Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 14.22

Subject:	Procurement and Management of State-Issued Wireless Devices
Information Contact:	DSHS Central Purchasing Unit
Authorizing Source:	WAC 292-110-010, Use of state resources Directive by the Governor 11-18 Office of the Chief Information Officer Policy 191 Cellular Devices DSHS Administrative Policies: Chapter 5, DSHS Records and Privacy 14.07, Control of Capital Assets; 15.15, Use of Electronic Messaging Systems and the Internet; 16.10, Reporting Loss of Public Assets to SAO; 18.64, Standards of Ethical Conduct for Employees; and DSHS Information Security Standards Manual section 3.9
Effective Date:	May 24, 2013
Revised:	January 18, 2018
Approved By:	Original signed by Sharon Swanson Senior Director, Policy and External Relations

Purpose

To manage the procurement, assignment, and use of Department-issued wireless devices, including cell phones, smartphones, air cards, tablets, netbooks, and other devices as applicable.

To define the appropriate use of these state resources to ensure Department business is conducted as economically and efficiently as possible, and to:

- Manage Department wireless devices and plans;
- Manage requirements for the request, approval, assignment, and return of wireless devices; and
- Manage guidelines and responsibilities for the use and monitoring of Department-issued wireless devices

Scope

This policy applies to all Department employees who assign, manage, or use Department-issued wireless devices.

Definitions:

Mobile Device Management (MDM): A system for administering mobile devices in an enterprise to ensure agency policies are applied and adhered to.

Media Sanitization: The removal of any DSHS data from media, so that the asset can be safely redeployed to another DSHS office, sold to the public, or destroyed**.**

Wireless Device: A portable device with cellular communications capability, including cellular phones, air cards, smartphones, tablets, netbooks, and similar electronic devices.

Wireless Coordinator(s): One or more individuals selected by a Program's appointing authority. Coordinators are responsible for policy compliance and ensuring the optimization of their Program's wireless accounts with assistance and guidance of the CPU Wireless Program Specialist. Coordinators will be delegated appropriate access on the contracted wireless provider's website to perform their specific duties.

Wireless Program Specialist: A position within DSHS responsible to ensure compliance of Agency wireless policy through coordination with other state agencies and contracted wireless providers. This position provides ongoing guidance, including plan and procurement recommendations, and account management and monitoring.

Wireless User: Any DSHS staff assigned a Department-issued wireless device.

Policy

A. Department Wireless Device Optimization Strategy:

1. With DSHS Partners:

    a. Wireless Coordinator(s) must use Department of Enterprise Services (DES) master contracts to open new wireless accounts and purchase wireless devices. Non-state contract purchases will be reviewed by the Central Purchasing Unit (CPU) on a case-by-case basis and require a documented compelling business justification be submitted to CPU;
    b. The CPU must coordinate with DES and contracted wireless providers to combine and centralize service plans within agencies to streamline billing and management; and
    c. The CPU must work with the Technology Services Division (TSD) and Enterprise Technology (ET) to ensure wireless devices that require a data plan meet minimum requirements for compatibility and security.

2. Inside DSHS:

    a. Department programs must appoint one or more Wireless Coordinator(s) to work in coordination with the Wireless Program Specialist and the program's field staff, to ensure compliance and optimization of wireless accounts and devices;

b. The administrations and programs must ensure employees are assigned to the most appropriate plan and services for the lowest available costs, while meeting the program's business needs.

B. Requirements for Issuing, Managing, and Returning Wireless Devices

1. Device Procurement Request and Approval

   a. Each program must identify the business needs for issuing wireless devices. Wireless Coordinators in coordination with the of the Wireless Device Program Specialist must identify the most appropriate contracted wireless provider and service plan to result in the lowest cost to the Department, while meeting the stated business need;
   b. Administrations and programs must follow the approved DSHS purchasing procedures and system to obtain procurement authorization from the applicable signing authority; and
   c. One or more of the following must be met to initiate a wireless device request:
      i. Employee's job requires field work where land-line phones or internet access are inaccessible or inefficient;
      ii. Employee's job requires field work, and a need for immediate or on-call availability, including email;
      iii. Safety issues associated with the employee's job responsibilities; or
      iv. Other documented and approved exceptions.
   d. Each DSHS employee must complete a Remote Access Form (03-443) prior to device assignment.

