Web Proxy for Business Needs Standard

Introduction

The State of Oklahoma provides internet access for the sole purpose of supporting business activities necessary to carry out job functions. The operation of the internet relies heavily on the proper conduct of the users who must adhere to the guidelines as outlined in this standard. It is expected that use of state resources to access the internet is business-related and consistent with the mission of the State of Oklahoma.

Access to the internet is granted to all state employees and contractors. By using this resource, users accept full responsibility for their actions and agree to use the resource in an ethical manner. In an effort to help protect end users, OMES IS has technical safeguards in place.

Employees and contractors are subject to federal, state and local laws governing many interactions occurring on the internet.

Purpose

This document establishes guidelines for acceptable use of the internet at the State of Oklahoma and establishes criteria and expectations for roles which are required to operate outside the enterprise secure web gateway protections.

Standard

OMES IS subscribes to a web filtering services to reduce risk to state data, services and employees. The service provides protection through anonymizing web traffic by concealing IP addresses, and defending devices against virus, malware, worms, trojans and ransomware by scanning files downloaded from the web. Additionally, the service provides advanced protection including browser exploits such as cross-site scripting and file-type vulnerabilities.

OMES IS prohibits the use of internet sites that pose a security risk to state data and systems. Security risks include malicious domains and IP addresses, sites known to harbor and/or deliver malicious code and utilize trackers to track user's activities. Additionally, internet sites that display illegal content or do not serve a legitimate business purpose are prohibited. OMES IS may block or restrict the use of such sites as it determines appropriate.

Website access is granted based on agency and state business requirements. The state CIO, or their designee, has the authority to determine and implement appropriate levels of internet access for employees and contractors.

In some instances, individuals with specific roles may need access to sites otherwise blocked in order to fulfill their job duties. The business requirements for these roles must be coordinated with Cyber Command via a service request to the OMES Service Desk.

Users in roles provided additional website access are also required to do the following:

- Complete security awareness training (SEAT) twice annually.
- Successfully complete quarterly phishing exercises.
- Not use administrator accounts to browse the web as defined in the Administrator Account Standard.
- Ensure workstations have appropriate security controls installed and operating as defined by OMES IS.
- Be logged into the state's secure web gateway solution at all times during use.
- Lock workstations with password protection when not in use.
- Properly secure workstations and other computing devices when not in use.
- Not store workstations in motor vehicles.
- Utilize passwords with a minimum length of 15 characters. Passwords shall include at least one lowercase letter, uppercase letter, numeral and special character.
- Change passwords at least every 60 days.
- Protect passwords at all times and never share directly or indirectly by allowing others to reasonably observe or find them written down.
- Use discretion when browsing these websites to protect others from viewing or misusing content.

Failure to meet these requirements may result in suspension to network access and/or computer account(s). Restoration of access will be at the sole discretion of the state CIO or state CISO.

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

- Administrator Account Standard.
- Vulnerability Scanning Standard

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/06/2021	**Review cycle:** Annual
Last revised: 11/16/2022	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	