

**TOWN OF SILVER CITY
CREDIT/DEBIT CARD ACCEPTANCE AND PROCESSING POLICY**

TABLE OF CONTENTS

Introduction	Page 2
Scope	Page 2
Applicable Policies and Procedures	Page 2
Acceptance of Processing	Page 2
Handling Credit/Debit Card Information	Page 2-3
Payment Channels	Page 3 (2-1-1, 2-1-5)
Accounting Controls	Page 3
Refunds/Voids/Credits	Page 3 (3-1-1)
Reconciliation	Page 3 (3-1-2)
Convenience Fee	Page 3
Terminals	Page 4
Payment Card Industry Data Security Standards	Page 4

Introduction

The purpose of these procedures is to provide guidance for accepting credit/debit card payments for services throughout the Town of Silver City accounting controls to mitigate risks of credit/debit card fraud, and an understanding of the Payment Credit Card Industry (PCI) regulations.

Scope

All town employees involved in processing credit transactions and in the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) are subject to the terms of this procedure.

Applicable Policies and Procedures

Payment Card Industry Executive Charter and Compliance Policy
Town of Silver City Internal Controls Policy

Acceptance and Processing

- 1-1-1 Credit/Debit card payments shall be used for the sole purpose of processing payment transaction for services provided by the Town of Silver City to the cardholder. Cash advances or any cash are not authorized at the Town of Silver City.
- 1-1-2 New Services will be requested through the Finance Department in accordance with these standards and approved by the Finance Director. The cost of equipment will be paid from department funds, the Town will obtain the processing fees. Technology implementation must be in accordance with the Payment Card Industry Data Security Standards (PCI DSS).
- 1-1-3 Departments must use the credit/debit card payment processor under contract with the Town of Silver City. The Finance Department will assist in obtaining new services and equipment working with the contracted credit card payment processor. Departments shall not contact the payment processor directly for new equipment or services.

Handling Credit Card Information

In accordance with PCI DSS, Req 12.6.1, all employees involved in processing credit/debit card transactions and the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) must be trained upon hire.

Protecting cardholder data is essential; thus, every effort shall be made NOT to store cardholder information in any form. Any physical access should be appropriately restricted to data or systems that house, process, or transmit cardholder data to not provide the opportunity for persons to access and/or remove devices, data, system, or hardcopies.

For each Payment Channel, the acceptable PCI DSS compliance method is explained below:

- 2-1-1 **Via the phone:** Staff can take credit card payments over the phone.
- 2-1-2 **Via U.S. Mail:** Every effort should be made to not accept credit/debit card information via U.S. mail. If a payment is received with credit/debit card information as a form of payment, the staff will reach out to the customer and inform them this payment cannot be processed.
- 2-1-3 **In Person:** When processing a credit/debit card transaction into the system or POS terminal, it must be processed in full view of the customer. Staff is prohibited from writing or storing card information. Credit/debit card information will be processed directly into the system or POS terminal while the customer is present at the location. Security Controls must be in place when handling in person transactions. The POS terminal will be turned for accessibility by the card user.
- 2-1-4 **Via Fax or Email:** Credit/debit card information cannot be accepted via fax or email or any other unsecure communication medium. If a customer does send an email with their card information, the information should be deleted from all email folders. The customer should also be contacted to indicate that the information has been deleted and the transaction has not been processed. The staff member can work with the customer to complete the transaction in an authorized manner.

Accounting Controls

3-1-1 Refunds, Voids, Credits

1. There will be no refunds issued for credit/debit card payments to the Town of Silver City.
2. There will be no voids issued for credit/debit card payments to the Town of Silver City.
3. Credits will be applied to the customer account for future billing.

3-1-2 Reconciliation

Each day the batches must be closed and reconciled using the daily reports provided with the end of day packet closing.

A detailed reconciliation process will be done monthly in conjunction with the bank reconciliation done by the Finance Department. All copies will be retained for Audit Review.

All deposits will be reviewed and approved by the finance officer.

Convenience Fee

A 3% convenience fee may be charged for credit/debit card transactions.

Terminals (Point of Sale (POS) Equipment

Terminals shall be stored in a physically secure location when not in use. There shall be a documented and periodic review process in place performed at least quarterly to detect any tampering of equipment (unauthorized Payment Card Skimmers) and a log must be maintained of the periodic review.

The Town of Silver City does not use wireless terminals, if this equipment becomes necessary the wireless terminals shall connect directly to the Town of Silver City; approved processor in accordance with Point-to-Point Encryption (P2PE) devices. **Portable devices that attach to tablets, smartphones, etc. are not PCI compliant and should not be used. The Finance Department must be contacted to order credit card equipment.**

Payment Card Industry Data Security Standards

The PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of common-sense steps that mirror security best practices. Noncompliance of these standards can result in significant fines assessed to the Town of Silver City and may result in loss of the ability to accept credit/debit cards.

In order to ensure compliance with PCI DSS requirements an annual PCI Self-Assessment Questionnaire must be completed and submitted to DFA with the interim budget by June 1st of each year.

All standards for the PCI DSS Requirements can be found at:

<https://www.pcisecuritystandards.org/>