

## **PCI Compliance Policy**

### **I. POLICY PURPOSE**

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, the City of Lake Forest has established a formal policy and supporting procedures regarding PCI compliance, which relates to credit card transactions conducted by customers with the City. The policy incorporates: 1) card holder data retention and disposal, 2) PCI change management, and 3) Information Technology (IT) area access procedures. The IT area access procedure is to ensure that the confidentiality and integrity of the City's IT assets are maintained by controlling the flow of visitors, vendors and guests within an IT area. This policy will be evaluated on an annual basis to ensure its adequacy and relevancy regarding the City's needs and goals.

### **II. SCOPE**

Cardholder data retention and disposal, as well as PCI change management, is limited to any employees authorized to process credit cards as payment for City goods and services. The IT area facility access applies to all City employees.

### **III. POLICY DEFINITIONS**

- A. Card Holder Environment:** Any person, process or technology involved with any part of processing a credit card transaction. The document outlining the Card Holder Environment is attached. The word 'environment' used in this document will also signify the Card Holder Environment.
- B. Change Management:** The controlled identification and implementation of required changes within the Card Holder Environment.
- C. PCI:** The Payment Card Industry (PCI) is a Security Council of major credit card company representatives. Their goal is to protect credit card holder information. They have published a regulations document called Data Security Standards (DSS) version 3.0.
- D. Card Verification Code or Value:** Data element on a card's magnetic stripe that uses a secure cryptographic process to protect data integrity on the stripe and reveals any alteration or counterfeiting (referred to as CAV, CID, CVC, CVV or CSC, depending on payment card)

- CAV – Card Authentication Value (JCB payment cards)
- CVC – Card Validation Code (MasterCard payment cards)
- CVV – Card Verification Value (Visa and Discover payment cards)
- CSC – Card Security Code (American Express)

The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit un-embossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:

CID - Card Identification Number (American Express and Discover payment cards)  
CAV2 - Card Authentication Value 2 (JCB payment cards)  
CVC2 - Card Validation Code 2 (MasterCard payment cards)  
CVV2 - Card Verification Value 2 (Visa payment cards)

- E. Primary Account Number (PAN):** Acronym for primary account number and also referred to as account number. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
- F. Cardholder Data:** Cardholder data is any personally identifiable information associated with a user of a credit/debit card. Primary account number (PAN), name, expiration date, and card verification value 2 (CVV2) are included in this definition.
- G. Service Code:** Three-digit or four-digit value in magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange or identifying usage restrictions.
- H. Personally Identifiable Information:** Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.
- I. PIN:** Acronym for "personal identification number." Secret numeric password known only to the user and a system and is used to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.
- J. PIN Block:** A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the Primary Account Number.
- K. PTS:** Acronym for "PIN Transaction Security" and pertains to manufacturers of PIN Entry Devices.
- L. PCI Change Management Committee:** A committee appointed by the City Manager including but not limited to the Finance Director, Assistant Finance Director and the Information Technology Assistant Director.
- M. EMV: Acronym for Europay, MasterCard and Visa,** a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions. These cards are in use in Europe.
- N. Information Technology (IT) Area:** Any location that contains network, server, or telecommunications equipment that is not physically secured by additional physical separation and not intended for use by an end user. This includes the Data Center, server rooms, and network closets but excludes the IT cubicle work areas.
- O. Sponsor:** The employee responsible for inviting the visitor.
- P. Visitor:** Any person not employed by the City.

#### IV. STATEMENT OF POLICY.

##### A. Retention

Cardholder data will be retained in accordance with Payment Card Industry Data Security Standards (PCI DSS) provisions, which allow for certain data elements to be stored while other data elements are not. The display of the Primary Account Number (PAN) information will be masked; however limited employees and other parties with a legitimate need may view the entire PAN information if necessary. The following tables list the maximum period of time cardholder data elements can be stored based on storage medium.

Appropriate facility controls must be used to limit and monitor physical access to systems that store cardholder information.

