PENNA TURN PIKE **PA TURNPIKE COMMISSION POLICY** *This is a statement of official Pennsylvania Turnpike Policy*		**NUMBER**: 8.01 **APPROVAL DATE**: 10-18-2011
POLICY SUBJECT: **Acceptable Use of Commission Technology Resources**	**RESPONSIBLE DEPARTMENT:** **Information Technology**	**EFFECTIVE DATE**: 10-18-2011 **REVISED DATE**: 06-18-2019

A. **PURPOSE**:
The purpose of this policy is to inform Pennsylvania Turnpike Commission (Commission or PTC) authorized users of the policies, responsibilities and procedures related to the acceptable use of Commission Technology Resources. Every effort must be made to ensure the confidentiality, integrity, and availability of Commission information assets and to assist the Commission in complying with applicable state and federal laws. All Commission authorized users are required to read this policy and sign the applicable Acceptable Use of Technology Resources Acknowledgment form to verify their understanding of this policy.

B. **SCOPE**:
This policy applies to all Commission Authorized Users who have to access to Technology Resources. This policy should be read in conjunction with the Commission's Code of Conduct.

C. **GENERAL POLICY**:
Acceptable Use of Commission Technology Resources ("Technology Resources") by Authorized Users. This policy is designed to prevent use that may be illegal, unlawful, abusive, or which may have an adverse impact on the Commission or its Technology Resources. In addition, it identifies the permissible and effective uses of Commission Technology Resources.

Abuse or misuse of Commission Technology Resources. The improper use of Commission Technology Resources by Employees may result in disciplinary action, up to and including termination of employment. The improper use of technology resources by Contractors or Consultants may result in disciplinary action that may include termination of engagement, and other formal action under the terms of the applicable contract or debarment under the Commonwealth Contractor Responsibility Program. When warranted, the Commission may pursue or refer matters to other authorities for criminal prosecution against anyone who violates local, state or federal laws through the misuse of its Technology Resources.

Violations of this policy are to be referred to the Information Security Office or the Compliance Department. Authorized Users are encouraged to assist in the enforcement of these standards by promptly reporting any observed violations to the Information Security

Office or the Compliance Department (e.g., the Fraud and Abuse Hotline). Violations of this policy may not be investigated independently by individuals or departments.

Ownership of Commission Technology Resources. All Commission Technology Resources are the sole and exclusive property of the Commission. Authorized Users have no property or other rights to any Commission Technology Resource and do not control the access to or the use of Commission Technology Resources.

Authorized Users have no expectation of privacy when using Technology Resources. Authorized Users have no expectation of privacy in any electronic files, data or records stored on or accessed through Technology Resources nor in any communications sent or received via, or stored within, Technology Resources.

Authorized Users may not access unauthorized data and should take measures to protect the security of their data. As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or Commission Technology Resources for which they do not have authorization or explicit consent.

- Plugging in unauthorized devices to the PTC network is strictly prohibited and may result in the loss of access.
- Authorized Users must use passwords and/or encryption in a manner that is consistent with Commission technology standards.
- Authorized Users must keep passwords secure and must not share them with others.
- During the normal workday, the lock computer feature must be used to protect the workstation to prevent unauthorized access.
- An individual who has been assigned a portable computing device, such as a laptop, tablet or smartphone, must not leave the computing device unattended in unsecured/public areas.

Authorized Users must maintain the confidentiality of sensitive data. The unauthorized access to, disclosure or dissemination of Commission or other sensitive, privileged or confidential information, including, but not limited to, personally identifiable, protected health, attorney-client privilege or financial information, is not permitted. Information that is transmitted over public networks may be intercepted or modified by persons other than the intended recipients of that information. Therefore, appropriate precautions as prescribed by Information Security IT Standards must be taken when sending Commission confidential or other sensitive information to an external recipient or when transmitting such data over a public network. Individuals shall not make unauthorized copies of confidential, sensitive or privileged information. Commission business applications help ensure the confidentiality of sensitive data, prevent data loss, and support records management requirements. Authorized Users should use Commission-approved business applications (including email) when conducting Commission business. Further, if a user is notified that Commission Technology Resources in his or her possession are subject to a litigation or records hold, s/he must take the steps necessary to comply with the hold requirements.

Commission Technology Resources are intended for business use and should be used primarily for that purpose. Commission Technology Resources are tools that the Commission has made available for Commission business purposes. Where personal use of Commission Technology

Resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the Commission, limited use for personal purposes is permitted consistent with other Commission policies and the standards set forth in the Commission's Code of Conduct. Streaming of non-business media at the workplace is not permitted. The use of Commission Technology Resources to operate a personal business, for personal gain in any form, or for other inappropriate use is prohibited. Any personal use which is inconsistent with Commission policy or law is prohibited. Examples of unacceptable personal use may be communicated from time to time and will have the same force and effect as if specifically listed in this policy.

