Information Technology Policy

Credit Card Use for e-Government

Number
ITP-SEC017

Effective Date
September 7, 2006

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
October 2024

1. Purpose

This Information Technology Policy (ITP) establishes an enterprise-wide policy to ensure uniformity of customer service and security of credit card information across the Commonwealth enterprise.

2. Scope

This ITP applies to all offices, departments, boards, commissions and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Definitions

Enterprise Electronic Payment Solution: The Commonwealth's preferred mechanism for the acceptance, processing, and support services of electronic payments. The Enterprise Electronic Payment Solution is available to agencies via a statewide merchant services contract and integrates with the SAP enterprise resource planning system, (hereinafter referred to as "SAP").

4. Background

Many agencies are implementing e-government applications that allow customers to pay fees online with the use of a credit card. Agencies shall take extra care to safeguard their cardholder data and improve their front line of defense to avoid internal and external security compromises. Protecting sensitive information builds a good business practice, as well as a solid reputation.

American Express, Discover, Master Card and Visa USA each have operating regulations that state when a charge to a card may occur. In general, a credit card may not be

charged until the order is filled (i.e., goods are shipped, or services are rendered). There are exceptions, for example, a deposit for a hotel room may be charged when the room is reserved.

Credit card issuers' operating regulations prohibit the establishment of maximum, or minimum, dollar amounts for credit card transactions.

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by Visa and MasterCard and endorsed by other payment vendors including American Express and Discover. The standard includes requirements from Visa's Cardholder Information Security Program, MasterCard's Site Data Protection, the American Express Data Security Operating Policy and the Discover Information Security and Compliance. Using the PCI requirements allows agencies to validate against a single set of security standards.

5. Policy

Any e-government application that accepts credit card payments shall allow customers to make payment using any of the four major credit card issuers:

- American Express
- Discover
- MasterCard
- VISA USA

5.1 Payment Card Industry (PCI) Data Security Standards (DSS) Requirements

All agencies that process or store cardholder data and have access to the information as a result of Internet, mail, fax, or telephone acceptance of credit card account information are required to comply with the American Express, Discover, VISA USA, and Master Card International operating regulations and the PCI DSS. PCI DSS is intended to protect cardholder data in the card-not-present industry. A card-not-present transaction can include Internet, mail, fax, or telephone acceptance of credit card account information.

Comprehensive information on PCI requirements and merchant levels may be found on the PCI Security Standards Council website.

PCI DSS Information can be found below for each of the major credit card issuers:

- American Express
- Discover
- MasterCard
- VISA

All third-party vendors that agencies use to fulfill PCI compliance will be retained at the agency's expense via the Invitation to Qualify process. Resources on this process can be found in the References section of this ITP.

The Office of Comptroller Operations performs activities detailed in Management Directive 310.24 relative to each agency's credit card applications to ensure they satisfy business requirements in an efficient and effective manner. The Office of Administration Office of Information Technology supports agencies in establishing

connections to and overall maintenance/support of the Enterprise Electronic Payment Solution. PCI standards documentation (annual self-assessment, quarterly network security scans and, if the agency is a level 1 merchant, results of the annual on-site review) will be maintained by each agency with copies sent to the Office of Administration, Office for Information Technology, Chief Information Security Officer (CISO) at RA-CISO@pa.gov.

Note: Credit card companies (Visa, MasterCard, etc.) can impose restrictions, fines, or prohibit an agency from participating in programs, if it is determined to be non-compliant.

5.2 Electronic Payments

All electronic payments shall adhere to the guidance provided in *Management Directive 310.24 Amended, Accepting Electronic Payments for Commonwealth Revenues.*

The Commonwealth merchant services contract includes the Enterprise Electronic Payment Solution provider for credit card transactions accepted over the Internet. Agencies are required to ensure credit card transactions, processed via the Internet, are submitted to the current approved Enterprise Electronic Payment Solution provider for processing as outlined in *STD-SEC017A, Enterprise Electronic Payment Product Standards* (Commonwealth access only). Information about the current Enterprise Electronic Payment Solution provider is available on the Office of Comptroller Operation's Accepting Electronic Payments website.

Agencies may utilize one of the following integration services from the Enterprise Electronic Payment Solution:

1. Direct connection of e-government web applications that process credit card transactions with the Enterprise Electronic Payment Solution provider utilizing the provider's Internet web service(s).

2. Outsource e-government web applications, that process credit card transactions, to the approved Commonwealth vendor that provides:

    - E-government web application services for processing credit card transactions.
    - Transfers credit card information to the Enterprise Electronic Payment Solution provider.

Agencies shall refer to the Enterprise Service Catalog for details on this service.

6. Responsibilities

6.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

6.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

6.3 Third-party vendors, licensors, contractors, or suppliers shall:

Accept credit card payments and adhere to *PCI requirements* (if applicable per contract).

7. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/Glossary.aspx*
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 210.12, Amended, Electronic Commerce Initiatives and Security*
- *Management Directive 310.23, Amended, Commonwealth Purchasing Card Program*
- *Management Directive 310.24, Amended, Accepting Electronic Payments for Commonwealth Revenues*
- *STD-SEC017A, Enterprise Electronic Payment Product Standards* (Commonwealth Access Only)
- *Office of Budget – Accepting Electronic Payments Documentation*
- *DGS Invitation to Quality (ITQ) Information for Commonwealth Users*
- *DGS ITQ Application Guide for Suppliers*
- *Enterprise Service Catalog*
- *Official PCI Security Standards Council Site*

8. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

9. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on *https://itcentral.pa.gov* for Commonwealth personnel and on the Office of Administration public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

10. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	09/7/2006	Base Policy	N/A
Revision	08/14/2013	Refresh	N/A
Revision	04/2/2014	ITP Reformat	N/A
Revision	08/09/2021	• Updated links • Added third party vendor language to Scope and Responsibilities. • Added link to Office of Budget's Accepting Electronic Payments Documentation Updated Related ITPs, Publication Version Control and Exemption Sections	N/A
Revision	10/12/2021	• Update policy language to approved Commonwealth vendor. • Adjusted third party vendor language in Scope and Responsibilities Sections.	N/A
Revision	06/09/22	• ITP Refresh • Legacy ePay Web Services removed (Section 3.3)	N/A
Revision	10/03/2023	• Annual review • Added supporting document STD-SEC017A, references added in policy language and under Related ITPs/Other References. • Added Background section and moved detailed Purpose language to new section. • Added links to PCI Council Site. • Updated reference links. • Added reference to MD 310.24 and statement requiring electronic payments to adhere to MD.	Revised IT Policy Redline <10/03/2023>