| PA TURNPIKE COMMISSION POLICY<br>*This is a statement of official Pennsylvania Turnpike Policy* | | **NUMBER**: 8.07<br>**APPROVAL DATE**: 09-18-2007 |
|---|---|---|
| **POLICY SUBJECT:**<br>**Mobile Device Policy** | **RESPONSIBLE DEPARTMENT:**<br>**Information Technology** | **EFFECTIVE DATE**: 11-20-2014<br>**REVISED DATE**: 11-02-2020 |

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 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 who use Managed Mobile Devices to access Commission Technology Resources.

C. **GENERAL POLICY**:

**1. All Managed Mobile Devices:**

**Mobile Access to Email**
All PTC Authorized Users with PTC-credentials can access PTC mail, calendar and contacts on their mobile devices or a computer using a web browser and Outlook Web Access (OWA). Outlook Web Access does not store email data permanently on the device, so there is no automated long-term storage of PTC data on the device. Mobile apps store data within the app on the device, creating a security risk if the device is accessed by unauthorized users. Accessing PTC email and related data through mobile apps requires the Commission's Mobile Device Management (MDM) solution be installed on the device to enforce security settings, making it a "managed device." This is available for any mobile device – whether owned by the Commission, employees, or contractors/independent consultants – with a need to access Commission email or other authorized applications and resources.

**Mobile Device Management**
The MDM solution allows the Commission to remotely delete managed apps in case the mobile device is returned, transferred, misplaced, lost, or stolen or in other circumstances as determined in the Commission's sole discretion.

**Expectations of Privacy**

PTC Authorized Users have no expectation of privacy when using Commission Technology Resources, including PTC email and PTC-owned mobile devices (see Policy Letter 8.01 Acceptable Use of Technology Resources).

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 applies to the device. The security policy implemented may include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity and encryption.

The following clarifies what PTC can and cannot access on a mobile device:

- **Personal devices:** PTC only has remote access to basic information about the mobile device, including device make, model, operating system, serial number and owner name. PTC does not have remote access to the employee's calling and web browsing history, text messages, personal email, contacts, calendar, passwords, photos or files. PTC only has remote access to PTC emails and files in apps managed through the PTC MDM solution.

  PTC can delete these apps or the data they contain at any time, without disturbing personal data and apps. PTC cannot delete other data on the mobile device or reset the device to factory settings. The Commission may, in its sole discretion, terminate access to Commission Technology Resources at any time.

- **PTC-owned devices:** Like with personal devices, PTC has remote access to basic information about the device, including device make, model, operating system, serial number and owner name. PTC does not have remote access to the employee's calling and web browsing history, text messages, personal email, contacts, calendar, passwords, photos or files. PTC only has remote access to PTC emails and files in apps managed through the PTC MDM solution.

  Because a PTC-owned mobile device is PTC property and is intended primarily for PTC-related business, PTC can delete managed apps or reset the device to factory settings at any time, with or without cause.

**Acceptable Use**

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 Letter 8.01 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 and 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 available to conduct Commission business. Further, if a user is notified that its Commission Technology Resources are subject to a litigation or records hold, the user must take the steps necessary to comply with the hold requirements.

Authorized Users are prohibited from texting from their mobile devices while driving. Authorized Users are expected to always follow applicable local, state, and federal laws and regulations regarding the use of electronic devices. Authorized Users who are charged with traffic violations resulting from the use of their Managed Mobile Devices will be solely responsible for all liabilities that result from such actions and may be subject to discipline.

Authorized Users working in hazardous areas must exercise caution when using Managed Mobile Devices while in those areas, as such use can potentially be a safety hazard.

Authorized Users must comply with data copyright requirements. Employees may not store proprietary information from or related to former employment on the Commission's Mobile Devices. PTC's policy is to respect copyright and trade secret provisions. Users must refrain from using mobile device cameras to record proprietary or sensitive information without prior authorization from their supervisor.

As with other types of authorized work, all time spent by nonexempt, hourly employees using mobile devices for work purposes will be considered hours worked and the time is compensable and will count toward overtime eligibility as required by law. Nonexempt, hourly employees may not use their mobile devices for **work purposes** outside of their normal work schedule without prior authorization from management. This includes all types of **work-related** communication. Similarly, employees may not use their mobile devices for **work purposes** during periods of unpaid leave without prior authorization. Employees may, however, use their mobile devices for non-work purposes outside of their normal work schedule and during periods of unpaid leave in accordance with Commission policies.

**Mobile Device Security**

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).

Authorized Users must take appropriate precautions to prevent others from obtaining access to their Commission Technology Resources. 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.

Authorized Users are expected to exercise the same discretion using their personal devices as is expected for the use of company devices. Commission policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Authorized Users who do not comply with or abide by the policies detailed in this document shall be subject to revocation of access to Commission Technology Resources, including 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 when it 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 (8.01), the Commission's Code of Conduct, and other Commission policies and IT standards.

Authorized Users shall surrender Commission-owned 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 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 the Commission-owned devices, and any associated data on said 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 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.

Phone records may be subject to audit to ensure compliance with all policies and procedures.

**3. Personal 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 supervisor. Additionally, the Commission's MDM solution must be installed and active on their device. Otherwise, they will be limited to using OWA to access PTC email.

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 the requirements identified for personal mobile devices.

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. 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.

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 applications.

**4. Personal Mobile Device Reimbursements**

The Commission will provide reimbursement for using personal devices for Commissioners, the CEO, COO and their direct reports. With approval from 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 to the CEO as needed. The Human Resource Department will maintain a list of all Employees receiving reimbursements.

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 and business applications, located both on premises and cloud-based, 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 IT Security within 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 IT Security within the Information Technology Department.

    - If applicable, an Employee-Owned Mobile Device Reimbursement Request form must be submitted using the IT Service Portal.

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 IT Security within 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 Technology Officer (CTO).

*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 Authorized Users contained herein.

I expressly acknowledge that: (1) I have no expectation of privacy except that which is governed by law when using Commission Technology Resources; (2) I will not text while driving; and (3) the Commission will not be responsible for any loss or damage of personal applications or data resulting from the use of a Managed Mobile Device.

I understand that violations of the Commission's Mobile Device Policy 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 its Mobile Device Policy and require Authorized Users to reconfirm their agreement to abide by and comply with the terms of the modified policy.

**Employee Name (printed): _____**

**Employee Signature: _____**

**Date: _____**

Attachment B

# Mobile Device Policy

## Contractor or Independent Consultant Acknowledgement

I understand that the Commission's Mobile Device Policy 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 Commission's Mobile Device Policy, and agree to abide by and comply with the requirements set forth in it.

I expressly acknowledge that: (1) I have no expectation of privacy except that which is governed by law when using Commission Technology Resources; (2) I will not text while driving; and (3) the Commission will not be responsible for any loss or damage of personal applications or data resulting from the use of a Managed Mobile Device.

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 or my employer's 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 its Mobile Device Policy and require Authorized Users to reconfirm their agreement to abide by and comply with the terms of the modified policy.

**Print Name: _____**

**Company: _____**

**Signature: _____**

**Date: _____**