2. Device Assignment

   a. Asset tagging and the Mobile Device Management (MDM) system (see DSHS IT Standards Manual, IT Standard: 8.4. Mobile Device Security Settings) provides a record of the equipment and assignment to the responsible wireless user.
   b. Administrations are responsible for coordinating the asset management of the wireless devices before issuing the device to the end user;
   c. When a wireless device is issued by an administration/program:
      i. the device must be assigned to an individual staff member;
      ii. if the device is being issued to a work group, a primary individual within the work group must be assigned responsibility for the device;
   d. Administrations are responsible for determining whether their employees can have multiple data lines.

3. Monitoring Device Usage

a. Administrations are responsible for managing and retaining public records related to wireless device usage including, but not limited to, billing and usage records, according to the Retention Schedule.
b. Administrations are responsible for purging and retaining any photos or other data records saved on the wireless device in accordance with record retention schedules.
c. Administrations must monitor monthly billing statements and usage reports to identify employee eligibility, potential misuse, usage overages, proper billing and enforcement, and potential savings.
d. Administrations are responsible for keeping usage logs for shared workgroup devices. These logs will allow users to check a device in and out and can be referenced in monitoring activities.
e. If potential misuse of a Department-issued wireless device is suspected, the user's supervisor will be notified. It is the Administration's responsibility to investigate and decide what level of corrective or disciplinary action is required.

4. Device Return

a. The employee must return state devices to their supervisor when the employee leaves a position or is no longer an authorized wireless device user. It is the responsibility of the supervisor to contact their Administration's purchasing and asset staff to complete the return of the wireless device.
b. In the event the device is returned, the Wireless Coordinator will notify IT to update MDM.
c. Wireless service will be immediately cancelled or suspended as applicable, upon the exit or transfer of an employee with a wireless device. The contents of the device must be "wiped" in accordance with media sanitization standards and records retention schedules before the device is disposed of or reassigned. Any photos or other data records saved on the device must be retained in accordance with record retention schedules.
d. Upon cancellation, the wireless device must either be retained for backup or be disposed of and sent to the Facilities Maintenance Surplus Service Warehouse for handling.

5. Lost or Stolen Devices

In the event of a lost or stolen wireless device:

a. The employee must immediately notify their supervisor.
b. The supervisor notifies the Enterprise Technology Service Desk.
c. The Enterprise Technology Service Desk:
   - Notifies the administration's Mobile Device Management Team;
   - The DSHS Wireless Program Specialist; and,
   - The administration's Wireless Coordinator.

- Sends the employee the Loss of Public Funds, Assets, or Illegal Activity Report form 17-169, to be filled out by the employee within one business day if the device is not found.

C. General Use, Records, and Security Guidance

1. The employee in possession of the Department-issued wireless device is responsible for the proper use of the device. Use of any Department-issued wireless devices must be in accordance with all existing RCW, WACs, agency policies, and state security standards regarding the appropriate use of state resources and communication devices, including, but not limited to, those listed in the Authorizing Source section of this policy.

2. The physical security of wireless devices is the responsibility of the authorized employee and must be kept in their physical presence whenever possible. Wireless devices that can access state resources must not be left unattended and must be locked in an enclosed area when stored.

3. All contents of a Department-owned wireless device including calls, usage, billing and data records, photos, and any personal data on the device are deemed public records. These records may be subject to records retention requirements, public disclosure requests, litigation hold, review, or audit. Employees should not expect privacy on Department-issued devices and communications.