# POLICY 410.041: CREDIT/DEBIT CARD AND ACH/ECHECK TRANSACTION PROCESSING

## OBJECTIVE

To ensure that no Card Holder Data will be stored, archived or retained within the Aviation Authority's environment whether on paper or electronically; the Aviation Authority is cognizant of and is compliant with PCI DSS standards through change monitoring and implements proper procedures, security controls, and protocols regarding acceptance of Electronic Funds Transfers (EFT); and all departments and staff that process or transmit credit card data recognize the importance of privacy and remain in compliance with PCI DSS standards.

This policy covers all acceptable types of Electronic Funds Transfers transacted in person at Point of Sale Terminals or online via an e-Commerce Portal.

## SCOPE

Any Aviation Authority employee, department, contractor, or agent who, in the course of doing business on behalf of the Aviation Authority, is involved in EFT processing or who has authority over a system that accepts EFT transactions for the Aviation Authority is subject to this policy. Actions by an employee which result in the Merchant of Record's privileges being revoked may result in disciplinary actions in accordance with Policy 204.02, Allegations of Misconduct.

## DEFINITIONS

**ACH/Electronic Check (ACH/eCheck) –** acceptance of an electronic version of a paper check for payment of an Aviation Authority invoice or transaction. eChecks are processed through the Automated Clearing House (ACH) Network. The ACH Network executes electronic exchanges, transfers of money, from one account to another, either within a single financial institution or across multiple financial institutions.

**Card Holder Data** – as defined in Policy 1010.02, PCI DSS Annual Compliance.

**Credit/Debit Card –** acceptance of a credit card or debit card for payment of an Aviation Authority invoice or transaction.

**Electronic Funds Transfer (EFT)** – an umbrella term that is inclusive of payments made to the Aviation Authority by either Credit/Debit Card or ACH/eCheck. EFT's can be performed via e-Commerce Portal or POS Terminal.

**Electronic Commerce Portal (e-Commerce Portal)** – refers to a secure website (portal) that allows the payer to enter payment data remotely using a Credit/Debit Card or ACH/eCheck.

**Merchant of Record** – each department authorized to accept Electronic Funds Transfers for Aviation Authority transactions.

**Merchant ID #** - sometimes called a Merchant Account Number, service entitlement number, or service establishment number.

**Payment Card Industry Data Security Standard (PCI DSS)** – standard defined by the Payment Card Industry Security Standards Council (consortium of major credit card brands). This standard was created to increase controls around Card Holder Data to reduce credit card fraud.

**Point of Sale (POS) Terminal** – refers to a stand-alone device for processing Credit/Debit Card payments. A POS Terminal transaction differs from an e-Commerce Portal in that the payer and card are present, onsite at the time of the transaction.

## ACCEPTANCE OF ELECTRONIC & CREDIT CARD PAYMENTS

1. All Card Holder Data is subject to Policy 1010.02, PCI DSS Annual Compliance.
2. Each department authorized to accept EFTs will be a Merchant of Record and will have one or more Merchant ID #s to segregate transactions for each Merchant of Record.
3. The Finance department will have full authority and approval regarding which departments will be allowed to accept EFTs based on business case, estimated number of transactions, and the business processes and internal controls as defined by the department. Generally, only departments that are authorized to collect cash or check payments for the Aviation Authority will be authorized to accept EFTs.
4. Each Merchant of Record must incorporate additional security controls into existing departmental procedures. An internal departmental procedure covering EFTs will be required and approved by the Finance department prior to allowing EFT transactions for the Merchant of Record.
5. The Finance department will have full authority to revoke a Merchant of Record's privileges.
6. The Aviation Authority may accept EFTs through the following methods:
    - WiFi/Cellular POS terminal devices to accept onsite payments from customers
    - Electronic Commerce Portal to accept secure, online payments

7. The Aviation Authority may pass through fees and other costs associated with EFTs to the cardholder at the time of the transaction. Fees will be determined by the Finance department.
8. Employees, contractors, and agents with access to card holder data must sign a PCI DSS Card Holder Data Confidentiality Agreement (Form 410.041.1) to acknowledge that they have read and understand this policy. The signed PCI Confidentiality Statement shall be forwarded to Human Resources for inclusion in the personnel file of each employee or in the appropriate contract file.

**SEE ALSO**

- Section 204.02, Allegations of Misconduct
- Section 410.04, Revenue Control/Accounts Receivable
- Section 1010.00, Use of Technology Resources
- Section 1010.02, PCI DSS Annual Compliance

## APPROVAL AND UPDATE HISTORY

**LAST APPROVAL**

Aviation Authority Board: May 21, 2014
Chief Executive Officer: May 12, 2014

**SUPERSEDES**

All Previous

# Greater Orlando Aviation Authority
# PCI DSS Card Holder Data Confidentiality Agreement

This document represents a Confidentiality Agreement that pertains to Aviation Authority employees, contractors, or agents authorized to service and accept Electronic Funds Transfer (EFT) transactions. Please carefully review the terms stated below.

As an authorized employee, contractor, or agent of the Aviation Authority, I, _____ acknowledge that I may have direct access to Sensitive Data as defined in the Aviation Authority's Policy 1010.00, Use of Technology Resources, Card Holder Data as defined in Policy 1010.02, PCI DSS Annual Compliance, and privacy information for Aviation Authority customers and payers.

To protect the availability, confidentiality, and integrity of the systems and processes and maintain the confidentiality of the customer or payer information for payments that the Aviation Authority accepts, I agree to the following:

- I will conduct and perform EFT transactions for Aviation Authority business purposes only and I will not write down, record, photograph, or store any customer or payer privacy data or Card Holder Data in any form, paper or electronic.

- I have received, read, understand and agree to abide by the Aviation Authority's Organizational Policies 410.041, Credit/Debit and ACH/eCheck Transaction Processing; 1010.00, Use of Technology Resources; and 1010.02, PCI DSS Annual Compliance. I am aware that any violation of these or other policies may subject me to disciplinary action under Policy 204.02, Allegations of Misconduct, loss of use and access privileges, and other penalties.

Employee/Contractor Signature: _____ Date: _____

Print Name: _____

Department/Contractor: _____

Department Vice President Signature: _____ Date: _____

Human Resources Signature: _____ Date: _____