City of El Paso

Credit Card Handling and Processing Policy

September 1, 2021

Prepared by:
Office of the Comptroller
Treasury Services Division

No Previous Revision

The mission of the Office of the Comptroller is to provide fiscal management and financial reporting, administer treasury services and provide grant accounting information to City Management and elected officials so that they can make informed decisions regarding the provisions of City services.

TABLE OF CONTENTS

CITY OF EL PASO

Credit Card Handling and Processing Policy

1.0 INTRODUCTION

This policy has been written in accordance with the City of El Paso's policies currently in effect. Treasury Services Division of the Office of the Comptroller is responsible for this policy. Any questions can be directed to the Treasury Services Division (TSD).

2.0 PURPOSE

This Policy describes the management of the payment gateways and equipment used for the processing of credit cards as a form of payment and the management of payments and fees associated with credit cards for the City of El Paso (City). This policy is intended for all City staff responsible for processing credit card payments. The responsibility to observe these policies belongs to departments, whose employees accept credit cards as a form of payment.

3.0 GOALS AND OBJECTIVES

- Maintain a current list of active devices and payment gateways that capture payment card data.
- Ensure that applicable personnel are trained.
- Establish a system of internal controls that provide reasonable assurance for safeguarding the equipment and credit card activity from fraud or theft, maintaining the reliability of financial records and segregation of duties.

4.0 DEFINITIONS

- **Credit Card** – A credit card is a payment card issued to users to enable the cardholder to pay a merchant for goods and services based on the cardholder's promise to the card issuer to pay them for the amounts plus the other agreed charges.

- **Merchant id (MID)** – A merchant id is a unique code provided to merchants by their payment processor. This code is transmitted when payments are processed.

- **Monthly Reconciliation** - The process of reconciling the credit card payment by MID presented by the bank, to the general ledger to ensure all payments and fees are posted accurately and timely.

- **PCI Compliance** – The Payment Card Industry (PCI) compliance mandated by credit card companies to help ensure the security of credit card transactions in the payments industry.

5.0 EQUIPMENT

5.1 Inventory

Departments are to maintain a current list of equipment and payment gateways, including third party processors that capture the departments' credit card payments. A list of employees who have access to the equipment and payment gateways must also be maintained. The lists are to be sent to TSD, 5 business days after every calendar quarter.

5.2 Equipment Inspections

All credit card equipment is to be inspected for tampering or equipment malfunctioning which include added devices or unfamiliar thumb drives, broken parts and any evidence of upgrades. If there is any evidence of tampering or malfunction TSD and Information Technology Services (ITS) must be notified immediately.

5.3 New Payment Gateway or Equipment Purchases

Procurements must be reviewed by TSD and ITS prior to purchase. ITS will review your current processes and provide guidance, recommend the equipment or payment gateway, as well as ensure that the remote access, wireless technologies, firewall and functionality is what is best for the department and the City. ITS will assist with the Technology Purchase Request (TPR) required by Purchasing for the technology purchase. TSD will assist with the bank account and the new MID and/or will add the MID provided by the third-party vendor to the department's MID list in order to send the department an accurate and complete monthly bank activity report.

6.0 CREDIT CARD PROCESSING

6.1 Notification of Changes

It is the department's responsibility to notify TSD if the charges made are not posting to the bank or if the charges posted do not belong to the department.

6.2 Development of Procedures

Each department is to develop and maintain written procedures, which do not supersede the guidance provided in this policy. The procedures developed are to be submitted no less than on an annual basis to TSD.

6.3 Acceptance of Payments

Departments will not accept credit card payments for: 1) Debt payments and 2) Non-sufficient funds (NSF) checks.

7.0 TRAINING

Departments will ensure that applicable personnel are trained in PCI compliance, to be aware of suspicious behavior related to credit card devices and activity on no less than on an annual basis and new employees will be trained at time of hire. Departments will submit a statement to TSD certifying that such training has been completed. ITS, Security Assurance program may assist in making PCI training available.

8.0 SECURITY AND CONTROLS

8.1 Equipment Physical Security

Departments must maintain proper internal controls over credit card equipment and credit card payment information. Physical access to credit card equipment must be restricted to trained and authorized personnel. An access log of employees who are authorized to handle credit card transactions must be maintained and monitored.

8.2 Storing Card Information

Credit card information will not be stored, this includes credit card numbers, date of expiration and security codes. No cardholder data is to be captured by the departments' in any manner including, but not limited to, writing down any cardholder information.

8.3 Separation of Duties

Departments must maintain adequate separation of duties.

8.4 System Access

For systems, such as point of sale devices not managed by ITS, proper account and password management is required. Each system user must be assigned a unique user account with unique ID. No user account or password sharing is allowed. Appropriate complex passwords must be set.

8.5 Information Response

In order to maintain compliance with this Policy and PCI requirements, immediate response to TSD and ITS's notification of changes to technology, equipment, credit card rules, PCI requirements and updates is required.