



CLERK OF THE BOARD

2016 MAY 13 PM 12: 24

CLERK, CIRCUIT & COUNTY CTS
MIAMI-DADE COUNTY, FLA.
#1

OPERATIONAL DIRECTIVE NO. 16-03

Effective Date: MAY 28, 2016

SUBJECT: POLICY ON PAYMENT CARD DATA SECURITY

PURPOSE AND SCOPE: To establish a policy, practices and guidance to protect cardholder data of entities and individuals transacting business with the Miami-Dade Aviation Department (MDAD) as established and required for compliance under the Payment Card Industry Data Security Standards (PCI DSS).

I. AUTHORITY

- A. Miami-Dade County Code, Chapter 25, Aviation Rules and Regulations.
- B. Operational Directive 99-02 – Miami-Dade Aviation Department Written Directive System.
- C. Operational Directive 99-03 – Miami-Dade Aviation Department Written Directive System.
- D. Payment Card Industry Data Security Standards Version 3.1 – PCI Security Standards Council, LLC. (www.pcisecuritystandards.org)

II. DEFINITIONS

- A. Cardholder Data: Refers to information contained on the full magnetic strip or the account number plus any of the following identifiers: cardholder name, expiration date or service code.
- B. EMV (Europay MasterCard and Visa) Technology: It is a technical standard for smart payment cards, payment terminals and automated teller machines that read card data stored on integrated circuits rather than magnetic stripes. This standard requires credit card issuers to provide customers with a card containing the imbedded chip technology. The primary benefit of this technology is a reduction in card-present transaction fraud through use of a unique multi-factor authentication process versus the traditional magnetic stripe data that could be easily reproduced. Merchants failing to implement new card readers capable of processing EMV chip cards will bear the responsibility of fraudulent charges incurred as a result of its non-compliance. (Smart payment cards are also referred to as chip-and-pin cards or chip-and-signature cards.)
- C. PCI Security Standards Council: An independent council created by the five leading payment card industry brands, American Express, Discover Financial Services, JCB International,

MasterCard Worldwide and Visa International responsible for establishing security standards to safeguard cardholder information.

D. Self-Assessment: The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI-DSS.

III. BACKGROUND

The Payment Card Industry Data Security Standards (PCI DSS) are technical and operational requirements developed and mandated by the PCI Security Standards Council. The Standards were created to increase security controls over the storage, processing and transmission of cardholder data to reduce payment card fraud and losses to the industry resulting from data security breaches. All entities that accept any of the above branded payment cards must maintain compliance with the security standards. Risks and penalties for non-compliance include denied credit card transaction processing, fines, customer litigation, compensation costs for lost or stolen data and increased compliance requirements for the organization.

PCI DSS compliance is a process that requires continuous assessment of the operation to identify and address recognized or perceived vulnerabilities. As such, adopting necessary procedures and actions is necessary to assure such compliance. All Miami-Dade Aviation Department (MDAD) Divisions that collect, maintain or have access to cardholder data must comply with this PCI policy. In addition, business partners working at MDAD controlled airports must also adhere to the security standards and provide protection to the traveling public, individuals and other entities.

In addition to meeting the requirements for PCI DSS compliance, the Department must also comply with standards requiring use of payment terminals capable of processing smart payment cards with EMV chip technology. PCI and EMV compliance are not substitute or alternate standards as each one focuses on protecting different aspects of cardholder data and transactions. EMV helps to reduce card-present fraud by validating transactions while PCI compliance protects card data that is stored, processed, and transmitted through data networks. As such maintaining compliance of both standards as required will improve overall credit card security and reduce the Department's liability in instances of fraudulent transactions or data breaches.

IV. POLICY

Department policy prohibits collecting and storing credit card information manually in customer files or in an electronic format on any computer, server or database, including spreadsheets. It also prohibits the emailing of credit card information for payment processing or any other purpose. This policy will outline procedures and actions to meet the control objectives outlined in the PCI DSS and provide training to employees who are responsible for processing credit card transactions.

V. PRACTICES

Adherence to the standards requires assessment of the major control objectives within the payment card network and data environment:

A. Build and Maintain a Secure Network: The Department maintains a firewall configuration to restrict connections and traffic within the network and in the cardholder data environment. Data transmission is also encrypted to protect against malicious attempts to access information. In addition, authentication data to access the network such as system passwords are unique and require periodic update and do not consist of defaults supplied by vendors.

B. Protect Cardholder Data: Department networks do not store payment card information. The MDAD network is used as an encrypted pass-through of this data for authentication and processing by third party vendor applications. Employees who process transactions are also strictly prohibited from manually collecting or recording payment card information for any purpose. All payment card transactions must be processed either through payment devices at the point of sale or the Department's online payment system.

C. Maintain a Vulnerability Management Program: Anti-virus programs and mechanisms have been deployed on systems to protect against the activities of malicious software and hackers. These programs are kept current and evaluated periodically to assess effectiveness. Security patches are also installed to protect system components and software from known vulnerabilities.

D. Implement Strong Access Control Measures: Access to cardholder system components and devices capturing payment card data is limited to employees whose job function requires such access. A list of all payment devices in use is maintained by the Finance Division and includes information such as make, model, location and device serial number.

E. Regularly Monitor and Test Networks: The Department's Information Systems Division is responsible for assuring Department networks are monitored and regularly tested to assure all security measures and processes are in place, functioning properly, and kept up to date.

VI. INCIDENT REPORTING

A. PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data. Vulnerabilities identified should be promptly addressed as data breaches can present a significant risk to the Department.

B. Managers overseeing areas where payments are received should periodically ask employees if credit card information is being copied, written or retained in files to verify ongoing compliance.

VII. EMPLOYEE TRAINING

The Miami-Dade County Information Technology Department (ITD) has created a mandatory online web training module for all personnel responsible for processing, reviewing, reconciling, or

approving credit card transactions, processes, or systems. Aviation Department employees whose job functions include any of the activities described above will be required to attend. This training program should provide valuable information regarding any new requirements under the standards and provide awareness of the importance of maintaining cardholder data secure.

VIII. AMENDMENTS

The Department reserves the right to amend this OD at any time and from time to time.

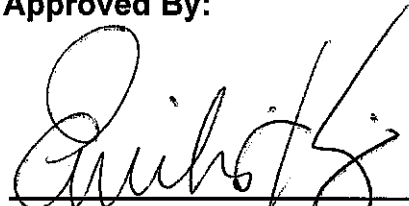
IX. SEVERABILITY

If any court of competent jurisdiction determines that a provision of this OD is illegal or void, the remainder of this OD shall continue in full force and effect.

X. EFFECTIVE DATE

This OD shall become effective 15 days subsequent to its filing with the Clerk of the Circuit Court as Clerk of the County Commission. This OD shall remain in full effect until revoked or amended.

Approved By:



Emilio T. González, Aviation Director

Date: 5/12/16