

# Standard Operating Procedure (SOP): Room Assignment and Key Management

This SOP details the procedures for **room assignment and key management**, covering the allocation of rooms to guests or employees, key issuance and retrieval processes, security protocols for key handling, record-keeping of key distribution, and measures to prevent unauthorized access. The goal is to ensure efficient room allocation, maintain security, and provide clear accountability for all keys issued within the facility.

## 1. Purpose

To standardize and clarify procedures for assigning rooms and managing keys in order to ensure security, accountability, and operational efficiency.

## 2. Scope

This SOP applies to all staff involved in room assignment and key management for guests, visitors, and employees in the facility.

## 3. Responsibilities

- Front Desk/Reception: Manages room assignment and issues/retrieves keys.
- Security Personnel: Monitors security aspects of key control.
- Supervisors/Managers: Oversee compliance and address exceptions or incidents.

## 4. Procedure

### 4.1 Room Assignment

1. Verify the identity of the guest or employee requiring a room.
2. Consult the room availability list or system.
3. Assign an appropriate room based on requirements and availability.
4. Update the room assignment log or system with occupant details.

### 4.2 Key Issuance

1. Retrieve the key corresponding to the assigned room from the secure storage area.
2. Record key issuance in the Key Register, noting:
  - Name of recipient
  - Room number
  - Date and time issued
  - Issuer's name/signature
3. Physically hand over the key and verbally instruct on security protocols.

### 4.3 Key Retrieval

1. Upon check-out or room change, request the return of all issued keys.
2. Verify the key against records and room number.
3. Sign in the return in the Key Register, including date/time and recipient signature.
4. Secure the key in the appropriate storage area immediately.

### 4.4 Security and Access Control

- Keys must only be issued to authorized individuals.
- Lost or damaged keys must be reported immediately to a supervisor.
- All master keys should be stored separately and only accessible to authorized personnel.
- Regular audits of key inventory and logs must be conducted as scheduled.

### 4.5 Record-Keeping

- Maintain accurate and up-to-date logs of all key transactions.
- Retention of records must be in line with facility policy (e.g., minimum of 1 year).
- Records should be available for review in the event of security incidents.

## 5. Measures to Prevent Unauthorized Access

- Strictly prohibit sharing of keys.
- Change locks immediately if keys are reported lost or stolen.
- Implement electronic access where feasible for better tracking.
- Educate all key holders on their responsibility to safeguard keys.

## **6. Exceptions & Incident Management**

- Document all exceptions (e.g., lost keys, denied access) and report to management.
- Initiate investigation according to security protocols if unauthorized access is suspected.

## **7. Review & Update**

This SOP should be reviewed annually or following any major incident or policy change.