Standard Operating Procedure for Compromised Office Entrance

Purpose

This SOP describes the actions to be taken by the security personnel in the event of a compromised office entrance, such as a forced entry, a lock malfunction, or a security breach. The objective of this SOP is to ensure the safety and security of the office premises, assets, and personnel, and to prevent further damage or loss.

Definitions

- **Compromised office entrance**: Any situation where the normal access control or physical security of the office entrance is compromised, such as a broken lock, a damaged door, a lost key, a stolen card, or an unauthorized entry.
- **Security personnel**: Any staff or contractor who is responsible for the security of the office, such as security guards, security officers, or security managers.
- **Office entrance**: The main entry point to the office, such as the front door, the lobby, or the reception area.

Procedures

1. Upon discovering or receiving a report of a compromised office entrance, the security personnel on duty should immediately notify the security manager and the office manager, and provide the following information:
   - The location and nature of the compromise
   - The time and date of the compromise
   - The possible cause and extent of the compromise
   - The current status and condition of the office entrance
   - The actions taken or planned to secure the office entrance
2. The security personnel on duty should also assess the level of risk and urgency of the situation, and determine the appropriate response, such as:
   - Calling the police or emergency services, if there is a threat to life, property, or evidence
   - Calling the maintenance or repair service, if there is a need to fix or replace the lock, door, or other equipment
   - Calling the access control or IT service, if there is a need to reset or revoke the access cards, codes, or passwords
   - Calling the cleaning or disposal service, if there is a need to clean or remove any debris, dirt, or hazardous materials

3. The security personnel on duty should also take the necessary measures to secure the office entrance, such as:
    - Locking or blocking the compromised entrance, if possible
    - Posting a sign or a notice to warn or inform the staff and visitors of the situation
    - Deploying additional security personnel or equipment to monitor or guard the compromised entrance
    - Redirecting the staff and visitors to use an alternative entrance, if available
4. The security personnel on duty should also document the incident and the response, and prepare a written report, including the following details:
    - The name and contact of the security personnel on duty
    - The name and contact of the security manager and the office manager
    - The name and contact of any other parties involved or notified, such as the police, the maintenance, or the access control service
    - The description and photos of the compromised office entrance and the surrounding area
    - The timeline and actions of the incident and the response
    - The outcome and impact of the incident and the response
    - The recommendations and lessons learned from the incident and the response
5. The security manager should review the report and the response, and provide feedback and guidance to the security personnel on duty, and take any further actions as required, such as:
    - Conducting an investigation or an audit to determine the cause and the responsibility of the compromise
    - Implementing corrective or preventive actions to avoid or reduce the recurrence or the severity of the compromise
    - Updating or revising the security policies, standards, procedures, or guidelines to improve the security practices
    - Conducting training or awareness sessions to educate the security personnel and the staff on the security procedures and the best practices

Revision History

- Version 1.0: Created by Bing on 03 Jan 2024