Physical Access Control Standard

Introduction

The State of Oklahoma is committed to maintaining security of its facilities through strict control of building access. 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

The document provides guidance on the layout of physical badges in order to be compatible with the statewide badging access control system and to define the underlining support model.

Standard

Physical access to non-public areas of state facilities is controlled by using state-issued badges that must be compatible with the statewide physical security control system. 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.

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.

Additionally, all state facilities must adhere to the Physical Security Systems Standard. Only OMES IS authorized access control systems shall be used on state facilities as defined in the Physical Security Systems Standard. Oklahoma Cyber Command manages the state physical security systems.

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 Standards Standard.
- Physical Security Systems Standard – Confidential Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 03/02/2022	**Review cycle:** Annual
Last revised: 03/02/2022	**Last reviewed:** 08/17/2023
Approved by: Joe McIntosh, Chief Information Officer	