Policy No. 191 - Mobile Device Usage

PURPOSE

The state recognizes mobile devices for many personnel are valuable tools that aid the state in conducting business in an effective and timely manner. These tools can help employee productivity and promote public and employee safety. This policy intends to address privacy, records retention, the stewardship of confidential state information and related issues raised by mobile device usage.

This Policy defines the minimum steps expected of state agencies in order to ensure the efficient assignment, use and management of mobile devices while protecting state public records, employee privacy, client privacy and consumer information. This policy is intended to: Enhance the security of state operations and information assets; Ensure agencies and employees are aware of their responsibilities.

POLICY STATEMENTS

1. State agencies have an affirmative duty under state law to retain, preserve exempt and non-exempt public records, and produce non-exempt public records in response to a request, including those created, accessed, used or stored on mobile devices. Agencies also have a duty to preserve and produce records for litigation purposes. Public records, both exempt and non-exempt, include those records – including, but not limited to, texts, voice mail, email, instant messaging, calendars, photos, and video – an employee prepares, owns, uses, receives or retains within the scope of employment. Agency mobile device usage policies must address and conform to these requirements.
2. An agency may approve expanded requirements beyond those identified herein to manage its mobile device program.
3. Agencies must determine which of the following mobile solutions their employees may use for agency business:
    3.1. State-owned and State-controlled Devices;
    3.2. Personal Devices
4. All mobile solutions used for state business must be equipped with up-to-date, currently-patched Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) software;
5. Agencies must adopt a Mobile Device Policy and directly communicate that policy to each of their employees when revised
6. Agency Mobile Device Policies must:
    6.1. Govern employee use of mobile devices for agency business;
    6.2. Articulate employees' basic rights and responsibilities concerning mobile device usage;

6.3. Outline the process by which the agency receives access to public records prepared, owned, used or retained on mobile devices, including encrypted communications;
6.4. Provide guidance for protection of confidential data, records, and customer information;
6.5. Provide guidance for proper records management (creation, storage, and disposition) on mobile devices;
6.6. Undergo annual agency review for possible update.

7. Agencies must provide training for employees explaining the agencies' mobile device policies, including but not limited to the following topics:
   7.1. Employee rights and responsibilities;
   7.2. Privacy concerns for the types of devices used, as well as how to avoid disclosure of employee personal information;
   7.3. What constitutes a public record on a mobile device;
   7.4. Security measures the employee is expected to take to protect the mobile device and the public records stored there from theft, loss or unauthorized disclosure;
   7.5. Steps the employee must take upon request to make public records on the device and its contents available to the agency for review, litigation, disclosure and records management;
   7.6. What kinds of mobile devices or solutions (if any) are prohibited under agency policy;
   7.7. How to notify the agency if a mobile device is lost, stolen, destroyed or compromised;
   7.8. Protecting client privacy and personal information in the course of public service.
8. Agencies must comply with this policy by June 30, 2019.

CONTACT INFORMATION:

Contact the OCIO Policy & Waiver Mailbox if you have questions about this policy.

SUNSET REVIEW DATE: May 11, 2021

ADOPTION DATE: May 11, 2018

APPROVAL DATE: June 12, 2018

APPROVING AUTHORITY: Rob St. John, Acting State CIO & Chair of TSB