OKLAHOMA
Office of Management
& Enterprise Services

Physical Security Standard

Introduction

The State of Oklahoma is committed to maintaining security of its facilities through strict building access control. The state's environment requires controlled access to help ensure the safety of state employees and facilities from unlawful or unauthorized access. It is necessary to take appropriate measures to protect the confidentiality, integrity and availability of state data and resources.

Purpose

This document establishes minimum standards for physical security and building life safety systems.

Definitions

- 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.
- Integrator – The vendor responsible for the installation and configuration of the physical security system.
- Physical intrusion detection system – A software and hardware system that detects unauthorized physical access to a building or room through technological means, typically including motion sensors, door contacts and management software.
- Surveillance system – CCTV camera systems.
- VLAN – Virtual Local Area Network.
- Life safety building systems – A software and hardware system designed to protect people in a building during emergencies, including fires, earthquakes, and other hazardous events, and can include fire alarms and suppression systems.

Standard

Badge layout: Access badges must be compatible with the statewide physical security control system and must be ordered through Oklahoma Cyber Command to prevent duplication of badge ID numbers. Badge format is uniform to ensure compatibility with the system, reduce the risk of counterfeit badges and facilitate accurate identification. Oklahoma Cyber Command manages and stores the format for all state-issued badges. Any variance to the approved format requires approval from the state Chief Operating Officer.

As accurate identification is critical to maintaining physical security in all state facilities, hats and sunglasses shall not be worn in pictures used to produce physical access/state ID cards. Due to the sensitivity of the information, the badge format and requirements are classified as confidential. Access to review the information may be granted as defined in the Confidential Standards standard.

Life safety building systems: OMES has established the following design and operational requirements for life safety building systems (fire alarms and suppression systems).

- All systems deemed as life safety must be designed in a highly available architecture with multiple redundancies and no single point of failure.

- Systems must be segmented on the network and not intermingled with other non-life safety systems.
- Operational requirements include 24-hour component monitoring and alerting.
- Must have deployable staff to support 24-hour monitoring and alerting components.
- Staff supporting 24-hour monitoring and alerting components must have 24/7 access to physical equipment.
- Replacement components must be available within two business hours for metropolitan locations and within four business hours for locations outside metropolitan areas.
- Systems must be tested at least twice per year.
- Systems must have established maintenance windows that adhere to the Change Management Standard.

Physical security hardware/software.
All hardware and software related physical security or building life safety equipment must conform to current industry standards and be approved by Oklahoma Cyber Command prior to acquisition and installation.

- All physical security systems must be connected to a segregated security VLAN.
- All networking and installation work must conform to current CIO standards governing their application.
- All physical security systems must be installed by a security systems integrator licensed by the State of Oklahoma.

Refer to the Permitted Technology Standard for the current list of approved physical security and building life safety vendors and products. Follow the process contained within the Permitted Technology Standard for evaluation and decisioning for any technology not contained on this list.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 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

- Confidential Technology Standard.
- Change Management Standard.
- Permitted Technology Standard.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 09/05/2025	**Review cycle:** Annual
Last revised: 09/05/2025	**Last reviewed:** 09/05/2025
Approved by: Dan Cronin, Chief Information Officer	