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**: 06-18-2024
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 (authorized 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 are subject to 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 authorized users as they are published. All authorized users shall adhere to the existing and future standards established as an extension of the principles of this policy 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 authorized 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.

Security Incident Review Committee

This committee is charged with reviewing the conduct of employees who have had multiple instances of non-compliance with the IT Department's Security and Awareness Training Standard relating to real threats, as well as periodic phishing tests. The committee will determine appropriate corrective and/or disciplinary actions to be taken to reduce the risk that an individual may pose to the Commission.

The Security Incident Review Committee is comprised of the following members:

- Chief Technology Officer
- Assistant Chief Technology Officer – Security and Infrastructure
- Information Security Officer
- Chief Counsel
- Director of Human Resources
- Department head of the employee coming before the Committee

Violations of this policy shall be referred to the Information Security Officer or the Director of Human Resources 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 consultants who are authorized to use or to have access to Commission Technology Resources.

Commission Business Applications - software or a set of programs located on premises or cloud-based that PTC owns or licenses (including software-as-a-service or similar subscriptions) that are used by PTC to perform PTC business functions, support PTC business processes, manage PTC data, or facilitate PTC decision-making.

Commission Computer Systems - Hardware and software, both on premises and cloud-based that the Commission owns, rents, controls, licenses or uses to perform PTC business functions and activities, including supporting the function of PTC Business Applications. Computer Systems include but are not limited to individual desktop computers, laptops, tablet computers, servers, virtual machines, routers/switches and other networking devices, wired or wireless telephones, cellular phone, smartphones, 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.

Commission Data and Records are Information in electronic form (data or documents) that documents a transaction or activity of the PTC, including information generated from computer use, internet use, email communication and other electronic communication (whether sent, received, or stored), as well as the content of such communications.

Commission Facilities – Buildings that the PTC owns, rents or otherwise uses to conduct PTC operations, including but not limited to administration buildings, maintenance sheds and related buildings, tunnels, communications towers, and networking and utility buildings in support of fiber optics and open road tolling gantries.

Commission Technology Resources include, but are not limited to, the following: all Commission-Owned Data and Records, Commission Computer Systems and Business Applications, Information Technology (IT) and Operational Technology (OT) that PTC owns, licenses, rents, controls, or otherwise uses in PTC operations.

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.

Informational Technology (IT) - The entire spectrum of information processing technologies, including software, hardware, communications technologies and related services.

Operational Technology (OT) – On premises, cloud-based and vendor managed hardware and software that detects or causes a change through the direct monitoring and/or control of physical equipment, devices, processes, and events across the PTC enterprise.

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.

F. 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.