Standard Operating Procedure (SOP)

Access Control and Authorization Procedures

This SOP defines the **access control and authorization procedures** to regulate and monitor entry to secure areas within an organization. It includes methods for verifying identities, issuing access credentials, managing permissions, and revoking access when necessary to ensure the safety and security of personnel, information, and assets. The procedures ensure that only authorized individuals gain access, reducing risks of unauthorized entry and enhancing overall security compliance.

1. Purpose

To establish standardized procedures for controlling and monitoring access to secure areas, ensuring only authorized personnel are permitted entry and reducing organizational risks associated with unauthorized access.

2. Scope

This SOP applies to all employees, contractors, visitors, and any other individuals requiring access to secure or restricted areas.

3. Definitions

Term	Definition
Access Control	Methods and policies used to restrict or allow entry to physical or logical assets.
Authorization	The process of granting individuals permission to access specific resources.
Credential	Item (badge, keycard, biometric, password) issued for identity verification and access granting.

4. Responsibilities

- **Security Manager:** Oversee implementation and enforce compliance with SOP.
- **Human Resources:** Notify Security of staff hirings, terminations, and role changes.
- **IT/Facilities:** Manage and monitor electronic access control systems.
- **Employees/Contractors:** Adhere to access protocols and report anomalies.

5. Procedure

1. **Identity Verification**
    - Ensure all personnel present a valid photo ID or biometric verification upon first registration.
    - Visitors are to be escorted and must sign the visitor log.
2. **Issuance of Access Credentials**
    - Provide authorized personnel with credentials appropriate to their role (keycard, fob, PIN, etc.).
    - Log all issued credentials in the Access Management System (AMS).
3. **Permission Management**
    - Grant access strictly on a need-to-know/need-to-access basis.
    - Review permissions at least quarterly and upon any change in personnel status.
4. **Monitoring Access**
    - Monitor all access points with surveillance and electronic access logs.
    - Audit access logs regularly (monthly or more frequently in high-security areas).

5. **Revocation of Access**
    - Revoke credentials immediately upon employee termination or change of role.
    - Collect all physical credentials (badges, keys, devices) during exit procedures.

6. **Incident Reporting**
    - Report lost or stolen credentials immediately to Security.
    - Investigate unauthorized access attempts or suspicious activity.

6. Documentation & Records

- Maintain logs of issued and revoked credentials.
- Document access reviews and audit findings.
- Store records securely for a minimum of 3 years.

7. Review & Revision

This SOP should be reviewed annually and updated as necessary to reflect changes in personnel, technology, or policy requirements.

8. References

- Company Security Policy
- Data Protection and Privacy Guidelines
- Physical Security Standards

9. Approval

Name	Title	Date	Signature