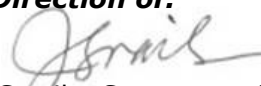



MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania Governor's Office

Subject: Accepting Electronic Payments for Commonwealth Revenues	Number: 310.24 Amended
Date: November 18, 2019	By Direction of:  Jen Swails, Secretary of the Budget  Michael Newsome, Secretary of Administration
Contact Agency: Office of the Budget, Office of Comptroller Operations, Bureau of Accounting and Financial Management, Telephone 717.787.6496	

This directive establishes policy, responsibilities, and procedures for accepting electronic payments for the payment of Commonwealth revenues. This amendment adds definitions and procedures and adds a requirement for the preparation and submission of a security assessment prior to the acceptance of electronic payments. Marginal dots are excluded due to major changes.

- 1. PURPOSE.** To establish policy, responsibilities, and procedures for accepting Electronic Payments for the payment of taxes, licensing fees, registration fees; for admission to facilities; for the sale of products; and payment for other services that provide revenue to the Commonwealth.
- 2. SCOPE.** This directive applies to all departments, boards, offices, commissions, and councils (hereafter referred to as "agencies") under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are encouraged to follow this directive or implement similar policies, responsibilities, and procedures.
- 3. OBJECTIVES.**
 - a.** To maximize electronic commerce (e-commerce) opportunities and improve the speed and efficiency with which the Commonwealth collects revenue.
 - b.** To ensure the acceptance of Electronic Payments as a method of payment that benefits the Commonwealth and provides a secure mechanism for consumers to conduct financial transactions with the Commonwealth.

- c. To ensure compliance with Payment Card Industry (PCI) Data Security Standards (PCI DSS) as identified by the PCI Security Standards Council.

4. DEFINITIONS.

- a. **Approved Bank Account.** An account established for use by a Commonwealth agency and approved by the Office of the Budget, Office of Comptroller Operations, Bureau of Accounting and Financial Management (OB/OCO/BAFM).
- b. **Business Case.** A document that describes the reason for initiating a project or task for Electronic Payments.
- c. **Electronic Payment.** The use of payment cards, chip cards, or mobile/digital wallets to transfer funds for the purpose of obtaining a service.
- d. **Information Technology (IT) Resources.** Include, but are not limited to, the following: the Commonwealth'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 phones, pagers, beepers, personal data assistants and handheld devices, and, further, includes use of the internet, electronic mail (email), instant messaging, texting, voice mail, facsimile, copiers, printers or other electronic messaging through Commonwealth facilities, equipment or networks (collectively "IT Resources").
- e. **Payment Card Industry Data Security Standard (PCI DSS).** An information security standard for organizations that handle branded credit cards from major card schemes. It is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.
- f. **Security Assessment.** A process conducted by the Office of Administration, Office for Information Technology's Enterprise Information Security Office (OA/OIT/EISO) that defines, identifies, and classifies security vulnerabilities of IT Resources.

5. POLICY.

- a. Agencies must complete a Business Case, with the assistance (as needed) of OB/OCO/BAFM, to include the following information:
 - (1) An explanation of how Electronic Payments will improve the effectiveness and efficiency of the revenue collection process.

- (2) A cost/benefit analysis justifying the acceptance of Electronic Payments. The cost/benefit analysis should include, at a minimum, expenses related to electronic payment fees, processing fees, banking costs, the cost of equipment required to accept Electronic Payments, and the financial gain resulting from the accelerated receipt of revenues using the most recent General Fund yield rate.
- b. Agencies must obtain approval from the Chief Accounting Officer or designee to proceed with the acceptance of Electronic Payments based on the Business Case.
- c. Agencies must review and comply with IT Policies that are published by the Office of Administration, Office for Information Technology Enterprise.
- d. Approved Bank Account(s) must be established, as necessary, for the receipt of revenues within the terms of the merchant services contract.
- e. After approval of the Business Case and the Security Assessment, agencies will follow the implementation processes to complete the set-up as outlined in the [*e-Commerce Business Guide for Electronic Payment Processing*](#).

