PA TURNPIKE COMMISSION POLICY *This is a statement of official Pennsylvania Turnpike Policy*		**NUMBER**: 5.03 **APPROVAL DATE**: 10-03-2011
POLICY SUBJECT: Access Control Policy	**RESPONSIBLE DEPARTMENT:** Facilities and Energy Management Operations; Traffic Engineering and Operations	**EFFECTIVE DATE**: 10-23-2014 **REVISED DATE**: 10-07-2014

A. PURPOSE:

To establish a policy to manage access at the Pennsylvania Turnpike Commission (PTC). Managed access will provide a safer work environment and contribute to the protection of PTC assets.

B. SCOPE:

This policy applies to all PTC employees including full-time, temporary, supplemental, and summer, as well as contractors, subcontractors, consultants, subconsultants, concessionaires, authorized service providers, emergency response companies, and government agencies and entities.

C. GENERAL POLICY:

Access at PTC facilities, gates, and other access points must be managed at all times, including access to sensitive or restricted areas within PTC facilities.

Access is managed using security controls such as card-operated locks and mechanical locking mechanisms. In order to gain access at PTC facilities, gates, and other access points, authorized personnel must use their assigned ID access card, key, or other security control.

Authorized personnel are required to display their ID access cards at all times.

Visitors -

All visitors are required to sign in upon arrival and sign out upon departure from a PTC facility. Upon signing in, the visitor will be issued a visitor ID badge, which must be worn during the entire visit at the PTC facility. Visitors must remain in the reception area until they are accepted by an employee from the department related to their visit. The accepting employee must escort the visitor or arrange for an escort during their visit and ensure that the visitor signs out at the end of their visit.

Anyone without a valid ID access card programmed for door access must follow established PTC visitor procedures.

D. DEFINITIONS:

Active Employee – Any PTC employee in compensable status. The term does not include PTC retirees or employees on S&A, Workers' Compensation, non-intermittent FMLA, Union Leave or Personal Leave.

Authorized Personnel – Active PTC employees and contractors, subcontractors, consultants, subconsultants, concessionaires, authorized service providers, emergency response companies, and government agencies and entities that have been provided with ID access cards or other security control devices programmed for access at doors or other access points.

Consultant – An individual or an individual employed by a firm, partnership, corporation, or joint venture awarded a contract by the PTC. The provisions of this policy are binding upon each consultant and subconsultant.

Contractor – An individual or an individual employed by a firm, partnership, corporation, or joint venture awarded a contract by the PTC. The provisions of this policy are binding upon each contractor and subcontractor.

FEMO Department – The PTC Facilities and Energy Management Operations Department.

Gate or other Access Point – A moveable structure or similar barrier that controls non-tolled entry and/or exit passage at a PTC roadway and/or building facility.

Identification (ID) Access Card**:**

1. An official employee badge issued by the PTC that displays an employee's photograph, name, and identification number programmed to permit access through use of a card reader.

2. An official Non-Revenue card or Function card issued by the PTC that displays the company's name (and/or employee's name) and identification number programmed to permit access through use of a card reader.

PTC Facility – One or more buildings or structures related by function and location to the PTC, which include maintenance, fare collection, administrative facilities, tunnels, and tower sites.

Security Control Devices include but are not limited to:

1. Identification (ID) access cards programmed for access at doors or other access points
2. Keys that operate cylinders in mechanical locks
3. Wireless devices that rely on a unique credential being presented to a reader

Visitor - Any individuals who are not authorized personnel.

E. PROCEDURES:

Identification (ID) Access Cards

- All active employees will be issued ID access cards for identification and access control. For new or replacement cards, employees must submit an Employee ID Card Request/Return Form to the mailbox for Card\Key Access and Repairs. ID access cards for employees can also serve as non-revenue cards. See Policy Letter 7.14 – Non-Revenue Cards for Employees – for additional information.

- Authorized personnel will be assigned ID access cards and/or other security control devices as needed. ID access cards for authorized personnel can also serve as non-revenue cards. See Policy Letter 7.13 – Non-Revenue Cards for Individuals Who are Not Turnpike Employees – for additional information.

FEMO will assign to an individual's security control devices the access privileges that are needed in their current PTC position. Additional access privileges will require approval in writing by the employee's department head, and the managing director of the facility and/or affected department where applicable

- ID access cards must be worn visibly at all times while at a PTC facility.

- Security control devices must never be loaned, transferred, given to others, misused, duplicated, modified, or altered.

- For personnel other than active employees and Pennsylvania State Police, security control devices must be assigned an expiration date.

- Lost or stolen security control devices must be reported to the Facilities Access Coordinator within forty-eight (48) hours of discovery.

Individuals who are assigned keys or other security control devices to access PTC facilities or open access gates are responsible for these items. *See Policy Letter 6.3 - Procedure for Management of Pennsylvania Turnpike Keys* - for additional information. Any unattended open access gate must be immediately reported to the Traffic Operations Center upon discovery. Any person found to have left a gate open may be subject to disciplinary action.

Key Requests – A key access request form must be completed, approved by the employee's supervisor and department head, and submitted to the Facilities Security Supervisor or his designee for approval and processing via the mailbox for Card\Key Access and Repairs. Key Requests for areas managed by other units will require the additional approval of the responsible department's department head and/or the managing director of the facility.

Termination of Employment – Immediately upon termination, resignation, or retirement, the affected employee's supervisor is responsible for packaging all ID access cards, keys, and other security control devices that were issued to the employee and forwarding them to the Facilities Access Coordinator. The employee must complete and submit a Key Return Form and/or an Employee ID Card Request/Return Form along with the items being returned. If the ID access card or other security control device is not

immediately available, the Facilities Access Coordinator must still be notified immediately by the employee's supervisor, via the mailbox for Card\Key Access and Repairs, in order to disable the functionality of the ID access card or other security control device.

Employee Transfer -- Upon transfer, the affected employee's supervisor is responsible for packaging all keys and other security control devices that were issued to the employee and are no longer needed and forwarding them to the Facilities Access Coordinator. The employee must complete and submit a Key Return Form and/or an Employee ID Card Request/Return Form along with the items being returned. If the functionality of an ID access card or other security control device must be disabled or revised, the employee's supervisor must notify the Facilities Access Coordinator at least one week prior to the transfer by submitting an Access Change/Issues Form to the mailbox for Card\Key Access and Repairs.

Audits –Reviews of key and other security-control assignments and access privileges are to be performed at least every three years. Reviews will typically be performed or coordinated by FEMO and the Compliance Department. Managers and supervisors are also responsible for reviewing key and other security control device assignments and access privileges for their staff.

PTC Facility Security Risk Assessments – Assessments will be performed as needed by FEMO, Operations, Safety, and Incident Response, and Information Technology in conjunction with the Compliance Department and the Pennsylvania State Police.

Alarms and Notifications – The PTC electronic access control system will be configured to trigger a non-audible alarm when a controlled access point is found to be unsecured for a specified period of time.

Emergency Access – In the event of an emergency, e.g. power outage, card reader malfunction, etc., access to the facility must be approved by the building manager, the managing director of the facility, or the employee's department head.

Violations – Violations will be investigated at the discretion of the FEMO, Compliance, and Legal Departments. Violations will be referred to the Compliance or Legal Departments to initiate the formal review process. Individuals found to be in violation of this policy may be subject to disciplinary action, up to and including immediate termination.

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