Mobile Device Management Policy

Effective: February 1, 2014
Revised: May 1, 2017
Reviewed: May 1, 2017

References:
- Utah Code Title 63G, Chapter 2, Government Records Access and Management Act (https://le.utah.gov/xcode/Title63G/Chapter2/63G-2.html);
- Utah Administrative Code Rule R895-7, Acceptable Use of Information Technology Resources (https://rules.utah.gov/publicat/code/r895/r895-007.htm); and

Purpose:
This policy addresses the use of mobile devices to access State data.

Definitions:
As used in this policy:

1. "DAS" means the Department of Administrative Services.
2. "DTS" means the Department of Technology Services.
3. "Mobile Device" means a mobile computing device (such as a mobile phone, smart phone, tablet computer, or laptop computer) that can access a State network and store information.
4. "Mobile Device Management" (MDM) means a technology system that is used to ascertain if mobile devices attempting to connect to the network have required security controls configured.
5. "State Data" means non-public information owned by the State of Utah. It includes State email, calendar, and contacts when used or stored outside of a web-browser.

Policy:
1. An employee using a mobile device to access state data shall follow DTS Policy 5000-0003 (Enterprise Mobile Device Policy).
2. An employee using State-owned or personal mobile devices to access or store State data is required to:
   a. Protect the mobile device from theft, damage, abuse, and unauthorized use.
b. Notify the employee's supervisor as well as the DTS Help Desk or Enterprise Information Security Office (###-###-####) within one hour if the mobile device is lost or stolen, or as soon as practical after the device is noticed to be missing.

c. Install Mobile Device Management software, drive encryption, or applications on the device prior to connecting it to State systems.

d. Use a 4-digit device password or thumbprint reader on the mobile device.

e. Use Anti-virus software if using an Android device.

3. By installing a Mobile Device Management agent on their personal mobile device, an employee agrees to:
   a. Allow the State access to the content stored on the device.
   b. Give the State the right to remotely disable or wipe the data stored on the mobile device in the event the device is lost or stolen.
   c. Hold the State harmless for any damage to the device or its operating system and related software as a consequence of using the State network, other computing resources, or the Mobile Device Management agent.

4. An employee may use a web browser on a personal mobile device to access email, calendar, contacts, or other State data available through a web-browser without installing a Mobile Device Management agent on the employee's personal mobile device if the employee signs out and closes the webpage after each session.

5. An employee using a State-owned mobile device may not modify the device or its operating system in any way which could potentially violate or void a manufacturer’s warranty or allow superuser administrative privilege to the operating system such as (but not limited to) “jailbreaking” an iOS device or “rooting” an Android device.