Family Law Software
A CENTERBASE COMPANY

Physical Security Program Policy

This document outlines the organization's policy for **physical security** for all office spaces and data center facilities to protect personnel, assets, and information systems from unauthorized access, damage, theft, and environmental hazards.

1. Scope and Responsibilities

Area	Scope	Responsibility
Scope	All owned, leased, or managed facilities, including **corporate office spaces** and **data center(s)**.	
Security Team	Develop, implement, and maintain the physical security program; manage access control systems.	**Chief Information Security Officer (CISO)** and **Facilities Management**.
All Personnel	Adhere to all physical security policies, report suspicious activity, and challenge unescorted strangers.	All employees and contractors.

2. General Facility Requirements (Offices and Data Centers)

All facilities must adhere to the following baseline security controls:

- **Access Control:** Use an **electronic access control system** (e.g., key cards, biometrics) at all entry/exit points. Mechanical keys should only be used as a backup.
- **Visitor Management:** All visitors must **sign in**, present valid government-issued ID, be issued a **temporary badge**, and be **continuously escorted** by an authorized employee. Visitor logs must be retained for at least 90 days.

- **Perimeter Security:** Exterior doors and windows must be **secured** (e.g., locking mechanisms, reinforced glass). Vehicle access should be restricted where possible.
- **Video Surveillance (CCTV):** Deploy **cameras** at all facility entrances, exits, common areas, and high-value asset locations. Recordings must be **retained for a minimum of 30 days**.
- **Lighting:** Maintain adequate **lighting** around the facility perimeter, parking areas, and entrances during non-daylight hours.
- **Emergency Procedures:** Post clear and visible instructions for handling emergencies, including fire escape routes and communication plans.

3. Office Space Security Controls

Office spaces house employees and general company assets, requiring controls focused on personnel safety and general asset protection.

- **Badge Policy:** All employees must **wear their identification badge** visibly at all times within the facility.
- **Restricted Areas:** Areas containing sensitive information or equipment (e.g., server closets, executive offices) must be clearly marked and have **separate, logged access control**.
- **Clean Desk Policy:** Employees must clear all **Confidential** and **Internal** documents and removable media from their desks at the end of the workday and lock them away.
- **Equipment Security:** Desktops, laptops, and other valuable equipment must be **physically secured** to desks or workstations where feasible (e.g., using cable locks).

4. Data Center Security Controls (Highest Priority)

Data centers house critical IT infrastructure and data, requiring the most stringent, multi-layered security controls.

4.1. Layered Access Control

Data center access must implement a **"Mantraps"** or **two-factor authentication (2FA)** approach for entry into the equipment floor, requiring:

1. **Level 1 (External):** Badge/Key Card access to the facility perimeter.
2. **Level 2 (Internal):** Secondary authentication (e.g., Biometric scan) to enter the secure server room/cage.

4.2. Monitoring and Surveillance

- **24/7 Monitoring:** Data center facilities must be monitored **24 hours a day, 7 days a week** by trained security personnel (either on-site or remote).
- **CCTV Placement:** Cameras must monitor **all aisles, racks, entrances, and shipping/receiving areas**.
- **Rack and Cage Security:** Customer or segregated infrastructure must be housed in **locked cages or individual cabinets**. Keys must be strictly controlled and logged.

4.3. Environmental and Safety Controls

- **Fire Suppression:** Use **non-water-based fire suppression systems** (e.g., clean agent gas) in server rooms to prevent equipment damage.
- **HVAC and Power:** Implement **redundant HVAC** (Heating, Ventilation, and Air Conditioning) systems and **Uninterruptible Power Supplies (UPS)** with backup generators.
- **Water Detection:** Install **water and leak detection sensors** in critical areas (e.g., under raised floors) with immediate alerts to facilities staff.
- **Temperature Monitoring:** Implement automated monitoring for temperature and humidity to ensure optimal operating conditions and system integrity.

4.4. Equipment Movement

All equipment (new or removed) entering or leaving the data center must be documented and verified against an **authorized equipment manifest** before being allowed to pass security checkpoints. This prevents unauthorized asset removal.