Information Technology Operations Command Center Standard

Introduction

The State of Oklahoma has a responsibility to deliver and monitor IT systems, applications and data entrusted to it by its citizens. Therefore, it is necessary to take appropriate measures to ensure monitoring and event management of these systems. The ITOCC proactively monitors the IT stack through the network to servers and storage. Applications are monitored for abnormal conditions. To meet this obligation, Oklahoma Office of Management and Enterprise Services Information Services has established this standard to outline the requirements for OMES and vendors for event management.

OMES IS prescribes to a standardized process for managing incidents and events which is aligned with the Information Technology Infrastructure Library framework and methodology.

Purpose

This document establishes baseline controls to guide OMES teams and vendors in the purchase and installation of IT systems.

Definitions

Application – A program that performs a specific business function.

Firewall – A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

Monitoring – A process of gathering metrics about the operations of the state's IT environment's hardware and software to ensure infrastructure functions as expected in support of applications and services.

Network devices – A device used to connect computer systems together to transfer resources or files. Examples include Wi-Fi access point, switch, router, etc.

Server – A computer or system that provides resources, data, services or programs to other computers, known as clients, over a network.

Storage – A purpose-built server used for storing, accessing, securing and managing digital data, files and services over a shared network or through the internet.

Platform as a service – A complete development and deployment environment in the cloud where the underlying infrastructure and resources to support it are hosted and maintained by the provider, enabling the customer to develop, deploy and run applications ranging from simple cloud-based apps to highly sophisticated, cloud-enabled enterprise applications. Examples include Microsoft Azure and Google Cloud Platform.

Software as a service – A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted and maintained by the provider. SaaS is also known as "on-demand software" and web-based/web-hosted software. An example of this is Microsoft Office 365.

Infrastructure as a service – A form of cloud computing service that provides virtualized computing resources over the internet. The cloud provider maintains the infrastructure components such as storage, server and networking resources, and delivers them to the customer via virtual machines accessible through the internet. Examples include Microsoft Azure and Amazon Web Services.

Standard
All server and storage hardware and software assets must meet the specifications defined in this standard. Vendors supply the ability for systems to log data to the state-approved monitoring tools, as documented in the state's reference architecture. This document outlines the requirements set forth by OMES IS to implement system controls.

- The following systems and solutions must provide system data to the state-approved monitoring tools.
    - Platform as a service.
    - Software as a service.
    - Infrastructure as a service.
    - Applications.
    - Servers and storage.
    - Network devices.
    - Firewalls.
    - Building environmental systems.
- Vendors providing telecommunications shall provide notifications of outages.

All unplanned events or service interruptions follow the major incident management procedure for restoration of services.

OMES IS utilizes a centralized IT service management (ITSM) tool for incident and event management activities and documentation. The state's standard ITSM tool is documented in the enterprise reference architecture.

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

- Enterprise Reference Architecture.
- Internal – 05.03.02 Major Incident Management SOP.

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

Effective date: 01/18/2022	**Review cycle:** Annual
Last revised: 07/20/2022	**Last reviewed:** 07/13/2022
Approved by: Joe McIntosh, Chief Information Officer	