Credit and Debit Card Handling Policy
Updated July 7, 2014

City of Parkville
8880 Clark Ave. Parkville, MO 64152
Hours: 8:00-5:00 p.m. Monday -Friday
Phone Number 816-741-7676
Email: cityhall@parkvillemo.gov

Introduction and Purpose

The City of Parkville Municipal Code, Title VII, Chapter 800, Section 800.020 anticipates the acceptance of credit and debit cards for various municipal sales transactions and enacts convenience fee charges regarding the same. Per Section 112.080 (B) of the Parkville Municipal Code, this administrative policy establishes the procedures for proper handling of credit and debit card transactions processed through the USAePay gateway and the TSYS Card Swipe Machine.

The City of Parkville must take appropriate measures to protect credit and debit card numbers. Credit card and debit payments must be processed in compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements which are intended to limit exposure and/or theft of personal cardholder information. The City of Parkville must adhere to these standards in order to retain the ability to accept credit and debit card payments. This policy is intended to ensure that credit and debit card information is handled and disposed of in a manner that satisfies the City's obligation to protect such information to the level that is required by the PCI DSS.

Since any unauthorized exposure of credit or debit card information could subject the City to reputational damage and significant penalties, failure to comply with the policy contained within this document will be considered a serious matter.

Definitions

Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit and debit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information.

Cardholder Data is any personally identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Security Code (e.g., three-digit or four-digit value printed on the front or back of a payment card referred to as CVV2 or CVC2).

Application

This policy applies to all City of Parkville employees who process credit/debit card transactions and who have access to cardholder data.

General Information

The City of Parkville accepts credit and debit cards for many payments of goods and services through the USAePay gateway. USAePay is the City's primary credit or debit card processing application and is to be used for all credit and debit card transactions. Credit and debit card payments may only be accepted in the following manner: in-person, telephone, facsimile, physical mail (not e-mail).

Completed documentation must be submitted prior to payment. For example, a payment for a business license will not be accepted without the completed business license application.

The following credit or debit cards types may be accepted for payment: Discover, MasterCard, Visa, and American Express.

General Processing Procedures

E-Payment Gateway (City Hall Front Desk)

1. The customer shall be informed of any convenience fee prior to the transaction taking place.

2. Information shall be entered through the USAePay gateway and processed immediately. The cardholder data collected shall be:

- Card Type
- Cardholder Name

- Card Number
- Expiration Date
- Street Address
- State
- Zip Code
- Card Security Code (CVV2)

3. A receipt of the transaction will be emailed or printed for the customer, and an electronic copy will be kept by the City for record keeping until the completion of the annual audit.

4. The transaction documentation and merchant receipt will be stored in a secure (locked) area.

Card Present Transactions (Sewer Billing).

1. The card will be received and swiped immediately
    a. Picture ID is required if the card is not signed.

2. A receipt of the transaction will be emailed or printed for the customer and an electronic copy will be kept by City for record keeping until the completion of the audit.

3. The transaction documentation and merchant receipt will be stored in a secure (locked) area.

Access to Customer Credit and Debit Card Data

Only City personnel trained in the requirements of this policy may process credit or debit card transactions or have access to documentation related to credit or debit card transactions. The employee must be authorized by the City Clerk or Finance/Human Resources Director. Individuals who have access to credit or debit card information are responsible for properly safeguarding the data.

Employees not complying with approved safeguarding, storage, processing and administrative procedures will face disciplinary action up to and including termination. In addition, any employee engaged in credit or debit card processing fraud will be held responsible for any financial losses due to neglect in adhering to this policy.

Retention and Destruction of Cardholder Data

All credit or debit card information is to be treated with the same security and oversight as cash. Credit or debit card information will be kept to a minimum and cardholder data will be retained only as long as is necessary for business purposes, which is generally no longer

than 24 hours. Cardholder data will be destroyed when it is no longer needed. No credit or debit card information is to be retained by City of Parkville employees. Paper information will be shredded. Electronic files will be destroyed in a manner appropriate to the media on which they are stored.

All payments are processed via a payment gateway and merchant processor. Therefore no credit or debit card information is transmitted to or retained by the City of Parkville.

Receipt of Credit and Debit Card Information in Email

Under no circumstances will credit or debit card numbers received in an email be processed. The recipient of the credit or debit card number will respond to the sender with a standard template advising that the transaction cannot be processed and offering an acceptable method for transmitting card information. The email will be permanently deleted and credit or debit card numbers will be deleted from the response.

> **Email Response Template:** Thank you for your recent communication regarding payment for (item or event). For your protection, we cannot accept credit card information via email. Email is an insecure means of transmitting information (passwords, Social Security Number, etc.). Please visit our office or call 816-741-7676 during regular business hours to complete the transaction. Thank you.

Refunds

If payment was received from the customer by use of a credit or debit card, any refund is to be made only to the customer's credit or debit card. This will ensure the customer does not cancel the original transactions and get a refund through the credit or debit card company separately. This will also eliminate the possibility for fraud that exists if credit or debit card transactions are cancelled for refund by cash.

Oversight

The handling of credit and debit card transactions must segregate, to the extent possible, all duties related to data processing and storage of credit or debit card information. A system of checks and balances is established in which tasks are performed by different individuals in order to assure adequate controls. Refunds may only be processed with secondary approval by the Finance/Human Resources Director, City Clerk, or the Assistant to the City Manager. Daily reconciliation of front desk and sewer transactions will be conducted by the Finance/Human Resources Director.

Suspected Loss or Theft

Any employee who suspects the loss or theft of any materials containing cardholder data must immediately notify his/her supervisor and/or the Finance/Human Resources Director.

Acknowledgement

A copy of this policy must be read and signed by authorized personnel. Signed policies will be maintained in the personnel file.

Name: _____ Date: _____

Signature:_____

ATTEST:

Department Head: _____ Date: _____

Signature:_____