6. RESPONSIBILITIES.

- a. **Agency Heads** shall:
 - (1) Establish policies, responsibilities, and procedures consistent with this directive.
 - (2) Comply with the most current version of the PCI DSS posted by the PCI Security Standards Council.
 - (3) Identify the Agency Audit Organization (refer to *Management Directive 325.3 Performance of Audit Responsibilities*).
 - (4) Comply with Management Directive 325.13 *Service Organization Controls*, Guidance on Oversight Options for Service Organizations.
 - (5) Facilitate discussions between internal and external entities on all corrective action plans detailed in SOC reports and other audit reports.
 - (6) Ensure that the appropriate security training is provided to application developers and individuals who have access to point of sale (POS) terminals. Guidance is available on the [*Accepting Electronic Payments*](#) webpage.

- b. Office of the Budget, Office of Comptroller Operations, Bureau of Accounting and Financial Management (OB/OCO/BAFM)** shall:
- (1) Assist agencies in completing Business Cases.
 - (2) Review agency Business Cases and provide recommendations to the Chief Accounting Officer or designee.
 - (3) Assist agencies in establishing Approved Bank Accounts.
 - (4) Administer the statewide merchant services contract.
 - (5) Maintain and distribute to authorized users the *e-Commerce Business Guide for Electronic Payment Processing*.
 - (6) Request an audit of Approved Bank Accounts or Electronic Payment systems, as needed, in accordance with *Management Directive 325.03, Performance of Audit Responsibilities*.
- c. Office of the Budget, Chief Accounting Officer** or designee shall:
- (1) Approve or disapprove agency Business Cases.
 - (2) Notify OA/OIT/EISO through e-mail at RA-OAPCICOMPLYEISO@pa.gov of approved Business Cases.
- d. Office of Administration, Office for Information Technology, Enterprise Information Security Office (OA/OIT/EISO)** shall:
- (1) Provide information technology guidance to agencies on the Security Assessment and PCI DSS requirements.
 - (2) Provide guidance and ensure agencies are complying with all IT Policies and PCI DSS.
 - (3) Work with internal and external entities on IT-related activities required in corrective action plans detailed in SOC reports and other audit reports.
 - (4) Monitor compliance within the Commonwealth for all agencies accepting Electronic Payments.
 - (5) Perform the activities detailed in the *e-Commerce Business Guide for Electronic Payment Processing*.
- e. Office of Administration, Office for Information Technology, Bureau of Enterprise Solutions (OA/OIT/BES)** shall perform the activities detailed in the *e-Commerce Business Guide for Electronic Payment Processing*.

- f. Agencies** shall:
- (1) Complete and submit Business Cases as needed.
 - (2) Acquire approval of Business Case from the Office of the Budget, Chief Accounting Officer or designee.
 - (3) Establish Approved Bank Accounts.
 - (4) Utilize the "Electronic Payment" enterprise service offering detailed in the OA OIT Enterprise Service Catalog at: <https://itcentral.pa.gov/Pages/Enterprise-Services.aspx>.
 - (5) Agree to the electronic payment issuer terms and conditions for the acceptance of Electronic Payments.
 - (6) Comply with *Management Directive 325.13 Service Organization Controls*.
 - (7) Perform the activities detailed in the *e-Commerce Business Guide for Electronic Payment Processing*.
- g. Agency/Delivery Center Information Security Officer (ISO) or designee** shall:
- (1) Identify the individual overseeing the registration process for the agency.
 - (2) Review results of PCI audits and vulnerability scans. If required, ensures resolution of deficiencies to ensure compliance.
 - (3) For new agencies accepting Electronic Payments for the first time, monitor and ensure that the PCI audit passes within ninety (90) days of go-live for new implementations and on an on-going basis annually.
 - (4) Monitor and ensure that quarterly vulnerability scans are completed and successfully pass.
 - (5) For agencies adding additional Electronic Payment set-ups, ensure that annual audits include the new set-up information for implementation.

7. PROCEDURES.

a. Agency.

