

SUBJECT: Internal Controls for the Management of Mobile Communications Devices

NUMBER: 107- 001-015

DIVISION: Office of the Director

EFFECTIVE DATE: 01-01-2010

APPROVED: 

POLICY/ PURPOSE: This policy identifies minimum standards for agency internal controls relating to the management of charges for the use of Mobile Communication Devices (MCDs).

AUTHORITY: ORS 291.015, ORS 291.016, ORS 291.018, ORS 291.026, ORS 291.034, and ORS 291-038

APPLICABILITY: All Executive Branch agencies under direct authority of the Governor. Other agencies may follow this policy at their option.

DEFINITIONS:

Access Account
The account of each access number for voice/data transmission provided by a mobile communications provider.

Authorized User
The person or entity authorized to use the access number on the Access Account.

Mobile Communication Device (MCD)
A text messaging device or a wireless, two-way communication device designed to receive and transmit voice or text communication including mobile Global Positioning System (GPS). This policy applies to any Mobile Communication Device that requires the purchase of mobile communication services by the state.

Plan Charge
The charge assessed by a data or voice provider for each Access Account.

Texting
The act of sending a written message using a MCD such as a cell phone, BlackBerry or GPS.

ATTACHMENTS: Acceptable Use Agreement

GUIDELINES:

- I. General Use at work:
- Privately owned MCDs being used for personal calls should be used sparingly in the workplace.
 - MCDs are assigned to state employees in order to carry out their work while conducting state business.
 - The MCD can also be used as a pager for receipt of voice or text messages.
 - MCDs assigned to state employees are primarily for business use with occasional personal use as identified on a monthly basis and reimbursed through payroll deduction. MCDs are to be protected by the employee, used in an appropriate manner, and returned when employment ends.
 - Monthly charges for use of MCDs will be monitored for devices issued to employees and allows an employee's manager to determine the consequences of excessive or irregular use.
 - Use of camera phones is prohibited in restrooms and areas where confidential information is located.

Statewide Manual

POLICY NAME: Internal Controls for the Management of MCDs

POLICY NUMBER: 107-001-015

PROCEDURES:

Step Responsible Party

Action

1. Agency Director

Each agency director is responsible for:

- a. Ensuring that their agency has sufficient safeguards in place to ensure that expenditures for mobile communications are restricted to those necessary for the conduct of official state business. This includes ensuring that there are sufficient internal controls.
- b. Ensuring appropriate usage of MCDs (i.e. Restrictions on Personal Calls) and compliance with applicable rules and policies (i.e. Confidential information, Use while Driving according to Statewide Policy 107-001-016.
- c. Ensuring that only charges incurred by Authorized users conducting official state business are paid by the State; and
- d. Ensuring that Authorized Users are on the most cost effective plan for their type of use.
- e. Designating a Mobile Communication Plan Coordinator in writing with authority to open, manage and cancel Access Accounts.

2. Division Administrator

The division administrator is responsible to enforce this policy and:

- a. Informing employee of this policy and obtaining employee signature on Acceptable Use Agreement for all employees operating a motor vehicle in the scope of employment.
- b. Providing a good example of MCD use, and in guarding against excessive or inappropriate use of such devices by employees.
- c. Maintaining accurate record of violations of this policy.
- d. Implementing a mobile device maintenance program that includes pre-trip inspections, immediate withdrawal from service of any device with mechanical defects, and regular inspection and maintenance.

3. Mobile Communication Plan Coordinator

Each Mobile Communication Plan Coordinator is responsible for:

- a. Opening Access Accounts by authorizing vendors to issue Access Account numbers for Authorized Users.
- b. Managing Access Accounts by:
 - i. Maintaining a list of all MCD Access Accounts and corresponding Authorized User (employee names) with corresponding personnel identification numbers. List will also identify any special purpose accounts for audit purposes.
 - ii. Serving as a contact and liaison between Agency, Divisions and the vendor.
 - iii. Ensuring that specific staff is assigned to monitor Plan

Statewide Manual

POLICY NAME: Internal Controls for the Management of MCDs

POLICY NUMBER: 107-001-015

charges including use by unauthorized users, appropriateness of plans, and personal use.

