PA TURNPIKE COMMISSION POLICY *This is a statement of official Pennsylvania Turnpike Policy*		**NUMBER**: 8.07 **APPROVAL DATE**: 09-18-2007
POLICY SUBJECT: **Mobile Device Policy**	**RESPONSIBLE DEPARTMENT:** **Information Technology**	**EFFECTIVE DATE**: 11-20-2014 **REVISED DATE**: 11-04-2014

A. **PURPOSE**:
This policy governs the assignment of Commission-owned mobile devices to staff and the use of those devices to access Commission Technology Resources, and also provides guidelines for the use of employee-owned mobile devices, including smartphones and tablets, to access Commission Technology Resources.

B. **SCOPE**:
This policy applies to all Commission authorized users including full-time, temporary, supplemental, and summer employees ("Employees"), and contractors and independent consultants ("Contractors and Consultants") who access Commission Technology Resources such as email, documents, and Internet connectivity using Commission Managed Mobile Devices which include Commission-owned mobile devices, employee-owned mobile devices, and contractor/independent consultant-owned mobile devices (collectively "Authorized Users").

C. **GENERAL POLICY**:

1. All Managed Mobile Devices:

Any mobile device used to access Commission email or other authorized applications and resources – whether owned by the Commission, employees, or contractor/independent consultants – must have the Commission's Mobile Device Management (MDM) solution installed on it to enforce security settings and to allow the Commission to manage Commission data including, but not limited to, email, calendar entries, and Commission contacts in case the mobile device is returned, transferred, misplaced, lost, or stolen or in other circumstances as determined in the Commission's sole discretion.

Authorized Users should recognize that their use of, or access to, data provided by or through Commission Technology Resources may be traced, audited, accessed, reviewed, and/or monitored by the Commission or its authorized agents at any time, with or without notice to the Authorized User.

Authorized Users must accept that, when connecting a managed mobile device to Commission Technology Resources, the Commission's security policy will be applicable to the device. The security policy implemented may include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity and encryption.

An Authorized User will be allowed to utilize authorized Commission applications and resources provided that the Authorized User agrees to comply with and abide by this and any other Commission policy concerning electronic communications including, but not limited to, Policy 8.1 (Acceptable Use of Commission Technology Resources), and obtains the required management authorizations. The Commission, in its sole discretion, may terminate any and all connections to Commission Technology Resources without notification.

The Commission provides applications to support business purposes. These Commission applications also help to ensure the confidentiality of sensitive data, prevent data loss, and support records management requirements. Authorized Users should use Commission provided business applications (including email) when conducting Commission business. Further, if a user is notified that Technology Resources in his or her possession are subject to a litigation or records hold, s/he must take the steps necessary to comply with the hold requirements.

Authorized Users must take proper care of their managed mobile device(s). For example, these devices must not be left unattended in plain view, even for a short period of time; must not be left in a vehicle overnight; and must not be left unattended for any reason in vulnerable situations (e.g., public areas such as airport lounges, hotels and conference centers).

Lost or stolen managed mobile devices must be reported to the Service Desk or Network Control within 24 hours or when reasonably practical. This notification must take place prior to any cancellation of mobile voice and data services associated with the device.

Authorized Users must take appropriate precautions to prevent others from obtaining access to their Commission Technology Resources and data. Authorized Users must keep confidential, sensitive, or privileged information separate from personal data. Authorized Users shall not share with anyone assigned passwords, PINs or other credentials that provide access to Commission Technology Resources or share Commission data without authorization.

Authorized Users must take all reasonable steps to protect against the installation of malicious applications. This includes, but is not limited to, applying patches and updates provided by the mobile device manufacturer/carrier as they are made available.

Commission-managed mobile devices may not be “rooted” or “jail-broken” to allow the bypass of built-in security controls.

Authorized Users are prohibited from typing, reading or sending any information from their device while driving.

Authorized Users are prohibited from activating their device as a hot spot while at Commission facilities that have wireless capabilities.

Authorized Users must comply with data copyright requirements.

