Physical Office Security Policy**Company**: PatientPartner
Office Address: 1025 Prospect St, Ste 350, La Jolla, CA 92037

Objective: To safeguard company assets, employees, and sensitive information through comprehensive physical security measures at our office location.

Policy Guidelines:

1. **Access Control**:
    - **Door Code**: The door code provides secure access to the hallway. It is only shared with authorized personnel and is updated every six months or in case of personnel changes or security breaches.
    - **Key Distribution**: Physical keys are provided exclusively to internal employees. Contractors or visitors are not permitted to have keys. Employees must return keys upon leaving the company.
    - **Locked Doors**: Office doors must be locked at all times when not in use, ensuring doors are securely closed upon entry or exit.
2. **Security Cameras**:
    - Security cameras are installed in key access points, such as entryways and office doors.
    - Recordings are kept for a minimum of 90 days.
    - A quarterly review of the footage is conducted to check for policy violations or suspicious activity. Incidents are reported and documented immediately.
3. **Visitor Management**:
    - Visitors must sign in upon arrival and be accompanied by an internal employee throughout their stay.
    - Contractors and maintenance staff are pre-approved and supervised during their work on-site.
4. **Employee Responsibilities**:
    - Employees are required to report lost keys, suspicious activity, or security breaches to the COO or the designated security officer.
    - Security training is conducted during onboarding and refreshed annually for all employees.
5. **Emergency Procedures**:
    - In the event of a security breach (e.g., unauthorized access or theft), security footage is reviewed immediately.
    - After a breach, a comprehensive audit of security systems (locks, access codes, etc.) is conducted.
6. **Review and Compliance**:

- The security policy is reviewed annually or after a security incident to ensure compliance with ISO standards and industry best practices.
- A physical security report is generated quarterly and submitted for ISO compliance reviews.

7. **Backup and Incident Response**:
   - All security footage is backed up on a secure cloud or physical server.
   - In the event of a break-in, the incident response procedure includes notifying local authorities, filing an internal report, and conducting a full investigation.