Manufacturing Plant Security Standard Working Strategy (SOP)

Format

1. General

This SOP gives our procedures to ensure the physical security of the manufacturing unit, to include protection against unauthorized access, theft, vandalism, and other security threats.

2. Scope

This SOP applies to all employees, contractors, visitors, and security personnel .

3. Duties and Responsibilities -

- **Security Officer**: Oversees security operations, ensures adherence to SOPs, conducts security audits, and liaises with local law enforcement.
- **Security Personnel**: Monitors access points, surveillance systems, and enforces security protocols.
- **Facilities Manager**: Maintain security infrastructure, such as fences, gates, and lighting.
- **Employees Staff**: Follow security procedures, report suspicious activities, and ensure proper use of access controls.
- **Contractors and Visitors**: Comply with all security procedures and protocols.

4. Physical Barriers

- **Perimeter Security**:
  - Patrolling as per schedule with the help of control and monitoring applications.
  - Maintain fencing and gating around the perimeter of the manufacturing unit.
  - Ensure fencing is free of damage and has no unauthorized access points.
- **Building Security**:
  - Secure all doors and windows with appropriate locks and barriers.
  - Ensure external lighting is functional and covers all vulnerable areas.

4. Access Control

- **Employee Access**
  - Employees must wear company-issued ID badges visibly at all times.
  - Access to production areas and storage rooms is as per authorization.
  - Lost or stolen badges must be reported immediately to the Security Manager for deactivation and reissue.
- **Visitor Access**

- o Visitors must sign in at the reception, provide identification, and wear a visitor badge.
  - o Visitors must be escorted by an employee at all times.
  - o All visitors must sign out and return their badges before leaving.
- **Contractor Access**
  - o Contractors must be pre-approved and registered with the Security Manager.
  - o They must adhere to security protocols and be supervised while on-site.
  - o Contractors should report to the designated check-in area upon arrival and departure.
  - o Detailed process of Material Checks inward. Outward and returnable. Process for authorisation and reporting.

5. Surveillance and Monitoring

- **CCTV Systems**
  - o CCTV cameras are installed at key locations, including entry/exit points, production lines, and storage areas.
  - o Surveillance footage is monitored continuously by security personnel and stored for a minimum of [specify duration, e.g., 30 days].
  - o Regular maintenance and checks of the CCTV system are conducted to ensure operational effectiveness.
- **Alarm Systems**
  - o Intrusion detection systems and alarms are installed throughout the facility.
  - o Alarm systems are tested weekly to ensure functionality and a log maintained.
  - o Any alarm activation is promptly investigated by security personnel.

6. Incident Reporting:

- Procedure for reporting security incidents, including theft, vandalism, or unauthorized access.
- Ensure that all incidents are documented and investigated promptly.
- Detailed incident reports must be documented and reviewed to prevent future occurrences

7. Emergency Response

- **Evacuation Procedures**
  - o Clearly marked evacuation routes and emergency exits are posted throughout the factory.
  - o Regular fire and evacuation drills are conducted to ensure preparedness.
  - o Employees must be familiar with evacuation routes and assembly points.
- **Communication**
  - o In emergencies, the Security Manager will use [specify method, e.g., public address system, email, etc.] to issue instructions to employees.
  - o Emergency contact numbers are displayed prominently throughout the facility.

8. Asset Protection

- **Inventory Management**

- o On directions, Conduct regular inventory checks of raw materials, wire reels, and finished products to prevent theft and loss.
  - o Discrepancies in inventory must be reported to the Security Manager immediately.
- **7.2. Equipment Security**
  - o High-value machinery and tools should be secured when not in use.
  - o Access to sensitive areas, such as equipment rooms and storage areas, is restricted to authorized personnel.

9. Training and Awareness

- **Security Training**
  - o Provide regular security training to employees, including recognizing and reporting suspicious behaviour.
  - o Train security personnel on emergency response, use of security equipment, and conflict resolution.
  - o All employees must complete initial security training as part of their onboarding process.
  - o Refresher training is provided annually and whenever there are changes to security protocols.
- **Awareness Programs**
  - o Regular security awareness programs and briefings are conducted to keep employees informed about security best practices and updates.

10. Security Inspections

- **Routine Checks**:

  - o Conduct routine security inspections of the facility, including physical barriers, access controls, and surveillance equipment.
  - o Address any vulnerabilities or maintenance issues immediately.

- **Audits**:

  - o Perform periodic security audits to assess the effectiveness of security measures and compliance with SOPs.
  - o Review and update security procedures based on audit findings and emerging threats.

11. Review and Revision

- **Review**
  - o This SOP is reviewed annually or whenever significant changes to factory operations or security protocols occur.
  - o Updates and revisions are communicated to all employees.
- **9.2. Feedback**
  - o Management and Employees are encouraged to provide feedback on security procedures and report any issues to the Security Manager.

12. Document Control

- **Document Distribution**
  - A copy of this SOP is distributed to all employees and stored electronically in [specify location, e.g., internal network, document management system].
- **Revision History**
  - [Include a table or list detailing the revision history of the SOP, including dates and changes made.]

13. Appendices

- **Formats and Check Lists –**
  - Post and Site instructions.
  - Daily duty strength report
  - Daily activity report
  - Check list of locks and closure and opening of areas on and after closure of work
  - Specimen signature register and key issue matrix
  - Patrolling report
  - Alarm and sensors weekly check report
  - CCTV status
  - Incident report
  - Incident wise escalation matrix (For routine activity and emergency separately)
  - Security Process audit check lists for weekly and monthly checks.
- **Contact Information**
  - Security Manager: [Name, phone number, email]
  - Emergency Contacts: [List of relevant emergency contacts]
- **Floor Plans**
  - Evacuation routes, emergency exits, and key security areas as applicable.