State of Oklahoma Personal Device Standard

Introduction

OMES Information Services ("IS") is committed to protecting the State of Oklahoma's ("State") employees, partners and its citizens from illegal or damaging actions by individuals, either knowingly or unknowingly. To this end, OMES IS and agency management must give approval to an employee to use his or her personal device in connection with state business. In the event an employee is required to work from home, OMES IS automatically approves such use, provided the guidelines below are followed. Effective security is a team effort involving the participation and support of every employee who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly. Each employee who desires to use their own personal device in connection with state business must follow these guidelines. OMES IS reserves the right to revoke the privilege granted herein if the employee does not abide by the guidelines set forth below.

Purpose

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

Definitions

Personal Device: a "Personal Device" is defined as a personal computing device that connects directly to the state network services including but not limited to email and calendar services. This definition includes, without limitation, computers, smart phones and tablets.

State Record: A "State Record," for purposes of this standard, means 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.

General Use and Ownership

1. 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.
2. State records should not be downloaded or stored on personal devices.

3. Employees have a responsibility to immediately report the theft or loss of personal devices to supervisors. Supervisors shall report the event up the chain as may be necessary depending on the sensitivity of state records accessed by the personal device.
4. Employees may access, use or share state records via a personal device only to the extent it is authorized and necessary to fulfill assigned job duties.
5. 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.
6. Employees shall abide by the state's or the individual agency's Record Retention Policy for all state records.

Security

1. All personal devices that connect to state information systems or access state data or state records must comply with state security policies.
    i. State-approved anti-virus and anti-malware software must be installed on the personal device, kept up-to-date and currently enabled.
        1. Microsoft Defender Anti-Malware is available on Windows 10.
        2. Mac OSX has several protection and security tools built in
            a. XProtect (https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web).
            b. OSX Firewall (https://support.apple.com/en-us/HT201642).
            c. GateKeeper (https://support.apple.com/en-us/HT202491).
    ii. Employees are responsible for keeping personal devices current with all other security patches/fixes from the appropriate software update services. This includes, but is not limited to, applications such as Microsoft, Adobe, Firefox, Chrome, etc.
    iii. For increased protection of your personal device, enable full disk encryption
        1. BitLocker on Windows 10 (Enabling BitLocker for Windows 10).
        2. FileVault for Mac OSX (Enabling FileVault for Mac OSX).
        3. Encryption for Android (Enabling Encryption for Android).
        4. Apple phones are encrypted by default.
2. System level and user level passwords must comply with all internal password policies. The sharing of passwords or other authentication information is strictly prohibited.
    i. Use complex passwords that are at least 10 characters with upper- and lower-case letters, numbers and special characters.
    ii. Avoid common dictionary words.
    iii. Change passwords periodically.
    iv. Do not use the same password for all your accounts
        1. Using password manager helps store and manage multiple accounts.
3. 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.
4. 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.
5. Employees must not install software that allows the user to bypass standard built-in security features and controls, otherwise known as "jail breaking."

6. Employees who share the personal device with other individuals or family members must ensure such individuals do not access state records or business email while using the device. Further, employees must take necessary steps to secure physical state records while working in a space that is shared with other individuals or family members. Any loose documents that qualify as state records must be kept in a secure location in your home work space. While working remotely, employees must take extra precaution to ensure these documents are not lost, disposed of or otherwise used improperly.
7. Employees may only use state-approved and configured applications to access resources.
8. Avoid connecting to public or untrusted/insecure WIFI connections.
9. Employee will 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).