Tashundre Gilmore
Physical Security
W25 CTS1134.0T3:
NETWORKING

Requirements Summary

The client requires comprehensive physical security implementation to safeguard IT assets, data, and personnel across a facility that includes 9 offices, a breakroom, open lab/library, IT support room, server room with 4 racks, 10 classrooms, and a small room with laptops. Each area has workstations, VoIP phones, WAPs, and printers. Security implementation will focus on access control, surveillance, fire protection, and environmental controls to ensure compliance with laws and best practices.

Key solutions:

- **Access Control Systems**: Biometric/RFID locks should be deployed at server rooms and IT support areas with multi-factor authentication (badge + PIN) for high-risk zones
    - Teacher Offices will use standard lock and key provided to the teacher to lock up their respective offices if not occupied.
    - Same with classrooms but all classrooms will be locked after the last class times.
- **Surveillance Cameras**: IP cameras in key hallways, entrances, common areas, and server room with 24/7 recording.
    - The library is open but under 24/7 surveillance.
- **Server Room Security**: Locked racks, UPS systems, and restricted badge access. Server Room and IT support area is locked at all times.
- **Asset Protection:** Devices like printers and workstations will be monitored through RFID tagging and physical anchoring.
- **Visitor Management**: Check-in system at the front office and visitor badges.
- **Environmental Protections**: Smoke detectors, fire suppression system (FM-200 or clean agent), HVAC monitoring in the server room.

Government Laws

- **Federal**: **FERPA** - **Family Educational Rights and Privacy Act** (student info is involved). Ensure areas with educational data (labs/classrooms) have secure access and logging.
- **State/Regional/Local**: Must comply with local fire code regulations, building access laws, and data protection acts specific to the state of Florida

- **ADA Compliance**: Ensure security controls do not hinder accessibility requirements.
- **Data Protection Laws**: Implement physical security that aligns with data protection regulations such as GDPR (if any international data is stored).

Organizational Requirements

- Security policies will enforce badge-only access, device locking policies, and off-hour alarm systems.
- Regular training and awareness campaigns will ensure staff follow protocols.
- The organization must implement logging and reporting on physical access and device usage.

Industry & IT Best Practices

- **Multi-layered security** (defense-in-depth): Combining surveillance, access control, and physical barriers.
- **ISO/IEC 27001**: Follow security frameworks for protecting assets.
- **24/7 Monitoring**: Implement centralized NVR monitoring with redundancy.
- **Redundancy & Failover**: Secure backup power, temperature control systems, and data recovery options.