- (1) Identifies a need to accept Electronic Payments as a method of payment for a revenue stream or streams.
- (2) Prepares a Business Case for the acceptance of Electronic Payments and submits the Business Case to the OB/OCO/BAFM, and the General Accounting Division.

- b. Office of the Budget, Office of Comptroller Operations, Bureau of Accounting and Financial Management (OB/OCO/BAFM), and the General Accounting Division.**
 - (1) Provides necessary guidance to agencies for developing Business Cases.
 - (2) Analyzes the agency Business Case and provides recommendations for approval or disapproval to the Chief Accounting Officer or designee.
- c. Office of the Budget, Chief Accounting Officer or designee.**

Approves or disapproves the agency Business Case.

 - (1) If approved, notifies the agency and the Bureau of Accounting and Financial Management and instructs the agency to submit a Security Assessment application to the OA/OIT/EISO. E-mails OA, PCI Compliance EISO (RA-OAPCICOMPLYEISO@pa.gov) informing them of the approved Business Case for tracking.
 - (2) If disapproved, notifies the agency and the Bureau of Accounting and Financial Management of the reason for disapproval.
- d. Agency.**
 - (1) If the Business Case has been approved, prepares and submits to the OA/OIT/EISO a Security Assessment application as directed in *IT Policy SEC005 Commonwealth Application Certification and Accreditation*, *IT Policy SEC023 Information Technology Security Assessment and Testing Policy* and other relevant security-based IT Policies.
 - (2) If the Business Case has been disapproved, consults with the Bureau of Accounting and Financial Management and, when appropriate, prepares and submits an amended Business Case in accordance with section 7.a.(2) of this directive.
- e. Office of Administration, Office for Information Technology, Enterprise Security Information Office (OA/OIT/EISO).**
 - (1) Provides necessary security guidance to agencies for developing Electronic Payment solutions.
 - (2) Analyzes the appropriate assessments in accordance with *IT Policy SEC005 Commonwealth Application Certification and Accreditation*, *IT Policy SEC023 Information Technology Security Assessment and Testing Policy* and other relevant security-based IT Policies.

f. Agency.

- (1)** Sends a letter of authorization to the Commonwealth's merchant services bank to establish the Approved Bank Account, if necessary.
- (2)** Contacts the Commonwealth's merchant services bank, as needed, to finalize any details regarding the agency's Approved Bank Account, the agency's ability to accept Electronic Payments via internet transactions, and the agency's use of POS terminals and software.
- (3)** Engages the vendor to discuss the requirements for implementation.
- (4)** Follows the activity outlined in the *e-Commerce Business Guide for Electronic Payment Processing*.
- (5)** For agencies submitting at a Merchant Level 1 or Merchant Level 2, on an annual basis, send an e-mail with a copy of the Attestation of Compliance (AOC) to OA, PCI Compliance EISO (RA-OAPCICOMPLYEISO@pa.gov) and PCI_Compliance@firstdata.com. Submissions must be from an authorized Commonwealth employee.
- (6)** For agencies submitting at a Merchant Level 1 or Merchant Level 2, on a quarterly basis, send proof of successful completion of vulnerability scans to OA, PCI Compliance EISO (RA-OAPCICOMPLYEISO@pa.gov) and PCI_Compliance@firstdata.com. Submissions must be from an authorized Commonwealth employee.
- (7)** For agencies submitting at a Merchant Level 3 or Merchant Level 4, on an annual basis, successfully pass a PCI DSS audit using the Rapid Comply solution along with successfully passing quarterly vulnerability scans, if required. Submissions must be from an authorized Commonwealth employee.
- (8)** For agencies submitting at a Merchant Level 3 or Merchant Level 4 using external vendors/auditors to complete the annual PCI DSS audits, send an e-mail with a copy of the Attestation of Compliance (AOC) to OA, PCI Compliance EISO (RA-OAPCICOMPLYEISO@pa.gov) and PCI_Compliance@firstdata.com. Submissions must be from an authorized Commonwealth employee.

This directive replaces, in its entirety, *Management Directive 310.24*, dated October 18, 2016.