Commission Technology Resources must never be used in a manner that violates Commission policies. The use of Commission Technology Resources to send, view, access, download, store, display, print, or otherwise disseminate material that is sexually explicit, suggestive or pornographic, profane, obscene, threatening, discriminatory, harassing, fraudulent, otherwise offensive, defamatory, or unlawful is strictly prohibited. The use of Commission Technology Resources to degrade performance, deprive access to a corporate resource, or gain access to a system or information for which proper authorization has not been given is also strictly prohibited.

All Authorized Users must be provided with this directive. All Authorized Users shall be provided a copy of this policy and are required to read and sign the applicable Acceptable Use of Technology Resources Acknowledgment form to verify their receipt and understanding of this policy. Employees are required to sign the form provided as Attachment A, and Contractors and Consultants are required to sign the form provided as Attachment B, prior to their use of or access to Technology Resources. Copies of this policy may be provided either electronically or in hard copy.

D. **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.

IT Standard - A prescribed or proscribed specification, approach, directive, solution, methodology, product or protocol which must be followed. IT Standards shall be published/made available to internal PTC employees, consultants and independent contractors, as appropriate.

IT Procedure - An established process to be followed in order to ensure actions comply with policies or standards. IT Procedures shall reference an IT Standard or PTC Policy Letter and shall be published/made available to internal PTC employees, and consultants and independent contractors as appropriate. Procedures that reveal details about the Commission's technology environment that, if disclosed, may introduce a security risk shall have a more limited distribution.

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, 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.

E. **PROCEDURES**:

For Authorized Users

The Information Security Office and Human Resources must work together to ensure that all Authorized Users read this policy and sign the applicable Acceptable Use of Technology Resources Acknowledgment form to verify their receipt and understanding of this policy. Employees are required to sign the form provided as Attachment A and Contractors and Consultants are required to sign the form provided as Attachment B. Copies of signed forms will be maintained as part of the Employee's official personnel file or, in the case of Contractors and Consultants, in the Information Security Office's files.

For New Employees

- Human Resources will notify the Information Security Office regarding an employee's start date and position via an SAP batch process.

- Information Security will create a user account and assign required access privileges per the submitted IT service request.

- On or before the new employee's start date, Human Resources will provide the Information Security Office with a signed Acceptable Use of Technology Resources Policy acknowledgement form from the new employee

- An appropriate current photo of the new employee shall be provided to the Information Security Office as part of the employee onboarding process.

For Contractors and Consultants

- The Commission employee responsible for managing a contractor or independent consultant shall submit a request to provide the contractor or independent consultant with access to required Commission Technology Resources at least three (3) business days prior to the contractor's or independent consultant's arrival.

- Upon receipt of PTC manager's approval, the signed Acceptable Use of Technology Resources Policy Acknowledgement form along with a contact phone number and a current professional photo, the contractor or independent consultant will be provided with the requested access privileges and the Information Security Office will provide the manager who initiated the request with the login information.

- The Commission employee responsible for managing a contractor or independent consultant must notify the Information Security Office upon the termination of the

engagement for which the Contractor and Consultant obtained access to Commission Technology Resources. The Commission may, in its sole discretion, also terminate access to Commission Technology Resources at any time.

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

Acceptable Use of Technology Resources Policy

Employee Acknowledgement

I hereby acknowledge that I have received, read, and understand Policy Letter 8.01, Acceptable Use of Technology Resources, and agree to abide by the requirements set forth in it.

I understand that 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.

I further understand that my Commission Technology Resource usage, including electronic communications such as email, voice mail, text messages, chat strings, and other data and records, may be accessed and monitored at any time, with or without advance notice to me.

I understand that if I need further clarification or additional information, I may contact the IT Security Office.

The Commission can, at any time, and in its sole discretion, modify this user agreement and require mobile device users to reconfirm their agreement to abide by and comply with the terms of the modified agreement.

Print Name _____

Signature _____ Date _____

Attachment B

Acceptable Use of Technology Resources Policy

Contractor or Independent Consultant Acknowledgement

This user agreement does not prohibit contractors or consultants from performing services required by their contract with the Commission.

I hereby acknowledge that I have received, read, and understand Policy Letter 8.01, Acceptable Use of Technology Resources, and agree to abide by the requirements set forth in it.

I understand that Commission Technology Resources are governed by IT Standards and Procedures and that failure to comply with those Standards and Procedures may result in access being revoked.

I further understand that 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. Contractors and Consultants may be subject to actions as specified in their contract, as well as under the Commonwealth's Contractor Responsibility Program.

I further understand that my Commission Technology Resource usage, including electronic communications such as email, voice mail, text messages, chat strings and other data and records, may be accessed and monitored at any time, with or without advance notice to me.

I further understand that if I need further clarification or additional information, I may contact the Information Security Office.

The Commission can, at any time, and in its sole discretion, modify this user agreement and require mobile device users to reconfirm their agreement to abide by and comply with the terms of the modified agreement.

Print Name _____

Company _____

Signature _____ Date _____