Physical Security Checklist for SMBs

Perimeter Security

- Surveillance cameras installed and covering all entrances/exits
- Outdoor lighting for parking lots, walkways, and building perimeters
- Fencing or barriers around the property (if applicable)
- Access points minimized and secured

Building Access Control

- Entry doors secured with locks, keycards, or biometric access
- Visitor log or digital tracking system in place
- ID badges issued to employees and enforced
- Secure mail/package delivery area to prevent unauthorized access
- Alarm system installed and monitored

Office & Work Area Security

- Internal doors to restricted areas locked when not in use
- Server rooms and network closets secured with limited access
- Security cameras installed inside the office, monitoring sensitive areas
- Employees trained on proper security protocols (tailgating, unauthorized access)
- Desktop and laptop computers secured with locks

Employee and Visitor Security

- Visitor access restricted and escorted at all times
- Employees required to report lost/stolen badges immediately
- Background checks conducted for new hires (if applicable)
- Employees aware of security policies and emergency procedures

Surveillance & Monitoring

- Security cameras functioning and footage stored securely for at least 30 days
- Regular audits of surveillance footage for suspicious activity
- Motion detectors and alarms in key areas
- Alarm response plan in place and tested

Data & Document Security

- Sensitive paper documents stored in locked cabinets
- Shredders available and used for document disposal
- Visitor Wi-Fi network separate from business-critical systems
- Secure disposal process for outdated hardware (hard drives, USBs, etc.)
- Backup of critical data stored in a secure off-site location

Emergency Preparedness

- Fire extinguishers in place and employees trained on usage
- Emergency exits clearly marked and unobstructed
- Panic buttons installed in high-risk areas (e.g., reception, cash handling)
- Business continuity and disaster recovery plan documented

Vendor and Supply Chain Security

- Third-party vendors meet security standards before access is granted
- Regular security audits for contractors and maintenance staff
- Inventory control process in place to prevent theft or loss

Incident Response & Reporting

- Incident response team designated
- Procedures for reporting security breaches documented
- Drills conducted to test response to security incidents