IoT Device Standard

Introduction

This standard outlines guidelines and regulations for the responsible and secure use of internet of things devices within the Oklahoma state network, ensuring the safety, security, privacy and integrity of the network infrastructure.

Purpose

This standard is applicable to all employees, contractors, and third-party vendors who have access to the State of Oklahoma systems, networks and data. An IoT device is defined as any device that has an embedded operating system which does not support the installation of security agents, such as antivirus software, and is not designed for frequent software updates. Examples of these devices include printers, security cameras, smart speakers, smart lights, industrial control systems, smart TVs, video streaming devices, personal network-attached storage devices, VoIP phones, conference room systems, and digital signage.

Definitions

- IoT – Internet of Things; a network of interrelated devices that connect and exchange data with other IoT devices and the cloud.
- VLAN – Virtual local area network; a logical grouping of devices connected to the same network regardless of physical location.

Standard

Security measures.

- All IoT devices must adhere to the State of Oklahoma standards.
- Devices should have up-to-date firmware and security patches applied.
- Use strong, unique passwords for IoT devices, and change default passwords immediately upon setup in accordance with the Password Requirements Standard.
- Disable any default accounts and create new custom accounts where possible.
- Implement encryption protocols (e.g., WPA3) for wireless IoT devices.
- Regularly update and patch IoT devices to protect against known vulnerabilities. Any vendors failing to provide regular firmware/security updates for IoT devices should be avoided.
- Define the required services of the IoT device and disable or uninstall any additional features that are not required.

Network access.

- IoT devices must connect to designated and segregated IoT network segment VLANs.
- Unauthorized IoT devices, devices not meeting security standards (i.e., causing network-related alarms) or a device not receiving regular updates and posing a potential security risk may be disconnected.

Privacy and data handling.

- Users are responsible for ensuring that personal and sensitive data collected by IoT devices comply with applicable laws, regulations and State of Oklahoma policies.
- IoT devices should minimize data collection to the extent necessary for their intended purpose.
- When disposing of IoT devices, ensure the secure deletion of data and proper disposal according to state standards.

Violations of this standard may result in the suspension of IoT device access privileges and disciplinary action.

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
- Password Requirements Standard.
- OMES Policy & Standards.

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

Effective date: 03/06/2025	**Review cycle:** Annual
Last revised: 03/06/2025	**Last reviewed:** 03/06/2025
Approved by: Dan Cronin, Chief Information Officer	