Authorized Users who do not comply with or abide by the policies detailed in this document shall be subject to revocation of the mobile device privileges. Employees may be subject to additional disciplinary action up to and including termination. Contractors and Consultants may be subject to additional actions as specified in their contract, as well as under the Commonwealth's Contractor Responsibility Program.

2. Commission-Owned Mobile Devices

Mobile devices will be assigned to Authorized Users whose work location and/or job responsibilities require that they are available and reachable at all times or the assignment of a mobile device is determined to be operationally necessary by their direct report to the CEO/COO.

These devices are Commission property and intended for Commission business but may be used for limited personal use in accordance with the Acceptable Use of Technology Resources Policy, the Commission's Code of Conduct, and other Commission policies. For voice capable devices, Authorized Users will be enrolled in a shared pool plan in which all Authorized Users will share a pool of minutes for the entire Commission. Authorized Users will also have access to any additional features offered by the mobile carrier's current contract with the Commission. Currently, this includes unlimited data and texting for devices that are capable of supporting data and texting. Plan details and additional capabilities are subject to change without notice.

Authorized Users shall accept and may not change settings on the device that the Commission deems necessary to adequately secure the information on the device. Authorized Users acknowledge that any and all data on the device is subject to Commission review without notice.

If a device is misplaced, lost, or stolen, the Authorized User must notify the Service Desk or Network Control within 24 hours or when reasonably practical. The Commission may, at its own discretion, remotely wipe all data from the device and shall not be held responsible for the loss of any personal data that may have been on the device. Authorized Users are responsible for protecting any personal data on the device.

Authorized Users have no expectation of privacy when using Commission Technology Resources (including but not limited to information contained in text messages, emails, photos, internet access, telephone calls, and call logs contained or reflected on the Commission-owned device), which may be reviewed, copied and monitored by the Commission and/or produced to others by the Commission at any time, with or without notice to the Authorized User.

Phone records may be subject to audit to ensure compliance with all policies and procedures.
Authorized Users shall surrender mobile devices and provide device access codes to the Information Security Office immediately upon request from the Information Security Office for audit, e-discovery, investigative or law enforcement purposes.

Authorized Users may not wipe/erase Commission-owned mobile devices issued to them.

Authorized Users may not share Commission-owned mobile devices with anyone outside the organization, including family, friends or business partners.

Authorized Users may download and use applications from commercial or Commission-owned app stores provided the applications comply with Commission policies. Authorized Users are responsible for all costs not associated with and approved for Commission use including, but not limited to, personal applications and chargeable vendor features.

All costs associated with mobile device cellular service will be charged to the Authorized User's department. Such costs include, but are not limited to, equipment, initiation fee, monthly fees, non-customary charges, maintenance and repair of equipment, and programming and replacement of lost, stolen or damaged equipment.

3. Employee-Owned Mobile Devices

Employees wishing to use their personal device (i.e. BYOD) to access Commission email or other authorized applications will require prior approval from their direct report to the CEO/COO. Initial access will be limited to Commission email. Access to additional resources will require specific management approval. Employees may only use an authorized Commission email client to access their Commission email.

Employees who are granted access to the Commission's applications and resources (including email) must allow the installation of the Commission's MDM software on their device. This product must be installed to allow the Commission to provide security settings and to allow the Commission to manage any Commission data, including but not limited to, email, calendar entries, Commission contacts, and other Commission data, in case the mobile device is returned, transferred, misplaced, lost, stolen or under other circumstances as determined in the Commission's sole discretion.

If a device is misplaced, lost, or stolen, the Employee must notify the Service Desk or Network Control within 24 hours or when reasonably practical. The Commission may, at its discretion, remotely wipe/erase all Commission data on the device. If requested by the Employee, the Commission may, in its sole discretion, also attempt to issue a complete wipe/erase of the device. The Employee may not cancel the mobile cellular service for the device until a remote wipe/erase of Commission data is completed. The Commission shall not be held responsible for any personal data or apps inadvertently deleted while attempting to manage Commission data.

Upon termination of employment, or at any time within the Commission's sole discretion, the Commission may remotely remove all Commission applications and data from the device.

