

---

# Mobile Device Management Guidelines [1]

## Topics:

GM-15-004 Mobile Device Management

Issue Date: 12/15/2014

Effective Date: 12/15/2014

## PURPOSE

Mobile devices are proliferating rapidly in the State enterprise. While the devices can enhance productivity, they also bring new requirements for proper technology management. Mobile Device Management (MDM) providers continue to mature and to offer greater control to IT departments that are trying to stay ahead of their end users. GTA recommends that all agencies use some form of MDM, and the following guidelines represent some high-level considerations each agency should evaluate.

## GUIDELINE

**I. Comply with enterprise policies and standards, as well as any outside regulatory requirements under which they are governed.** The following enterprise PSGs are applicable to mobile device management. They can be reviewed at this link:

<https://gta.georgia.gov/psg/> [2]

- 1) Acquisition and Use of Telecommunications Services and Equipment, [PM-04-002](#) [3]. Specific components of this Statewide policy, jointly issued by the Office of Planning and Budget and GTA, apply to wireless and mobile communications and computing. Look for the following components:
  - a) Specify criteria for determining whether an employee's communications needs dictate the use of a wireless or mobile device.
  - b) Specify criteria for determining whether a wireless or mobile device shall be authorized for a specific employee or unit.
  - c) Establish procedures for approving the acquisition of wireless or mobile devices.
  - d) Establish procedures for reviewing and approving continued use of wireless or mobile devices.
  - e) Establish documentation standards.
  - f) Indicate any additional steps responsible agency staff will take to contain the costs of operating wireless or mobile devices. This requirement may require an agency to add to its employee off-boarding procedures necessary steps to recover any telecommunications devices assigned to departing employees (retiring, voluntary departure, termination etc.) and to stop vendors?

(telecommunications carriers) invoicing for the recovered equipment according to contract provisions, if such provisions are in the contract.

g) Maintain an inventory of all wireless devices that lists each individual device, the service provider for such device and the individual (or in the case of shared wireless devices, the smallest identifiable organizational unit) to which the device is assigned,

2) Remote Access, [PS-08-023](#) [4]. Policy with general applicability to remote access,

3) Teleworking and Remote Access, [SS-08-037](#) [5]. Establishing Rules for Teleworking and Remote Access,

4) Appropriate Use and Monitoring [SS-08-001](#) [6]. Specify authorized and unauthorized uses of wireless or mobile devices. Provide notice to employees of authorized and unauthorized uses,

5) Non-State Technology and Computing Devices [SS-12-002](#) [7]. Rules of appropriate use and all other governance regarding information and data security apply to non-State issued technology devices used to access non-public State information and technology resources,

6) Privacy in the Workplace, [SS-12-001](#) [8]. Providing notice to employees expressly stating there is no right to privacy for any use of State owned telecommunications equipment and terms and conditions of use,

7) Wireless and Mobile Computing, [SS-08-039](#) [9]. The deployment and operation of open, unsecured wireless network access technology is prohibited,

8) Secure Remote Access, [SS-08-038](#) [10]. Standard related to remote access,

9) Use of Cryptography, [PS-08-024](#) [11]. Policy with general applicability to cryptography,

10) Cryptographic Controls, [SS-08-040](#) [12]. Standard related to cryptography, and

11) Social Media Guidelines [GM-11-002](#) [13]. Guidelines for the use of social media.

## **II. Implement recommended minimum controls for use of mobile devices. GTA recommends the following controls be implemented to manage any mobile communication or computing device:**

1. Employee written acknowledgement of State Terms of Use and statement of authorized/unauthorized usage of the device,

2. PIN lock ? requires users to enter a passcode when opening their device. The policy can include a period during which the PIN Lock is not required if the device was very recently used,

3. Encryption of data stored on the device? Many mobile devices encrypt locally-stored data

by default, while some do not. GTA recommends that devices be required to use encryption if available at a level dictated by the authorized usage and stored data,

4. Ability to wipe state data and email without destroying user?s personal information in the event the device is lost, stolen or otherwise compromised, and

5. Ability to detect the operating system version on a mobile device and to detect a device whose operating system is in a compromised state. This allows the agency to detect possible compromise by

a known vulnerability in an older operating system version or to detect actions such as ?jailbreaking? or ?rooting?. Jailbreaking and rooting allows users to ignore agency and state policies relative to mobile devices. GTA recommends agencies implement a policy against placing State data on devices that have been jailbroken or rooted, and establishing potential agency responses to such practices.

**III. Select from commonly used controls to implement the agency WLAN and provide for selected managerial controls.** Agencies may implement other controls depending upon their need and security categorization of planned usage. As an example, AirWatch Mobile Device Management is a deployed service for Georgia Enterprise Technology Services (GETS) through which an agency selects its own MDM controls from over 100 specific settings to implement its policies through the AirWatch web console. See [http://gta.georgia.gov/press-](http://gta.georgia.gov/press-releases/2012-03-19/gta-launches-new-service-mobile-device-management) <sup>[14]</sup>

[releases/2012-03-19/gta-launches-new-service-mobile-device-management](http://gta.georgia.gov/press-releases/2012-03-19/gta-launches-new-service-mobile-device-management) <sup>[14]</sup> for more information.

Minimum recommended controls are as follows:

1. Prevent or manage the use of unauthorized backup and synchronization services, to prevent State data from synchronizing to consumer cloud accounts. These could include native services like Apple?s iCloud or additional services like DropBox,
2. Prevent or manage the use of unauthorized apps on devices, by either blacklisting apps or by whitelisting only those apps that are approved for use,
3. Provide a secure browser experience for accessing browser-based applications,
4. Manage the authorization of email synchronization on a per-device basis,
5. Provide a secure container for State data on the device, so that it can be centrally managed and removed if necessary, and
6. Implement data loss prevention (DLP) controls to maintain appropriate control over State data, particularly regulated data.

## TERMS AND DEFINITIONS

**Wireless Device** ? Device that receives and/or sends transmission using wireless technology such as cellular or radio frequency (RF) signaling. Examples include cellular or PCS phones, blackberries, personal digital assistance with connectivity,

**Mobile Device** - Device that is portable rather than continuously connected via physical wiring to electricity or network connectivity

---

Source URL: <https://gta.georgia.gov/psg/article/mobile-device-management-guidelines>