.

## **4.7 Response Strategy**

- Follow escalation protocols for various incident types (e.g., theft, intrusion, violence).
- Cooperate fully with law enforcement and investigators as required.
- Document all actions taken in response to incidents.

## **5. Documentation and Records**

- CCTV installation and maintenance logs
- Incident reports and logs
- Footage retention and destruction records
- Access authorization logs

## **6. Training**

All relevant staff must receive training on CCTV system usage, legal obligations, privacy policies, and incident reporting procedures. Refresher sessions to be held annually or as required.

## **7. Review and Update**

This SOP shall be reviewed annually or upon major system or policy changes, and updated as necessary to ensure ongoing effectiveness and legal compliance.