# SOP: Distribution and Access Control Procedures

This SOP details **distribution and access control procedures**, covering the systematic management of resource allocation, secure access authorization, monitoring of access points, identification verification, and role-based access restrictions. It aims to ensure that resources and sensitive areas are distributed appropriately and accessed only by authorized personnel to maintain security, accountability, and operational efficiency.

## 1. Purpose

To outline procedures for the controlled distribution of resources and enforcement of access control measures within the organization.

## 2. Scope

This procedure applies to all personnel, departments, and contractors engaged in the allocation, access, and monitoring of physical and digital resources.

## 3. Responsibilities

- **Access Control Manager:** Oversees access authorization, audits and reporting.
- **Supervisors:** Request and review personnel access as per role requirements.
- **IT/Facilities Staff:** Implement technical or physical access controls and maintain secure systems.
- **All Personnel:** Comply with access policies and immediately report breaches or unauthorized access.

## 4. Procedure

### 4.1 Resource Distribution Management

1. Departments submit resource allocation requests via the approved channel (e.g. request form or ticketing system).
2. Requests reviewed by supervisors for eligibility and necessity.
3. Resources distributed according to priority, policy, and availability.
4. Distribution logged in the Resource Register with recipient, date, and item details.

### 4.2 Access Authorization

1. Supervisors submit access requests for staff, specifying required areas or systems and justification.
2. Access Control Manager reviews requests for appropriateness and conflict of interest.
3. Approved access granted using role-based credentials (badges, codes, software accounts).
4. Access permissions reviewed quarterly and updated upon role changes or terminations.

### 4.3 Monitoring and Access Point Security

1. All entry and exit points equipped with monitoring devices (e.g. CCTV, access logs).
2. Logs reviewed daily for irregular activities.
3. Immediate investigation and reporting of unauthorized access attempts.

### 4.4 Identification and Verification

1. Personnel must display valid ID badges at all times in secured areas.
2. Visitors escorted and logged, with visitor badges issued and returned upon exit.
3. Dual verification (e.g. ID plus biometric or PIN) required for sensitive zones.

### 4.5 Role-Based Access Restrictions

1. Access rights assigned as per job role and least privilege principle.
2. Employees only receive access required for their responsibilities.
3. Temporary access reviewed and revoked after use.

## 5. Documentation & Records

- Resource Distribution Log
- Access Control Request and Approval Forms
- Access Logs and CCTV Footage
- Visitor Logs
- Incident Reports

## 6. Review and Audit

1. Access rights and distribution records reviewed at least quarterly.
2. Annual audit of procedures and logs by designated security team.
3. Continuous improvement recommendations documented and implemented as needed.

## 7. References

- Company Security Policy
- IT Access Policy
- [Relevant Regulations, e.g., ISO 27001, GDPR, etc.]

## 8. Revision History

| Date | Revision | Description | Author |
|---|---|---|---|
| 2024-06-12 | 1.0 | Initial SOP template released | Admin |