Mobile Device Usage Policy & Security Standard Background

Replaces IT Security Standard 141.10 (3.1.7, 5.2.4, 5.8) and Mobile Device Usage 191

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

- Updates to this standard draws from SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- Laptops and non-agency devices are now addressed by the policy.
- Requirements to communicate agency mobile device policies were updated include timing: onboarding, annually, and when revised.

What is the business case for the policy/standard?

- 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.
- This standard helps agencies increase freedom of movement while conducting state business with an understanding of the risks to their IT assets, and to employ appropriate controls.

What are the key objectives of the policy/standard?

The objectives of this policy are:

- Establish policy for the roles, responsibilities, and standard practices concerning the effective and efficient management of mobile devices used to access the state IT Assets and conduct government business.
- Ensure the understanding of risk and responsibility and that it is documented and understood.
- 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.

How does policy/standard promote or support alignment with strategies?

This policy strengthens IT Architecture & Security by requiring agencies to secure assets with the portability and high risk of potential incidents. It also addresses the use of non-agency mobile devices.

What are the implementation considerations?

- Agencies will need to verify and update awareness training to include mobile device policies.
- Agencies may need additional training and support.

How will we know if the policy is successful?

- Agencies will minimize data leakage from the use of mobile technology.
- Agencies will decrease the number and severity of incidents involving mobile devices including losses and resets.