##### Electronic Media Storage of Cardholder Data

Type of Cardholder Data	Retention Period	Business Justification/Requirements for Retention of Cardholder Data
Primary Account Number (PAN)	5 minutes	Can only be stored while waiting for an authorization. Exception: CLASS software.
Cardholder Name	5 minutes	Can only be stored while waiting for an authorization.
Expiration Date	5 minutes	Can only be stored while waiting for an authorization.
Service Code	5 minutes	Can only be stored while waiting for an authorization
Full Magnetic Strip/Track Data (Track 1 and Track 2)	Cannot be stored	
Card Verification Code or Value (CID, CAV2, CVC2, CVV2 Codes)	Cannot be stored	
Pin and Pin Block	Cannot be stored	

- To prevent unauthorized storage, only PTS approved PIN entry devices and PA-DSS validated payment applications should be used.
- Electronic media containing cardholder data must never be removed from any secure office environment without being physically destroyed or securely deleted with DoD 5220.22-M data sanitization procedures prior to removal. This applies specifically but not limited to copy/fax machines and their hard disk drives.
- The only other approved mechanism of electronically storing cardholder data is the current Parks & Recreation CLASS software system. CLASS stores credit card numbers forever and is approved by the City because additional steps have been taken to safeguard the card holder data.

##### Hard Copy Format Storage of Cardholder Data

Type of Cardholder Data	Retention Period	Business Justification/Requirements for Retention of Cardholder Data
Primary Account Number (PAN)	1 day	All printed receipts should only contain the truncated PAN. Paper copies of forms that contain the PAN information may be kept for a period of one day to allow time to enter the transaction.
Cardholder Name	1 day	Cardholder name can only be stored with the PAN for

		a period of one day to allow time to enter the transaction.
<b>Expiration Date</b>	1 day	Expiration date can only be stored for a period of one day to allow time to enter the transaction.
<b>Service Code</b>	1 day	Service code can only be stored for a period of one day to allow time to enter the transaction.
<b>Full Magnetic Strip/Track Data (Track 1 and Track 2)</b>	Cannot be stored	
<b>Card Verification Code or Value (CID, CAV2, CVC2, CVV2 Codes)</b>	Cannot be stored	
<b>Pin and Pin Block</b>	Cannot be stored	

- All hardcopy materials containing cardholder data must be stored in a secure and locked container (safe, cabinet, or desk).
- Hardcopy materials containing cardholder data must never be stored, unattended, in unlocked or insecure containers or open workspaces.
- Hardcopy materials containing cardholder data should be processed on the day received.

## **B. Disposal**

Once the maximum retention period has been allotted for cardholder data it must be securely removed from all electronic media, and any hardcopy must be disposed of according to procedures listed below.

All combination Copy/Fax machines with a hard drive that stores copies of Copy/Fax data containing Cardholder Data must have a contract with the vendor that covers the requirement to clean the hard drive of data prior to be removed from the premises.

All hardcopy shred bins must remain locked at all times (until shredding). Employees must make every effort to immediately shred cardholder information using *only* cross-cut or diamond-cut shredders.

## **C. PCI Change Management**

Appropriate controls must be used to limit and monitor access to the Card Holder Environment. The Change Management Committee will be responsible for the establishment of policy and procedures intended to ensure the protection of card holder data which is processed within the Card Holder Environment.

The Change Management Committee will be appointed by the City Manager and will include but not be limited to:

1. Finance Director
2. Assistant Finance Director
3. Information Technology Assistant Director

The Change Management Committee responsibilities include but are not limited to:

1. Approve all changes to the Card Holder Environment

2. Monitor the Card Holder Environment
3. Evaluate the Card Holder Environment on a periodic basis
4. Coordinate Training of the Card Holder Environment
5. Remediation of the Card Holder Environment

Departments and/or locations that accept or desire to accept credit card payments must have any and all environmental changes approved by the PCI Change Management Committee. Examples of changes to the environment are

1. A replacement PC or Printer
2. Office reconfiguration or construction changes
3. Replacement security cameras
4. New credit card processing software
5. New or replacement credit card swiper
6. New or replacement receipt printer

Departments and/or locations currently accepting credit card payments are:

1. Boat Dock
2. City Hall
3. Finance
4. Golf Course
5. Parks & Recreation
6. Police
7. Senior Center
8. Community Development (anticipated mid-2015)

Each Department/location will appoint a person to facilitate compliance with PCI DSS requirements for their portion of the environment under the direction of the PCI Change Management Committee.

#### **D. IT Area Access**

Visitors are required to have a sponsor. The sponsor is the City employee responsible for bringing the visitor(s) on site and ensuring the visitor follow the procedures outlined.

