OKLAHOMA
Office of Management
& Enterprise Services

System Acceptable Use Standard

Introduction

In support of its mission, the State of Oklahoma provides access to information technology resources for employees and contractors. Protecting and preserving these resources is a cooperative effort and requires all users to act responsibly and guard against abuse.

Purpose

This document provides guidance on responsibilities for employees and contractors when using state information technology resources.

Standard

Users are expected to report suspected illegal activity or abuse, especially if related to any damage to or problems with their files. Reports are made by emailing servicedesk@omes.ok.gov. Any defects discovered in the system accounting or system security are to be reported so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. System administrators are required to report suspected unlawful or improper activities to Oklahoma Cyber Command. Users have an affirmative duty to cooperate with Oklahoma Cyber Command in investigations of system abuse.

It is a violation of this standard to use the state's information technology resources for transmitting political campaigning, commercial or personal advertisements, solicitations, promotions, or programs, to libel, harass, threaten, or without authorization, invade the privacy or impersonate the identity of other individuals.

Additionally, it is a violation to use state information technology resources for the purpose of introducing a malicious program into the network, any server or any computer connected to the network. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the state, as well as criminal action.

This standard prohibits both the circumvention of mechanisms which protect private or restricted information, systems or networks, as well as use of state resources for unauthorized access to private or restricted systems or networks and/or damage to software or hardware components of those systems or networks.

Modifying or removing computer equipment, software, or peripherals without proper authorization is a violation of this standard.

Interfering with the intended use of information resources or without authorization, destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of electronic information and/or information systems are not all, but further examples of systems abuse.

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: 04/07/2022	**Review cycle:** Annual
Last revised: 10/18/2022	**Last reviewed date:** 03/08/2024
Approved by: Joe McIntosh, Chief Information Officer	