

Visitor Management and Office Access Control Standard Operating Procedure (SOP)

Version: 1.0

Classification: UNCLASSIFIED • FOR PUBLIC USE

1. Purpose

1.1 This Standard Operating Procedure (SOP) establishes standardized requirements for visitor management and office access control to prevent unauthorized physical access to organizational facilities, personnel, information, and assets.

1.2 These procedures support physical security best practices and align with the intent of the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Physical and Environmental Protection (PE) and Access Control (AC) control families.

2. Scope and Applicability

2.1 This SOP applies to all organizational facilities, including administrative offices, operational spaces, controlled areas, and restricted areas.

2.2 This SOP applies to all employees, contractors, interns, vendors, auditors, and visitors who access organizational facilities.

3. Definitions

3.1 Visitor: Any individual who does not possess an active employee or contractor access credential issued by the organization.

3.2 Escort: An authorized employee responsible for supervising a visitor while on organizational premises.

3.3 Restricted Area: Any area designated as requiring enhanced access controls due to sensitivity, safety, or critical systems.

3.4 Access Credential: A physical mechanism used to grant access, including badges, keys, personal identification numbers, or biometric identifiers.

4. Roles and Responsibilities

4.1 Executive Leadership is responsible for approving and enforcing organizational physical security policies.

4.2 Facilities Management is responsible for maintaining physical access systems, locks, doors, and associated infrastructure.

4.3 Security Personnel are responsible for monitoring access, reviewing logs, responding to incidents, and enforcing escort requirements.

4.4 Employees are responsible for displaying credentials, escorting visitors when required, and reporting suspicious or unauthorized activity.

5. Visitor Management Procedures

5.1 Visitors shall report to a designated entry point upon arrival.

5.2 Visitors shall present valid government-issued photo identification unless explicitly exempted by documented policy.

5.3 Visitor entries shall be recorded in a visitor log or visitor management system, including visitor name, host, check-in time, check-out time, and authorized areas.

6. Visitor Badging and Identification

6.1 Visitors shall be issued a temporary badge that is clearly distinguishable from employee credentials.

6.2 Visitor badges shall display a visitor designation and expiration date and shall be worn visibly at all times while on premises.

6.3 Visitor badges shall be collected upon exit and immediately invalidated.

6.4 Lost, stolen, or unreturned visitor badges shall be reported to Security and documented as a security incident.

7. Escort Requirements and Responsibilities

7.1 Visitors shall be escorted at all times unless explicitly authorized otherwise by Security or Facilities Management.

7.2 Escorts are responsible for ensuring that visitors do not access unauthorized areas, do not photograph or record sensitive spaces, and comply with all safety and security instructions.

7.3 Escort responsibilities include visitor pickup, continuous supervision, and visitor checkout.

7.4 Escorting supports physical access control and visitor control objectives consistent with NIST SP 800-53, Revision 5 (e.g., PE-3 and PE-8).

8. Access Control Principles

8.1 Physical access shall be granted based on the principle of least privilege and role-based access.

8.2 Access rights shall be approved by authorized personnel, documented, and reviewed periodically.

8.3 Shared access credentials are prohibited. Credentials shall not be loaned, shared, or reused under any circumstances.

9. Access Control Mechanisms

9.1 Approved access mechanisms may include proximity badges, smart cards, personal identification numbers (PINs), biometric systems, mechanical keys, or combinations thereof.

9.2 Access control systems shall be configured to log access events where technically feasible.

10. After-Hours Access

10.1 After-hours access shall require prior authorization and shall be limited to approved individuals and areas.

10.2 After-hours access events shall be logged and reviewed for anomalies.

11. Incident Reporting

11.1 Suspected or confirmed unauthorized access shall be reported immediately to Security.

11.2 Physical access incidents shall be documented and investigated in accordance with incident response procedures.

12. Review and Maintenance

12.1 This SOP shall be reviewed at least annually or following significant changes to facilities, threats, or regulatory requirements.