Standard Operating Procedure (SOP): Key Management and Issuance Processes

1. Purpose

This SOP details the **key management and issuance processes**, encompassing the systematic control, distribution, and tracking of keys to authorized personnel. It outlines procedures for key issuance, return, duplication, and loss reporting, ensuring security and accountability across all access points. The purpose is to protect assets, maintain controlled access, and prevent unauthorized entry through effective key management practices.

2. Scope

This SOP applies to all physical keys controlling access to company premises, offices, storage areas, and other secured facilities. It is binding for all employees, contractors, and visitors requiring access to restricted areas.

3. Responsibilities

- **Security Manager:** Oversees key management, maintains records, and ensures SOP compliance.
- **Authorized Personnel:** Responsible for safeguarding issued keys and complying with all procedures.
- **Key Custodian:** Issues, collects, and maintains inventory of all keys.
- **All Employees:** Report lost, stolen, or damaged keys immediately.

4. Procedure

4.1 Key Issuance

1. Personnel requiring access submit a **Key Request Form** to the Security Office.
2. Managerial approval is obtained before processing the request.
3. The Key Custodian verifies authorization and logs the key issuance in the *Key Register*.
4. The key is issued, and the recipient signs an acknowledgement of receipt and responsibility.

4.2 Key Return

1. Keys must be returned upon termination of access rights, change of role, or upon request.
2. The Key Custodian verifies key condition and updates the *Key Register*.
3. The recipient signs a return confirmation.

4.3 Key Duplication

1. Duplication of keys is strictly prohibited unless approved in writing by the Security Manager.
2. All duplicated keys must be logged and uniquely identified.

4.4 Lost, Stolen, or Damaged Keys

1. Any loss, theft, or damage must be reported to Security immediately using an Incident Report.
2. An investigation is conducted and corrective action (e.g., replacement, rekeying locks) is determined.
3. A new key may be issued if approved; all actions are documented in the *Key Register*.

5. Documentation and Records

- **Key Register:** Master log of all issued, returned, duplicated, lost, or destroyed keys.
- **Key Request/Issuance Forms:** Signed by requester and approving manager.
- **Incident Reports:** For lost, stolen, or damaged keys.

6. Compliance and Audit

1. The Security Manager conducts periodic audits of key inventory and records.
2. Non-compliance may result in disciplinary action and/or liability for losses incurred.

7. Appendices

Document	Description
Key Request Form	Document to request issuance of a key, includes approvals.
Key Register Template	Log for tracking key issuance and status.
Incident Report Template	Form to report lost, stolen, or damaged keys.