OKLAHOMA
Office of Management
& Enterprise Services

Chromebook Exception 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. Because of this, appropriate segregation of Google Chromebook workstation security exceptions is vital in maintaining the underlying cybersecurity standards within the state network of Oklahoma.

Purpose

This document establishes baseline controls to guide OMES teams and vendors on the installation and implementation of Google Chromebooks.

Definitions

Application – A program that performs a specific business function.

Chromebook – A laptop or tablet running the Linux-based Chrome operating system, a lightweight operating system, as its operating system.

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

GRE tunnel – Generic Routing Encapsulation tunnel protocol.

MDM – Mobile device management.

Monitoring – A process of gathering metrics about the operation 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.

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.

Zscaler – Cloud security platform providing cloud-delivered web and application connectivity.

Standard

All server and storage hardware and software assets must meet the specifications defined in this standard. Chromebooks purchased by the State of Oklahoma must fall under the following standards in order to maintain preponderance and existence on the network:

- Chromebooks must fall under their own respective network segment within the network and under the firewall, separated from normally approved devices (e.g., Windows and Linux workstations and servers), zone and/or VLAN or on the public network.
- Chromebooks must be networked via a GRE tunnel to Zscaler for proper policing of internet traffic and application security features.
- Violation of these rules will result in immediate removal of device from network.

If an agency or third-party (independent of the agency) utilizes Chromebooks within the organization, the agency or third-party vendor are expected to provide overall management of the Chromebooks with appropriate MDM tools.

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.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 07/05/2023	**Review cycle:** Annually
Last revised: 07/05/2023	**Last reviewed:** 07/05/2023
Approved by: Joe McIntosh, Chief Information Officer	