- c. Ensure that MCDs are securely stored when not assigned to Authorized Users.
- d. Cancelling Access Accounts when Authorized Users terminate state service and when MCDs are lost or stolen or access is disconnected for cause. Reporting information security incident/event when the MCD is lost or stolen.
- e. Securing removal or destruction of sensitive information prior to disposal or surplus of MCDs.

4. Supervisor of the Authorized User

The Supervisor of the Authorized User is responsible for:

- a. Determining if a valid business reason exists to provide a MCD and authorize Plan Charges for an Authorized User. Examples of valid business reasons include:
 - i. Official duties require the worker to be "on-call" away from workstations.
 - ii. Official duties require travel during their normal assigned work time.
 - iii. Official duties expose staff to danger.
 - iv. Official duties require an emergency or time-critical response.
 - v. Cost of device is justified by the gain in operational efficiency.

Issuance of a MCD and the authorization of Plan Charges expose the agency and state to liability for all charges resulting from the use of the MCD. Agencies need to be able to identify a business need when determining if the issuance of a MCD is necessary.

- b. Ensuring that the Authorized User:
 - i. Has received training on acceptable use, understands their responsibilities and signs an Acceptable Use Agreement.
 - ii. Knows the importance of protecting confidential and sensitive information contained on a MCD that can be released during voice/data transmissions or with the loss or theft of a MCD.
 - iii. Receives a copy of the policy.
- c. Coordinating with the agency's Human Resources office on mobile communications issues. Possible sanctions for misuse could include:
 - i. Forfeiture of Access Account;
 - ii. Required reimbursement of personal or other inappropriate use;
 - iii. Disciplinary actions including dismissal; and
 - iv. Criminal charges.
- d. At least annually, review and validate Plan Charges and Authorized Users to ensure that expenditures for Plan charges meet the requirements under this policy.

Statewide Manual

POLICY NAME: Internal Controls for the Management of MCDs

POLICY NUMBER: 107-001-015

5. Authorized User

The Authorized User is responsible for:

- a. Taking reasonable steps to ensure the physical security of MCDs. Report missing, lost or stolen MCDs to their Supervisor and Mobile Communication Plan Coordinator immediately.
- b. Using the MCD in a manner consistent with the Acceptable Use Agreement.
- c. Taking reasonable steps to prevent the release of confidential or sensitive information either during the voice/data transmission or from the loss/theft of the MCD.
- d. Understanding that sanctions, including dismissal, may result from the unauthorized use of the MCD.
- e. Understanding that using a MCD while driving a vehicle on state business requires the use of a hands-free accessory unless specifically exempt. Any traffic violations or payment of fines imposed for violation of any applicable laws are the Authorized User's personal responsibility.

Statewide Manual

POLICY NAME: Internal Controls for the Management of MCDs

POLICY NUMBER: 107-001-015

Acceptable Use Agreement

I, _____ acknowledge I am being granted use of state information assets in order to carry out my work and agree that my use of such assets will be conducted in a manner that ensures compliance with this Policy, Policy 107-01-010, and Policy 107-001-015, Oregon Accounting Manual Policy 40.10.00 PO and by Statewide Policy 107-001-016, Mobile Communication Device Usage While Driving.

I agree that any personal use of any provided Mobile Communication Device, will be identified on a monthly basis, and reimbursed to the agency through Payroll Deductions. I further understand that any personal use is also subject to taxation of the user.

I understand my usage will be monitored, without further warning, and that inappropriate usage may be cause for disciplinary action, including but not limited to reprimand, suspension, and termination of employment or Civil or criminal prosecution under federal and state law.

I understand that I must use a hands-free accessory when driving a motor vehicle while using a Mobile Communication Device, except where exclusions apply. Any traffic violations or payment of fines imposed for violation of any applicable laws are my personal responsibility.

I understand that the use of state information assets may be revoked at any time without further warning.

I acknowledge, I have read and understood this document by signing below. I further understand it is my responsibility to seek advice regarding any questions I might have regarding this document or policy prior to my signing.

_____ Employee Signature	_____ Manager/Supervisor Signature	_____ Date
_____ Print Name	_____ Print Name	_____ Date