The Commission assumes no responsibility for loss or damage associated with the use of an employee-owned device. Support for employee-owned devices, including backing up personal information and data, is the employee's responsibility.

Employees must maintain a device compatible with the Commission MDM platform. If a device falls out of compliance, it will be blocked from accessing Commission email and other authorized applications.

The Commission will provide mobile device reimbursement for Commissioners, the CEO, COO and their direct reports. Upon recommendation from a direct report to the CEO/COO, and approval by the COO, other Employees may also receive reimbursement. The reimbursement will be a standard amount based on the current costs for a single line consumer plan from the Commission's preferred mobile carrier. No additional reimbursement will be provided for additional devices or actual costs above the provided amount. The reimbursement amount will be reviewed regularly by the Information Technology Department which will recommend adjustments as needed to the CEO. The Information Technology Department will maintain a list of all Employees receiving reimbursements.

4. Contractor/Independent Consultant Owned Mobile Devices

The Commission, in its sole discretion, may make mobile access to Commission Technology Resources available through Contractor and Consultant-owned devices. In these instances, Contractors and Consultants must agree to and comply with all of the requirements identified for Employee-owned devices above.

Contractors and Consultants and the employee responsible for managing the Contractor's and Consultant's engagement must notify the Information Security Office upon the termination of the engagement for which the Contractor and Consultant obtained access to Commission Technology Resources. Upon notification, the Information Technology Department will remotely remove all Commission applications and data from the device. The Commission may, in its sole discretion, also terminate access to Commission Technology Resources at any time.

D. **DEFINITIONS**:

Authorized Users - Any employee who receives compensation from the Commission on an hourly, daily, or annual basis including full time, part time or probationary or is authorized by statute ("Employees"), and Contractors and Independent Consultants that use or have access to Commission Technology Resources.

BYOD – Bring your own device (BYOD) is the policy of allowing employees to bring personally owned mobile devices to the workplace, and use those devices to access Commission Technology Resources.

Managed Mobile Device – A mobile device – whether it is owned by the Commission or the Employee or a Contractor/Independent Consultant – that is secured and managed by the Commission's Mobile Device Management solution.

Mobile Device – A communications device that transmits and receives data, text, and/or voice without being physically connected to a network. This definition includes but is not limited to such devices as Smartphones, Tablets, and voice only cell phones.

Mobile Applications – This refers to software designed for any or all the mobile devices defined in this policy.

Mobile Device Management (MDM) – The Commission's solution for securing and managing mobile devices that access Commission Technology Resources.

Technology Resources – Commission Technology Resources include, but are not limited to, the following: all Commission data and records, including those pertaining to computer use, internet use, email communication and other electronic communication (whether sent, received, or stored), as well as the content of such communications; Commission's computer systems, together with any electronic resource used for communications, which includes but is not limited to laptops, individual desktop computers, wired or wireless telephones, cellular phone, smartphones, tablet computers, servers, virtual machines, routers/switches, etc. and further includes use of the internet, electronic mail (email), instant messaging, texting, voice mail, facsimile, copiers, printers or other electronic messaging through Commission facilities, equipment or networks.

Wi-Fi Hot Spot – A feature on a mobile device that allows it to become a wireless Internet access point.

E. **PROCEDURES**:

1. **The Service Desk Request** process will be used for all requests related to mobile devices.

2. **Commission-Owned Mobile Devices** may be assigned in accordance with the following guidelines:

    - Requests to obtain mobile devices, additional or replacement equipment, or additional features, such as hot spot capabilities, must include work-related justification.

    - A signed Mobile Device Policy Acknowledgement form (Attachment A or B, as appropriate) must be on file with the Information Technology Department.

    - The device will be added to the Human Resources list of objects on loan assigned to the employee and must be surrendered upon the end of or suspension from employment or at any time within the Commission's discretion.

    - Devices provided to Contractors and Consultants must be surrendered upon the conclusion of their engagement with the Commission or at any time within the Commission's discretion.

