

Access Control

1) Purpose:

- a) The purpose of this Standard Practice (SP) is to establish guidelines and procedures for access control in a building. The SP ensures the security, safety, and authorized access of individuals entering the premises while maintaining a controlled environment.

2) Scope:

- a) This SP applies to all employees, tenants, visitors, and contractors and is applicable to all access points within the building.

3) Access Control System:

- a) We will implement a comprehensive access control system to regulate entry and monitor access within the building. The system may include the use of key cards, access codes, biometric systems, or other approved methods.
- b) Designated personnel shall be responsible for overseeing and managing the access control system.

4) Authorized Access:

- a) Access permissions will be granted based on job roles, responsibilities, and authorization levels.
- b) A centralized database will be maintained to store and manage access control permissions for each individual.
- c) Access rights will be regularly reviewed and updated as needed, ensuring only authorized individuals have access to specific areas.

5) Access Requests:

- a) Employees, tenants, and contractors must submit access requests through the designated channels.
- b) Access requests should include the individual's name, job title, department, reason for access, and the specific area(s) requiring access.
- c) The appropriate authority should approve requests before access is granted.

6) Visitor Access:

- a) Visitors must register at the designated check-in point upon arrival.
- b) Visitors will be issued temporary access credentials or visitor badges, which will provide access only to authorized areas for the duration of their visit.
- c) An authorized employee or host should accompany visitors at all times.

7) Access Control Points:

- a) Access control points will be strategically located at entry and exit points, sensitive areas, and restricted zones within the building.
- b) Each access control point will be equipped with appropriate security devices, such as card readers, biometric scanners, or other approved mechanisms.
- c) Security personnel or designated personnel will monitor access control points, ensuring proper identification and verifying authorized access.

8) Monitoring and Auditing:

- a) The access control system will generate logs and reports of access activities, including entry, exit, and denied access attempts.
- b) Regular auditing of access logs will be conducted to identify any unauthorized access attempts or suspicious activities.
- c) Any anomalies or security breaches should be reported to the designated security personnel or management immediately.

9) Emergency Situations:

- a) Emergency access procedures should be established and communicated to all employees and tenants.
- b) During emergencies, such as fires or evacuations, access control systems may be overridden to facilitate rapid evacuation or emergency response.
- c) Designated personnel will be responsible for coordinating emergency access procedures and ensuring the safety of all individuals.

10) Training and Awareness:

- a) All employees, tenants, and contractors should receive training on access control procedures, including the proper use of access credentials, reporting suspicious activities, and emergency protocols.
- b) Regular awareness campaigns and reminders should be conducted to reinforce the importance of access control and security.

11) Documentation and Review:

- a) All access control activities, incidents, and access requests should be properly documented for future reference and review.
- b) Regular reviews and evaluations of this SOP should be conducted to identify areas for improvement and ensure its continued effectiveness.