GEORGIA DEPARTMENT OF CORRECTIONS Standard Operating Procedures		
Functional Area: Support Services Telecommunications	**Reference Number:** IVF02-0006	**Revises Previous Effective Date:** 11/01/2004
Subject: Wireless Devices		
Authority: Owens/Smith	**Effective Date:** 10/01/2014	Page **1** of **5**

I. POLICY:

A. To provide guidance for Georgia Department of Corrections' (GDC) staff to determine the need for wireless communication devices, and the usage, security, and compliance of these wireless devices with the Office of Planning and Budget (OPB) policy and the Georgia Computer Systems Protection Act. Assignment and reassignment of these wireless devices will be at the discretion of the Commissioner or his designee based on procedures outlined.

B. The Georgia Department of Corrections reserves the right to investigate, retrieve and read any communication or data composed, transmitted or received through voice services, online connections and/or stored on their respective servers.

II. APPLICABILITY:

All GDC employees assigned GDC wireless devices.

III. RELATED DIRECTIVES:

A. OPB Revised Policy on the Acquisition and Use of Telecommunications Services and Equipment dated December 16, 2008.

B. S.O.P. IV015-0010—Repayment for Failure to Return State-issued Property.

C. O.C.G.A. §16-9-90 (Georgia Computer Systems Protection Act).

IV. DEFINITIONS:

A. A wireless device is considered to be one of the following:

1. Cellular phone: A wireless phone that permits communication to and from mobile users within a specified area.
2. Smart phone: A cell phone that can handle phone calls, messaging and email. They often allow users to browse the internet.
3. Tablet with wireless access: A handheld device that combines computing, messaging, internet and networking features.
4. Commercial Frequency Two-way Radios: Digital radios operating on frequencies assigned to companies such as Southern LINC. These radios may have cell phone capability. They differ from radios that operate on public safety frequencies.
5. Mini Laptop: A laptop with access to the internet. No messaging or phone call capability.
6. Hotspot/Aircard: A wireless device that allows access to network for use with laptops.

V. ATTACHMENTS:

ATTACHMENT 1 - Justification for Wireless/Mobile Device

ATTACHMENT 2- Wireless Transfer Form

VI. PROCEDURE:

A. Determining the need for wireless devices

1. All requests for assignment of wireless devices (as defined in Section IV) shall be made in writing on the attached form entitled Justification for Wireless/Mobile Device.
2. State owned wireless devices may be assigned to staff who meets the criteria for assignment as defined on the attached form entitled Justification for Wireless/Mobile Device.
3. Approval from the employee's supervisor (i.e., Warden, Superintendent, or Office Director) **AND** the Division Director must be obtained prior to any further action being taken.
    i. Once the Wireless Support Office has received the approval from the Division office, the equipment will be ordered and shipped directly to the location that has made the request or will notify the location that the order is ready to be picked up.

4. Under no circumstances should an individual facility, unit or office procure their own wireless service and request payment for service from GDC until approval of a state-issued wireless device is secured.
5. Upon approval from the Commissioner or his designee, a pool wireless device may be made available to offices whose responsibilities require that a duty officer take calls 24 hours a day (i.e., Public Affairs, Engineering and Perimeter Security). Pool phones shall be rotated between duty officers. Officers are required to maintain logs of usage that must be submitted to appropriate managers.
6. Unless assigned as a pool wireless device, only the employee that is assigned a wireless device is permitted to use the wireless device for official state business only.
7. No reimbursement will be made to employees for use of their personal wireless device for conducting state business.

VII. WIRELESS DEVICE TRANSFER PROCEDURES

Wireless devices will be assigned to the user and relocated when the assigned user transfers or is reassigned to a different work site, as long as the new position requires a state-issued device. At the time of relocation, a wireless device transfer form must be filled out and submitted to the Wireless Support Office.

VIII. SEPARATION/TERMINATION FROM THE AGENCY

A. Upon separation or termination, a full security wipe of the device must be done by the User prior to departure from the agency.
    1. Supervising manager shall be responsible for ensuring the security wipe has been completed.

B. Employees are responsible for turning in all equipment and accessories (i.e. wall charger, car charger, keyboard case, holster case) that was originally issued. For any item that is not turned in, the assigned employee will be financially responsible for the replacement of those missing items.

VIX. LOST/STOLEN OR DAMAGED WIRELESS PROPERTY

A. Employees assigned a state-issued wireless device shall take proper care of the device. If lost, stolen, or damaged the employee may be held liable for reimbursement to GDC as outlined in SOP IV015-0010.

B. In the event a state-issued wireless device is lost, stolen, or damaged, the assigned user shall notify the Wireless Support Office immediately to ensure that all GDC information is wiped from the device and service is suspended.

1. If the device is stolen, a copy of the police report must be forwarded to the Wireless Support Office. The Division Director shall make the decision as to how the device will be replaced.

X. SECURITY

A. Protecting the information on the device

1. Assigned employee will protect the integrity of the information contained on any state- issued device by having a 4- digit passcode lock and ensuring that the assigned device is enrolled with GDC's mobile device management system.

B. Wireless Device Security Awareness Training

1. All GDC employees will be required to complete the Wireless Device Security Training each year.

XI. MONTHLY BILL REVIEW

A. An audit of the charges on wireless bills will be done on a monthly basis. Each Division Director shall be responsible for assigning a technology point of contact for their locations and notifying the Wireless Support Office. Each location shall use their assigned ID and password for the Tech Spend Report that is posted to Captiva to review the monthly charges.

B. Any discrepancies or unusual usage patterns will be reported to the Wireless Support Office.

1. In the event of any unusual usage patterns, the Division Director or their designee can request copies of the call detail from the Wireless Support Office.

XII. PROHIBITED USES OF STATE-ISSUED WIRELESS DEVICES

A. Conducting private or personal for-profit activities. This includes personal uses such as business transactions, private advertising of products or services and any activity meant to foster personal gain.

B. Conducting unauthorized non-profit business activities.

C. Conducting any illegal activities as defined by federal, state, and local laws or regulations.

D. Creating, accessing, or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating.

E. Creating, accessing, or participating in online gambling.

F. Infringement of any copyright, trademark, patent or other intellectual property rights.

G. Performing any activity that could cause the loss, corruption of or prevention of rightful access to data, or the degradation of system/network performance.

H. Conducting any activity or solicitation for political or religious causes.

I. Unauthorized distribution of state data and information.

J. Attempts to subvert the security of any state or other network or network resources.

K. Use of another employee's access for any reason unless explicitly authorized; attempts to modify or remove computer equipment, software, or peripherals without proper authorization.

L. Attempts to libel or otherwise defame any person.

XIII. MOBILE DEVICE MANAGEMENT

A. Every employee that is assigned a wireless device will ensure that said device is enrolled with GDC's Mobile Device Management Service.

B. Assigned employee will keep a secure passcode lock on the state- issued device to protect GDC information contained therein.

C. Each year employees assigned a GDC issued wireless device will be required to read and accept the GDC Terms of Use statement found in the mobile device management application.