SOP Template: Key and Access Card Distribution and Tracking

This SOP details the processes for **key and access card distribution and tracking**, including issuance protocols, user authorization, recording and maintaining access logs, loss and theft reporting procedures, periodic audits, and revocation of access rights. The purpose is to ensure secure management of physical access tools to protect facilities, maintain accountability, and prevent unauthorized entry.

1. Purpose

To establish standardized procedures for the authorized distribution, tracking, and revocation of keys and access cards, ensuring facility security and accountability.

2. Scope

This SOP applies to all employees, contractors, and visitors who require access to company-controlled facilities via physical keys or access cards.

3. Responsibilities

- **Security Department:** Manage key/access card inventory and logs, conduct audits.
- **Supervisors/Managers:** Authorize access based on role necessity.
- **Recipients (Users):** Safeguard issued items and promptly report loss or theft.

4. Key and Access Card Issuance Protocols

1. Recipients submit an Access Request Form approved by their manager.
2. Security verifies authorization and records recipient information.
3. Each key/access card is assigned a unique identifier.
4. Recipient signs an acknowledgment of receipt and responsibility.
5. Security updates the Access Log (see sample below).

Name	Department	Key/Card Number	Date Issued	Issued By	Date Returned	Returned To
Jane Doe	IT	K-105	2024-06-14	S. Smith		

5. User Authorization

- Access approval is based on role and necessity, confirmed by department manager.
- Security maintains up-to-date lists of authorized personnel for each restricted area.

6. Recording and Maintaining Access Logs

- All keys/cards are tracked in a secure, centralized log (physical or digital).
- Log entries include recipient details, access level, issuance and return dates.
- Logs are reviewed regularly for accuracy.

7. Loss and Theft Reporting Procedures

1. Recipient immediately notifies Security and direct supervisor.
2. Security deactivates lost access cards and initiates investigation if necessary.
3. A Loss/Theft Report is filed and corrective actions implemented.
4. New keys/cards may be issued following protocol with documentation.

8. Periodic Audits

- Security conducts audits of all issued keys/cards at least annually.
- Discrepancies are investigated, and any unaccounted-for items are addressed promptly.
- Audit results are reported to management.

9. Revocation of Access Rights

1. Upon termination, transfer, or change of role, keys and access cards must be returned to Security.
2. Access is immediately revoked in case of violation or upon staff departure.
3. Security updates logs and confirms deactivation of credentials.

10. References and Forms

- Access Request Form
- Loss/Theft Report Form
- Key/Access Card Acknowledgment Form

11. Revision History

Date	Version	Changes	Approved By
2024-06-14	1.0	Initial SOP release	D. Lee