

# Standard Operating Procedure

## Alarm System Activation and Deactivation

This SOP details the **alarm system activation and deactivation procedures**, covering step-by-step instructions for arming and disarming the security system, user authentication requirements, handling false alarms, system maintenance checks, emergency override protocols, and reporting mechanisms. The aim is to ensure effective and secure use of the alarm system to protect property and personnel from unauthorized access and potential threats.

### 1. Scope

This procedure applies to all staff authorized to operate the facility's alarm system.

### 2. Responsibilities

- **Security personnel:** Responsible for daily operation of the alarm system.
- **Management:** Ensure that only authorized personnel can access alarm system controls.
- **All staff:** Must report security incidents or alarm malfunctions immediately.

### 3. System Activation (Arming)

1. Verify that all doors and windows are securely closed and locked.
2. Approach the alarm control panel.
3. Enter your unique identification code using the keypad or authentication device.
4. Press the "Arm" or "Activate" button as indicated on the control panel.
5. Wait for visual or audio confirmation that the system is armed (e.g., beep, indicator light).
6. Exit the premises within the designated delay time.

### 4. System Deactivation (Disarming)

1. Enter the premises via authorized access points.
2. Proceed immediately to the alarm control panel.
3. Enter your unique identification code before the alarm delay expires.
4. Press the "Disarm" or "Deactivate" button.
5. Confirm successful deactivation via panel notification.

### 5. User Authentication Requirements

- Only authorized users with valid identification codes, keycards, or biometric credentials may arm/disarm the system.
- Personal identification codes must not be shared with others.
- Contact management immediately if your authentication method is lost, stolen, or compromised.

### 6. Handling False Alarms

1. Disarm the alarm as per Section 4.
2. Assess the source of the alarm immediately.
3. If safe, determine if the alarm was triggered accidentally.
4. Notify the security monitoring company of the false alarm using the predefined verification phrase.
5. Log the incident as a false alarm in the alarm system logbook or reporting system.

### 7. System Maintenance Checks

- Conduct monthly system tests according to manufacturer guidelines.
- Inspect sensors, alarms, and batteries for damage or wear.
- Document all maintenance activities and issues in the maintenance log.

## 8. Emergency Override Protocols

1. If emergency override is required (e.g., system malfunction or emergency exit permit), use the designated override code or procedure.
2. Notify security and management immediately following an emergency override.
3. Record details of the override, including the reason and personnel involved, in the incident report.

**Automatic logging of all overrides is required for audit purposes.**

## 9. Reporting Mechanisms

- All incidents, including false alarms, overrides, and malfunctions, must be reported to the security supervisor within one hour.
- Use the standardized incident report form or electronic system.
- Submit reports for monthly review and analysis.

## 10. Document Control

- This SOP shall be reviewed annually and updated as necessary.
- Distribution of this SOP is restricted to authorized personnel only.

---

SOP Owner: Security Department | Effective Date: \_\_\_\_\_ | Revision: 1.0