CSNP
CYBERSECURITY NON-PROFIT

Physical Security Guide for Business Premises

A comprehensive approach to protecting your facility, assets, and people through layered physical security measures.

CSNP SECURITY SERIES

Understanding Physical Security

What Is Physical Security?

Physical security protects your organization's people, property, and assets from physical threats. It's the foundation that supports your digital security measures—without it, even the strongest cybersecurity can be compromised.

A layered defense strategy, often called "defense in depth," creates multiple barriers that deter, detect, and delay potential threats while giving your team time to respond effectively.

Key Protection Layers

- Perimeter security: Fencing, lighting, and signage
- Building access: Locks, badges, and entry systems
- Interior controls: Secure zones and monitoring
- Asset protection: Safes, surveillance, and protocols

Effective physical security starts with understanding what you're protecting and who might want access to it.

Facility Access Control

Entry Points

Limit and monitor all doors, windows, and access routes. Every entry should be controlled, logged, and regularly audited.

Authentication Methods

Use key cards, PIN codes, or biometric systems. Consider multi-factor authentication for sensitive areas.

Access Levels

Implement role-based permissions ensuring employees only access areas necessary for their work responsibilities.

Regularly review and update access permissions, especially when employees change roles or leave the organization. Audit logs monthly to identify unusual access patterns.

Visitor Management Best Practices

01

Pre-Registration

Require advance notification for all visitors. Verify identity and purpose before granting access to your facility.

02

Check-In Procedures

Issue temporary badges, record visit details, and require photo identification at reception.

03

Escort Protocols

Assign staff escorts for visitors in restricted areas. Never allow unaccompanied access to sensitive zones.

04

Check-Out Process

Collect badges and verify departure. Maintain detailed visitor logs for security audits and incident response.

Workstation and Device Security

Clear Desk Policy

Lock away sensitive documents and portable devices when leaving your workspace, even briefly.

Screen Privacy

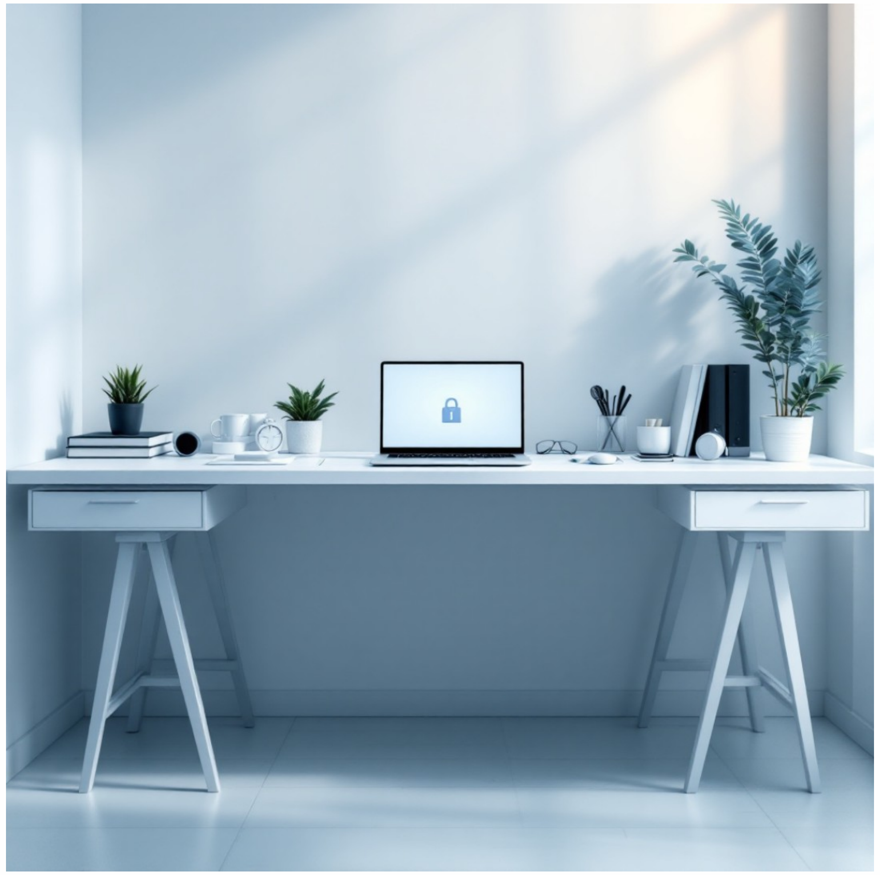
Use privacy filters and automatic screen locks. Position monitors away from windows and public areas.

Device Locks

Secure laptops with cable locks. Enable automatic locking after periods of inactivity.

Visitor Awareness

Be mindful of shoulder surfing. Cover keyboards when entering passwords or sensitive information.



Server Room and IT Infrastructure Security

Physical Access

Restrict server room access to authorized IT personnel only. Use separate authentication systems with detailed access logs.

Environmental Controls

Maintain proper temperature, humidity, and fire suppression systems. Monitor conditions 24/7 with alerts for anomalies.

Power Protection

Install uninterruptible power supplies (UPS) and backup generators. Protect against outages and electrical surges.

Document Security and Information Protection

Storage

Lock filing cabinets containing sensitive information. Use safes for highly confidential materials.

Disposal

Shred all documents before discarding. Use cross-cut shredders for maximum security.

Printing

Retrieve printed documents immediately. Don't leave sensitive materials unattended at printers.

Handling

Use "confidential" labels and track document movement with chain-of-custody logs.

Surveillance and Monitoring Systems

Strategic Camera Placement

- All entry and exit points
- Parking areas and perimeter
- Reception and common areas
- Server rooms and storage areas
- Loading docks and back entrances

System Requirements

Record continuously with minimum 30-day retention. Ensure adequate lighting, backup power, and secure storage for footage. Post visible signage to comply with privacy regulations.

Balance security needs with employee privacy. Clearly communicate monitoring policies and avoid surveillance in private areas like restrooms.

Emergency Procedures and Response

Evacuation Plans

Post clear evacuation routes and assembly points. Conduct regular drills and maintain updated emergency contact lists.

Alarm Systems

Install and test fire, intrusion, and panic alarms regularly. Ensure all staff know how to respond to different alerts.

First Response

Train designated staff in emergency procedures. Stock first aid kits and maintain emergency supplies in accessible locations.

Lockdown Protocols

Establish procedures for active threats. Practice secure room protocols and communication during emergencies.

About the Cybersecurity Non-Profit

> "Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."

Our Free Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety Online
- Senior Digital Safety
- Women's Security
- Parents & Educators Resources

Visit Us

csnp.org

Explore all our security resources and educational materials

Access Resources

csnp.org/resources

Download guides, checklists, and training materials—completely free