PENNA TURN PIKE	**PA TURNPIKE COMMISSION POLICY** *This is a statement of official Pennsylvania Turnpike Policy*	**NUMBER**: 5.03 **APPROVAL DATE**: 08-25-1978 **EFFECTIVE DATE**: 08-25-1978 **REVISED DATE**: 09-19-2023
POLICY SUBJECT: Access Control at PTC Facilities and Gates for Authorized Personnel	**RESPONSIBLE DEPARTMENT:** Engineering / Facilities Operations	

A. PURPOSE:

To establish a policy to manage access to various Pennsylvania Turnpike Commission (PTC) facilities and gates in order to provide a safer work environment while protecting the PTC's assets.

B. SCOPE:

This policy applies to all PTC employees. In addition, this policy applies to and is binding upon contractors, subcontractors, consultants, subconsultants, concessionaries, authorized service providers, emergency response companies, Pennsylvania State Police (Troop T) and government agencies.

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 and display their assigned access control card, ID access card, or other security control devices at all times. Keys used to gain access should be accessible and shown upon request.

This policy must follow PCI DSS Requirement 9, which states: "Restrict physical access to cardholder data. Any physical access to systems holding cardholder data allows individuals to access devices or data and destroy systems or hard copies. Consequently, such access should be restricted to authorized personnel only."

D. DEFINITIONS:

Access control card - Door/gate cards or proxy cards issued to PTC vendors/partners to manage access through doors at certain PTC facilities and PTC access gates on the turnpike system.

Active PTC Employee – Any PTC employee in compensable status. The term does not include PTC retirees or those on full time Union Leave.

Authorized Personnel – Active PTC Employees, vendors and partners including contractors, subcontractors, consultants, subconsultants, concessionaires, authorized service providers (ASP), emergency response companies, government agencies and any other PTC-authorized entities provided with ID access cards or other security control devices programmed for access at doors, gates or other access points.

Consultant – An individual or an individual employed by a firm, partnership, corporation, or joint venture under contract with the PTC.

Contractor – An individual or an individual employed by a firm, partnership, corporation, or joint venture under contract with the PTC.

Gate or other Access Point – A moveable structure or similar barrier that controls entry and/or exit passage at a PTC roadway and/or building facility that is not equipped with tolling equipment.

Government agencies – A Commonwealth agency or entity, including but not limited to PEMA, FEMA and/or PennDOT, whose employees may be provided with Security Control Devices pursuant to this Policy.

Identification (ID) Access Card- An official badge issued by the PTC to Authorized Personnel that displays the Authorized Personnel's photograph, name and identification number programmed to permit access through use of a card reader.

PCI DSS – Payment Card Industry Data Security Standard

Keys:
Unit Key- opens a room or office in a PTC facility (i.e. closet/evidence room/storage room)
Section Key – opens one building or more than one room in a PTC building (i.e., interchange, maintenance shed area, PSP barracks).
District Key – opens all PTC buildings or rooms in one particular district (i.e. all interchanges, maintenance sheds and gates within that district).
Master Key – opens all PTC buildings system wide (i.e. all PTC maintenance sheds, interchanges or PSP barracks, and gates across the entire system).

Proxy Card – A device using Radio Frequency Identification in conjunction with a proxy reader to provide access.

PSP – Pennsylvania State Police (Troop T).

PTC Facility – One or more buildings or structures owned by the PTC, which includes, but is not limited to, maintenance sheds, fare collection buildings, administrative facilities, tunnels, bridges and tower sites.

PTC Vendors/Partners – Consultants, engineering contractors, engineering CM/CI consultants, Emergency Responders (EMS), concessionaires (i.e. service plaza lessees), Authorized Service Providers and PSP.

Representative - The project manager or an authorized representative of PTC acting on behalf of the Chief Engineer pursuant to an active contract with the PTC.

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. Access control cards.
4. Wireless devices that rely on a unique credential being presented to a reader (i.e., proxy cards or by use of an app).

Visitor – Any individuals who are not Authorized Personnel.

E. PROCEDURES:

1. Authorized Personnel

a. **Identification (ID) Access Cards**:

- All active PTC employees will be issued ID access cards for identification purposes.
- Authorized Personnel will be issued ID access cards and/or other security control devices as needed and authorized.
- The ID access card must be worn and visibly displayed at all times while in a PTC facility. If wearing the ID access card would interfere with the employee's job duties or responsibilities, it must be available and displayed immediately upon request.
- Access privileges – Facilities Operations and/or IT Security will assign to the ID access card, the privileges needed for the Authorized Personnel. Additional access privileges will require approval by submitting the appropriate form through the ServiceNow portal.
- ID access cards must never be loaned, transferred, shared, misused, duplicated, modified or altered.
- Lost or stolen ID access cards must be reported to the Facilities Access Coordinator and/or Facilities Security Supervisor immediately.
- For new or replacement ID access cards Authorized Personnel or a Representative of the non-PTC employee Authorized Personnel, must be approved by submitting the appropriate form through the ServiceNow portal.
- The cost to replace a lost or stolen ID access card is $10.00; the replacement cost is subject to change without notice.

b. Keys:

- A key access request must be approved by submitting the appropriate form through the ServiceNow portal.

