pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

CoPA Policy for Credit Card Use for e-Government

ITP Number	***Effective Date***
ITP-SEC017	September 7, 2006
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

This Information Technology Policy (ITP) establishes an enterprise-wide policy for the security of credit card information.

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.

Many agencies are implementing e-government applications that allow customers to pay fees online with the use of a credit card. Commonwealth agencies, boards, and commissions are to 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. Agencies are encouraged to establish electronic fund transfer arrangements with customers who need to routinely make large payments.

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.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor’s jurisdiction. Agencies not under the Governor’s jurisdiction are strongly encouraged to follow this ITP.

3. Policy

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

- American Express
- Discover
- MasterCard
- VISA USA

Payment Card Industry (PCI) Data Security Standards (DSS) Requirement

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 Web site at the following link:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Information on merchant levels, penalties for violation, and frequency of required security assessments is available at the following page on the Visa Web site:

http://usa.visa.com/merchants/risk_management/cisp_merchants.html

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.

The comptroller's office is available to provide operational assistance relative to each agency's credit card applications to ensure they satisfy business requirements in an efficient, effective manner. 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 the Budget's Bureau of Audits at ra-OB_BOA@state.pa.us and the Office of Administration/Office for Information Technology/Chief Information Security Officer at ra-CISO@state.pa.us

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.

Electronic Payment

The Commonwealth banking/financial management contract includes an electronic payment solution provider for credit card transactions accepted over the Internet. All agencies under the governor's jurisdiction are required to ensure credit card transactions, processed via the Internet, are submitted to the aforementioned electronic payment solution provider.

Agencies may utilize one of the following integration services with the electronic payment solution provider under contract with the Commonwealth:

1) Direct connection of e-government web applications that process credit card transactions with the electronic payment solution provider utilizing the provider's Internet web service(s).

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

   a. e-government web application services for processing credit card transactions.
   b. transfers credit card information to the electronic payment solution provider under contract with the Commonwealth.

Legacy ePay Web Service:

1) Agencies are not required to use the legacy ePay web service that process credit card transitions for existing or new applications. The ePay web service has been placed into containment and will be phased out.

   - Agencies are asked to contact the OA/OIT for information regarding the legacy ePay web service.

2) Agencies are asked to review the business case for continued use of ePay with existing applications and begin planning a transition utilizing one of the following solutions:

   - A direct connection to the electronic payment solution provider under contract with the Commonwealth.
   - Outsource existing e-government web application to approved Commonwealth vendor(s) that interfaces with the electronic payment solution provider under contract with the Commonwealth.

3) Please see Enterprise service catalog for list of providers.

6. Responsibilities

Agencies are required to perform the actions outlined in this policy.

7. Related ITPs/Other References

8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

9. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	9/7/2006	Base Policy
Revision	08/14/2013	Refresh
	4/2/2014	ITP Reformat