3. **Employee-Owned Mobile Device Access** to Commission email and other authorized applications may be allowed in accordance with the following guidelines:

    - Requests for authorization to access Commission email and other authorized applications must include work-related justification for the access.

- A signed Mobile Device Policy Acknowledgement form (Attachment A) must be on file with the Information Technology Department.

- A signed Employee-Owned Mobile Device Reimbursement Request form (Attachment C) must be completed by Commissioners, the CEO, COO and their direct reports and forwarded to Payroll.

4. **Contractor/Independent Consultant-Owned Mobile Device Access** to Commission email and other authorized applications may be allowed in accordance with the following guidelines:

    - Requests for authorization to access Commission email and other authorized applications must include work-related justification for the access.

    - A signed Mobile Device Policy Acknowledgement form (Attachment B) must be on file with the Information Technology Department.

5. **Support for mobile device access to Commission Technology Resources**

    - Full Support for Commission-Owned devices – The Information Technology Department will support operating systems, hardware, connectivity, and Commission-approved applications.

Limited support for Employee-owned and Contractor/Independent Consultant-owned devices – Support is limited to Commission- managed applications. Primary support for user-owned devices is the user's responsibility. Users may be required to present their device to an IT support representative for installation or troubleshooting of Commission-managed applications. Other issues should be directed to the user's mobile device provider. Because of the numerous options that exist for both mobile devices and operating systems, there are no guarantees that any given application will work on a specific device.

6. **Exceptions**

    - Any exception to this policy must be approved in advance by the Chief Information Officer (CIO).

This Policy Letter supersedes all previous Policy Letters on this subject.

Attachment A

Mobile Device Policy

Employee Acknowledgement

I acknowledge that I have read Policy Letter 8.7, Mobile Device Policy, in full and understand the terms of use and my responsibilities as an Authorized User. I agree to abide by and comply with the terms of this policy and agree to fully and to the best of my ability comply at all times with the responsibilities of Users contained herein.

I make no claims on the Commission to protect any personal data and fully understand that I have accepted the terms of this policy without coercion of any kind from my employer.

I understand that violations of this agreement can result in revocation of Commission mobile device privileges, including BYOD eligibility, and may subject me to disciplinary action, up to and including termination.

The Commission can, at any time, and in its sole discretion, modify this user agreement and require device users to reconfirm their agreement to abide by and comply with the terms of the modified agreement.

Employee Name (printed): _____

Employee Signature: _____

Date: _____

Attachment B

Mobile Device Policy

Contractor or Independent Consultant Acknowledgement

I understand that this user agreement is not intended to interfere with contractors or independent consultants, such as myself, from performing services required by their respective contracts with the Commission.

I hereby acknowledge that I have received, read, and understand the Mobile Device Policy, and agree to abide by and comply with the requirements set forth in it.

I understand that the Commission may revoke my privileges at any time for any reason, and/or take appropriate action as specified in my contract with the Commission, as well as under the Commonwealth's Contractor Responsibility Program.

The Commission can, at any time, and in its sole discretion, modify this user agreement and require mobile device users to reconfirm their agreement to abide by and comply with the terms of the modified agreement.

Print Name: _____

Company: _____

Signature: _____Date: _____

Attachment C

Employee-Owned Mobile Device Reimbursement Request

I acknowledge that I have read Policy Letter 8.7, Mobile Device Policy, in full and understand the terms of use and my responsibilities as an Authorized User. In accordance with that policy, I am requesting reimbursement for the use of my personally-owned device. I understand that the reimbursement being provided is a standard amount based on the current costs for a single line plan from the Commission's preferred mobile carrier and that no additional reimbursement will be provided for additional devices or actual costs above the provided amount. I understand further that the reimbursement amount will be reviewed regularly and adjusted as needed.

I understand that reimbursements will be provided starting the first pay period after the start date provided below. I further understand that I can revoke this request by resubmitting this form with the Start Date left empty and providing an End Date.

Name (Print)	Employee ID
Title	Start Date
Signature	End Date (Leave blank unless you wish to stop Receiving reimbursements)