- Key Requests made by Troop T for other PSP units must be approved by submitting the appropriate form through the ServiceNow portal.
- Keys remain the exclusive property of the PTC and are provided to Authorized Personnel solely for PTC business purposes.
- Authorized Personnel who are issued or assigned keys are personally responsible for the key.
- Representatives of the PTC who issue assigned keys to Authorized Personnel are responsible for tracking keys issued in accordance with this policy.
- Upon request from the PTC, the Authorized Personnel are required to immediately return the key(s) to the Facilities Access Coordinator.
- Keys must never be loaned, transferred, shared, misused, duplicated, modified or altered.
- Lost or stolen keys must be reported to the Facilities Access Coordinator immediately.
- All costs associated with lost, stolen, loaned, transferred, shared, misused or duplicated keys will be charged to the Authorized Personnel to whom it was assigned in accordance with the following table:

Table 1

Key Type	PTC Employees and PSP	Contractor (Issued by Engineering, except Facilities Operations)	Contractor (issued by other PTC Departments, including Facilities Operations)	Emergency Responders/ Government Agencies (except PSP)
Unit	$30	$1000	$250	$125
Section	$60	$1000	$250	$125
District	$125	$1000	$500	$250
Master	$250	$1000	$1000	$500

- Any unattended open access gate that is not opened by operational necessity of the PTC must be immediately reported to the Network Control upon discovery.
- Employees must ensure that a gate closes following use of the gate.
- Any other Authorized Personnel found to have left open an access gate may have his/her key(s) revoked and held responsible for all associated PTC costs.

2. Terminated and/or Transferred Employees

- Immediately upon termination, resignation, retirement or transfer, the PTC employee must return all security control devices to the employee's supervisor. The employee's supervisor is responsible for packaging all security control devices that were issued to the employee and forwarding them to the Facilities Access Coordinator with the completed Key Return Form and ID Access Card Return Form.
- If the security control devices are not immediately available, the employee's supervisor shall immediately notify the Facilities Access Coordinator via the ServiceNow portal, in order to disable the functionality of the ID access card.
- If the functionality of the security control devices must be disabled or changed, the employee's supervisor must notify the Facilities Access Coordinator at least one week

prior to the termination, transfer, retirement or resignation by submitting the appropriate form through the ServiceNow portal.

- If an employee fails to return a key, the appropriate fee from Table 1 above will be deducted from the employee's last paycheck or by other appropriate means. The fee is subject to change without notice. The appropriate fee will be included on the appropriate form when the key is issued.

3. **Visitor Access to CAB, ERO and WRO** –All Visitors must sign in upon arrival and sign out upon departure from the CAB, ERO and WRO ("PTC Office Building"). Upon signing in, the Visitor will be issued a Visitor ID badge, which must be worn during the entire visit at the PTC Office Building. 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 and leaves the Visitor ID Badge at the end of their visit.

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

4. **Access Control Cards**:

   - The access control card replaces the keys and non-revenue cards previously issued to PTC vendors/partners.
   - PTC vendors/partners entering and exiting a job site at an access gate and/or certain PTC facilities must have a valid access control card specific to the geographical limits of the project.
   - Authorized Personnel must complete the **Access Gate Card Request form and Card Use Agreement** and forward to the appropriate Representative at least 30 calendar days in advance.
   - A $20.00 card processing fee is required for each access control card. Exceptions may be provided for emergency purposes as authorized in writing by the Chief Engineer.
   - The Representative for the assigned contract will issue no more than 25 access control cards to the Authorized Personnel on a project.
   - The PTC Representative may request additional access control cards, which may be approved in writing by the Chief Engineer based on the scope of the project.
   - The access control card will expire on the project completion date, subject to change at the request of the contractor and at the Representative's discretion in the event the project completion date is extended. Under no circumstances shall the access control card be extended beyond the project completion date unless approved in writing by the Chief Engineer.
   - PTC vendors/partners are responsible for monitoring and documenting access control card usage and shall provide requested documentation to support appropriate business usage to PTC upon request.
   - PTC Vendors/partners shall immediately report all lost or stolen access control cards to the Representative.

- Access control card privileges may be revoked for unauthorized use or any other reason in the sole discretion of PTC.

5. **Intelligent Key Management System**– A system used to manage, secure and audit keys and control access to keys for PTC facilities, equipment and assets. All keys contained in the intelligent key cabinets shall remain the exclusive property of the PTC and shall only be used for official PTC business or other authorized purposes.

    - Access privileges – Facilities Operations will assign the privileges needed to the employee as well as a gas pin # or ID access card.
    - Additional access privileges will require additional approval by submitting the appropriate form through the ServiceNow portal.
    - Authorized Personnel, other than Active PTC Employees, may be granted necessary access privileges to the Intelligent Key Management system upon approval, which will be assigned to the access control cards.
    - Authorized Personnel who are granted such access privileges are personally responsible for the key and all associated PTC costs for unauthorized use.
    - Keys shall not be loaned, transferred, shared, misused, duplicated, modified, altered or tampered with or given to a person without authorized access privileges.
    - Authorized Personnel are responsible for all costs associated with violations of this provision, including, but not limited to, replacement of lost keys, damage repair costs (including damage to gates and the key cabinets), theft of property, fare evasion and/or lost revenue.
    - Authorized Personnel must immediately notify the PTC's Access Coordinator if any keys are lost or there is any breach of access to the key cabinet.

6. **General Procedures applicable to access at PTC facilities and gates**

    Audits – Reviews of security control devices and turnpike access privileges must be performed at least annually. Reviews will be performed or coordinated by Facilities Operations. Managers, Supervisors and Representatives are also responsible for reviewing security control devices and appropriate usage by their staff or vendors/partners (contractors).

    PTC Facility Risk Assessments – Risk assessments of PTC facilities will be performed as needed by Engineering/Facilities Operations, Operations, Safety, Incident Response and Information Technology in conjunction with the PSP.

    Violations – Violations of this policy must be reported to the Human Resources Department.

    Active PTC Employees found to be in violation of this policy may be subject to disciplinary action, up to and including immediate termination and other costs as described above.

    Authorized Personnel who are not active PTC Employees found to be in violation of this policy may have PTC facilities access revoked and be responsible for property damage, replacement costs for lost security control devices, tolls and fines.

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