Personal Device Standard

Introduction

OMES Information Services is committed to protecting the State of Oklahoma's employees, partners and its citizens from illegal or damaging actions by individuals, either knowingly or unknowingly. To this end, employees must obtain management approval to use personal devices in connection with state business. Effective security is a team effort involving the participation and support of every employee accessing state information and/or information systems. It is the responsibility of every employee to know the guidelines, and to conduct activities accordingly. Each employee who desires to use personal devices in connection with state business must follow the requirements outlined in this document.

Purpose

This standard outlines the acceptable use of personal devices for state employees. This standard is in place to protect the state, its employees and citizens. Inappropriate use exposes employees and the state to risks including malware attacks, compromise of networks systems and services and legal issues.

Definitions

Personal device – Any personal computing device connecting directly to the state network services including email and calendar services. This definition includes, without limitation, computers, smart phones and tablets.

State record – For the purpose of this standard, information on a personal device created by, received by, under the authority of, or coming into the custody, control or possession of a state employee in connection with the transaction of public business, the expenditure of public funds or the administering of public property and as otherwise may be defined by the Oklahoma Open Records Act.

Standard

The following are general use and ownership requirements for personal devices.

- State records stored on electronic and computing devices, whether owned or leased by the state, the employee or a third party, remain the sole property of the state.
- State records should not be downloaded or stored on personal devices.
- Employees have a responsibility to immediately report the theft, loss of or otherwise compromised personal devices to supervisors and Oklahoma Cyber Command.
    - Supervisors shall escalate as necessary depending on the sensitivity of state records accessed by the personal device.
- Employees may access, use or share state records via personal device only to the extent it is authorized and necessary to fulfill assigned job duties.
- Employees are responsible for exercising good judgement regarding the reasonableness of personal use. If there is any uncertainty, employees should consult with their supervisor or manager.
- Employees shall abide by the state's or the individual agency's record retention policy for all state records.

The following are general security requirements for personal devices.

- All personal devices connecting to state information, accessing state data or state records must comply with state security policies and standards.
- All devices must have anti-virus and anti-malware software installed, kept up-to-date and currently enabled. OMES offers CrowdStrike Falcon for Home Use to all state employees. Employees can contact the OMES Service Desk to obtain installation instructions.
- Employees are responsible for keeping personal devices current with all other security patches from the appropriate software update services. This includes applications such as Microsoft, Adobe, Firefox, Chrome, etc.
- Full disk encryption should be enabled for increased protection of the device.
- System level and user level passwords must comply with all state password requirements. Sharing of passwords or any other authentication information is strictly prohibited.
    - Use complex passwords that are at least ten characters with upper- and lower-case letters, numbers and special characters.
    - Avoid common dictionary words.
    - Change passwords periodically.
    - Do not use the same password for all accounts.
- All personal devices must be secured with a password protected screensaver with the automatic activation feature set to 10 minutes or less. Employees should lock the screen or log off when the device is unattended.
- Employees must use extreme caution when opening email attachments on a personal device as those may contain malware. Please visit Using Caution with Email Attachments for additional guidance and information.
- Employees must not install software that allows the user to bypass standard built-in security features and controls, otherwise known as jail breaking.
- Employees who share the personal device with other individuals or family members must ensure individuals do not access state records or business email while using the device. Furthermore, employees must take necessary steps to secure physical state records while working in a space that is shared with other individuals or family members.
- Employees must not print state records from a personal device.
- Employees may only use state-approved and configured applications to access resources.
- Avoid connecting to public or untrusted/insecure Wi-Fi connections.
- Employee must not enable potentially dangerous mobile services while accessing state information services that can export or transmit nonpublic information to unauthorized devices without the user's knowledge. For example, serving as a mobile hotspot or enabling Bluetooth without using recommended safeguards that prevent unauthorized devices from connecting while connected to state information systems.

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: 04/01/2020	**Review cycle:** Annual
Last revised: 01/31/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	