### **V. PROCEDURES**

Credit/debit card information may not be distributed, once received by the City, either internally or externally, i.e., via email, fax or interoffice mail.

Any software or application that processes credit card information must be reviewed by the ***PCI Change Management Committee*** to verify PCI compliance.

Point of Sale terminal receipts must be programmed to mask the PAN information. A properly masked number will show only the last four digits of the PAN.

Hardcopies containing any PAN information must be shredded in a timely manner according to the procedures listed below.

The PCI Change Management Committee will meet a minimum of quarterly and will publish the meeting dates to those responsible for processing credit card payments.

The Committee will create a form to document requested changes to the environment and will distribute the form with instructions to those responsible for processing credit card payments. The form will be the formal request for a change to the environment.

The Committee will review all forms to ensure compliance with PCI DSS requirements. When a change is approved, the environment documentation will be updated to reflect the change.

In the event the City engages a Service Provider to perform credit card processing, the committee will take the following steps to ensure the Service Provider performs its activity in accordance with PCI DSS requirements.

- Require, by contract, that Service Providers are in PCI DSS compliance
- Require, by contract, that Service Providers report any security and data breaches to the City Manager within 48 hours of identification of the breach

The Committee will monitor the environment via its quarterly meetings and will advise members of the Card Holder Environment of changes of PCI DSS requirements when applicable.

The Committee will evaluate the environment on a periodic basis of at least yearly, using the City policies and procedures. The Committee will provide direction for updates to the policies and procedures and remediation of the environment. This activity should be completed prior to the self-assessment attestation.

The Committee will provide training or coordinate training for those involved with processing credit cards. Those receiving training must acknowledge that they have received the training and understand the safeguards required to protect the card holder data.

#### **A. Department Procedures**

Departments that process credit card payments shall develop specific internal procedures that will address this Policy. Specific items to include are:

1. Samples of all forms with tear strips for credit card number.
2. All storage locations used until destruction, who has access, and where the camera is that monitors the locations.
3. Description of how the tear strip is processed (i.e. timing of its removal, how it is removed, how and when it is destroyed).
4. Description of the destruction processing and specific type of shredder.

Departments and specific locations that currently process credit cards are:

1. Boat Dock
2. City Hall
3. Finance
4. Golf Course
5. Parks & Recreation
6. Police
7. Senior Center (Dickinson Hall)
8. Community Development (anticipated mid-2015)

Each Department / location is required to create, maintain and perform a yearly audit against these procedures.

## **B. IT Area Access Procedures**

Escorted visitors include, but are not limited to, visitors on site to perform building repairs, conduct product installations and maintenance, or meet with City staff. The visitor will sign in on a Log Sheet listing the following:

1. Date
2. Name
3. Company that they represent
4. The person they are here to see
5. The arrival time

They will need to be accompanied by a City Sponsor while in the IT Area.

Upon leaving the building, the visitor will sign out on the Log Sheet.

A sign-in log sheet will be maintained at each IT area. Department Directors will designate a person responsible for the maintenance of the log book at each City building that houses an IT Area. These log books will be kept for one (1) year.

## **VI. POLICY UPDATES.**

This Policy will be reviewed and updated as needed in order to reflect changes to the Card Holder Environment and address changes in PCI-DSS requirements.

## **VII. POLICY ADMINISTRATION.**

### **A. Oversight**

Responsibility for developing, implementing and updating this Policy lies with the PCI Change Management Committee.

### **B. Staff Training**

City staff responsible for implementing the Policy shall be trained either by or under the direction of the PCI Change Management Committee.

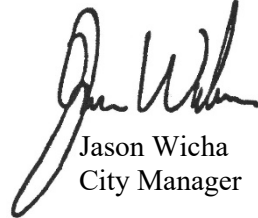
## **VIII. Discipline**

Violation of this policy will result in disciplinary action to be determined by the Director of Human Resources and the City Manager based on the type, severity and other circumstances surrounding the violation, up to and including termination. The City's possible tolerance of prior policy violations is no defense against disciplinary action under this policy.

**IX. Distribution**

This policy will be distributed to all employees who have access to card holder data and published on the Employee Information website, [www.citylf.org](http://www.citylf.org).

**ATTACHMENT: Cardholder Environment**



Jason Wicha  
City Manager