PENNA TURN PIKE	**PA TURNPIKE COMMISSION POLICY** *This is a statement of official Pennsylvania Turnpike Policy*	**NUMBER**: 8.12 **APPROVAL DATE**: 06-18-2019 **EFFECTIVE DATE**: 07-03-2019 **REVISED DATE**:
POLICY SUBJECT: IT Security and Risk Management	**RESPONSIBLE DEPARTMENT:** Information Technology	

A. PURPOSE:

The purpose of this policy is to inform Pennsylvania Turnpike Commission (PTC) authorized users (users) of their responsibilities to protect PTC Information Technology (IT) assets and to reduce risk of damage and cost of breach or misuse of those assets. Authorized users shall uphold these responsibilities through established and future PTC IT standards and procedures.

B. SCOPE:

This policy applies to all business processes and data, information systems, components, and PTC authorized users. All PTC authorized users, including full-time, part-time, temporary, supplemental and summer employees, contractors, independent consultants, third parties, and employees of partners and clients of the PTC who access the PTC's information resources are within the scope of this policy.

This policy should be read in conjunction with the policy letter *8.01 Acceptable Use of Commission Technology Resources*.

C. GENERAL POLICY:

It is the policy of the PTC to protect and account for all PTC IT assets through identification and maintenance of an asset inventory, including proper storage and disposal of information system media, and through control and regular maintenance of authorized user accounts. IT Security shall administer and protect the PTC's information assets in accordance with all applicable federal and state guidelines and regulations.

The IT Department will communicate new and changed IT standards to users as they are published. All authorized users within the defined scope of this policy will adhere to the existing and future standards established as an extension of the principles of this policy. All users shall carry out information security practices and principles generally accepted as due diligence/best practice within the business community to protect against incidents such as hacking, phishing, and social engineering.

D. PROCEDURES:

The PTC IT Security personnel shall manage, protect, and account for all PTC IT assets through maintenance and review of user accounts on a regular basis and control of access to all PTC systems and applications.

The PTC IT Department personnel shall educate and train all authorized users on an annual basis regarding the use, maintenance, and protection of PTC IT assets, including adherence to data classification.

IT Security shall identify, evaluate, monitor, and respond to information security risks and will continually maintain and update incident response capabilities.

Violations of this policy shall be referred to the Information Security Officer or the Chief Compliance Officer (e.g., through the Fraud and Abuse Hotline), and shall not be investigated independently, unless authorized by the CEO. Employees found to be in violation of this policy may be subject to disciplinary action up to and including termination. Contractors and Consultants may be subject to actions as specified in their contract, as well as under the Commonwealth's Contractor Responsibility Program.

E. DEFINITIONS:

Authorized User: Any employee who receives compensation from the PTC on an hourly, daily, or annual basis, including employment on a full time, part time, or probationary basis ("Employees"), and Contractors and Independent Consultants who use or have access to Commission Technology Resources.

Hacking: The act of attempting to break into a computer system illegally by an experienced, highly skilled programmer with the intent to steal data or sabotage the system.

Phishing: A form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels.

Social Engineering: Manipulating someone into performing actions or divulging confidential information.

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