Physical Security Systems Standard

Introduction

The State of Oklahoma has a responsibility to protect state buildings, assets, IT systems, applications and data entrusted to it by its citizens. Therefore, it is necessary to take appropriate measures to ensure the security of these public IT assets. The safety and security of the physical space and assets are a shared responsibility of all agencies in the State of Oklahoma. To meet this obligation, OMES IS has established this standard to outline the hardware and software requirements for access control, video surveillance systems and physical intrusion detection systems. Only OMES IS authorized access control systems, video surveillance systems and physical intrusion detection systems shall be used on state facilities.

Purpose

This document establishes baseline controls to guide state agencies in the purchase and installation of physical security systems and alarms.

Definitions

Integrator – The vendor who is responsible for the installation and configuration of the physical security system.

Networked video recorder – A computer system that records video transmitted over the network from multiple surveillance cameras and saves it to a storage device.

Access control system – A software and hardware system restricting entrance to a property, a building or a room through technological means, typically including automated locks and access cards and management software.

Physical intrusion detection system – A software and hardware system that detects unauthorized physical access to building or room through technological means, typically including motion sensors, door contacts and management software.

Standard

The State of Oklahoma requires licensing for vendors responsible for installation, inspection and testing of security alarm systems. Additionally, vendors installing and/or testing such systems and their employees must undergo a national criminal background check facilitated by a third party or the Department of Labor.

All physical security hardware and software assets must meet the specifications defined in this standard. This document outlines the requirements set forth by OMES IS to implement physical security system controls. The technical specifications for approved physical security systems are available upon request.

OMES IS has an established naming convention for physical security systems with the intent of providing users with intuitive information within the name. Therefore, naming conventions for all equipment must be in a format approved by OMES IS. No variation is allowed unless written approval is obtained from the Chief Information Security Officer.

Power and network telecommunications cabling should be protected from interception, interference or damage. Infrastructure for cabling must be consistent with the following:

- All cables must be installed by one of the following.
  - Integrator responsible for the project
  - Structured cable company approved by OMES.
- No cable is allowed to lay on the dropped ceiling or hard deck. It may be suspended no more than three feet above the ceiling wherever possible. Additionally, NVR cables should be installed in a data cable tray when provided.
- Cable hangers are required.

- For NVR, splicing is not permitted in CAT data cable and the distance cannot exceed 330 feet end-to-end. For electric door hardware and access control, splicing above the ceiling is not permitted except for when there is no access within a reasonable distance of the device. In this scenario, a junction box is required.
- NVR does not require a service loop; however, sufficient slack is recommended. Electric door hardware and access control requires a small service loop above every door. The service loop must not exceed three loops and should be neatly hung above the door and not on the ceiling.

The state's standard platforms for video surveillance, access control systems and physical intrusion detection systems are to be designed and implemented with the assistance of Oklahoma Cyber Command.

- All networked cameras used to record, or monitor must be connected to a separate network on the back of the NVR, as well as connect to a separate NIC. The system must only be accessed by the local NVR authorized users. Additionally, the NVR is used to view and playback data from the cameras.
- It is the security integrators responsibility to design an access control system in compliance with local safety codes. Any variance to the hardware configuration must be provided in writing by the agency prior to awarding a contract.
- It is the security integrator's responsibility to design a physical intrusion detection system in compliance with state and local codes. Any variance to the hardware configuration must be provided in writing by the agency prior to awarding a contract.
- A list of approved products is maintained by OMES Cyber Command.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- Physical Security System Technical Specifications.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/06/2021	**Review cycle:** Annual
Last revised: 11/30/2023	**Last reviewed:** 11/30/2023
Approved by: Joe McIntosh, Chief Information Officer	