Title: CSH109 CREDIT CARD PROCESSING AND HANDLING

Policy: Proper internal control should be maintained over credit card payments to the Municipality to mitigate risk of fraud, control fee expenses, and ensure proper recording of payments.

It is not permissible to retain full credit card information in any form once the transaction is complete.

Purpose: The Municipality of Skagway currently accepts credit cards at several locations within the Borough. The Municipality is responsible for safeguarding and protecting all consumer data received through credit card transactions in accordance with applicable laws and regulations such as Payment Card Industry Data Security Standard (PCI-DSS).

Scope: This procedure applies to all City Hall personnel who have access to credit or debit card numbers accepted for payments to the Municipality. This procedure applies to customer payments including, but not limited to: Harbor fees, utilities, services, permit fees, and property tax. Quarterly Sales Tax returns are not applicable under this procedure and require payment by check or cash only.

Responsibilities:

Borough Employee is responsible for entering credit card information into the credit card processing equipment via manual input or swiping the customer’s card and supplying all pertinent documents to the Borough Tax Clerk.

Borough Tax Clerk is responsible for maintaining daily reports from the merchant website to reconcile with payments received and apply payments to correct customer accounts in the accounting system.

Executive Assistant is responsible for maintaining employee personnel files and ensuring a current Information and Technology Security Policy is on file for authorized employees.

Borough Treasurer is responsible for reconciling general ledger (GL) accounts and bank statements on a monthly basis, including credit card transactions & associated fees.

Borough Manager is responsible for reviewing and approving bank statement reconciliations.

Definitions: PCI-DSS. The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

Procedure:

1.0 MERCHANT ACCOUNT AUTHORIZATION

1.1 All merchant accounts will be set up and maintained by the Borough Treasurer.

1.2 The Borough Treasurer will set up (when applicable) online access to each merchant account and maintain a secure list of login credentials.

1.3 Merchant account statements will be sent to City Hall to be reconciled to actual fees assessed each month and filed by the Treasurer.

2.0 ACCESS TO CUSTOMER CREDIT CARD DATA

2.1 Access to customer credit card data is authorized only to Municipal personnel who are responsible for processing or facilitating credit card transactions.

2.2 Only authorized personnel may process credit card transactions or have access to documentation related to credit card transactions.

2.3 A copy of the Municipality's Information and Technology Security Policy must be read and signed by authorized personnel on initial employment.

2.4 Signed policies will be maintained by the Administrative Assistant/Deputy Clerk and filed in the employee's personnel file at City Hall.

3.0 TRANSMISSION OF CREDIT CARD INFORMATION

3.1 Unsecure (unencrypted) transmission of cardholder data is prohibited. Credit card numbers and cardholder data may not be emailed, faxed, or sent via any electronic messaging technologies such as instant messaging or chat.

3.2 Under no circumstance will credit card numbers received through email be processed.

3.3 The recipient of the credit card number will respond to the sender with a standard template advising that the transaction cannot be processed and offer an acceptable method for transmitting card information. Credit card numbers will be deleted from the response prior to sending. See CSH109 Ex1 TEMPLATE RESPONSE FOR CREDIT CARD NUMBER RECEIVED IN EMAIL.

4.0 CARD NOT PRESENT TRANSACTIONS

4.1 When taking credit card information for processing via telephone, all data recorded is written in a receipt book. This data is limited to the following: cardholder name, account number, expiration date, billing zip code, and three-digit security code (CVV2).

4.2 An email address may be requested if the cardholder would like a receipt emailed to them as proof of payment.

4.3 Once the credit card is manually input into the credit card terminal for processing, the hand written receipt with the cardholder data is destroyed via paper shredder- **no credit card information is retained**.

4.4 A terminal receipt is printed and submitted to the Borough Tax Clerk to enter into the accounting system.

4.5 Once recorded in the accounting system, the Borough Tax Clerk files the credit card payment receipt & related documentation with the daily deposits.

5.0 CARD PRESENT TRANSACTIONS

5.1 A picture ID is required if the card is not signed.

5.2 Once the transaction is complete, the customer is given a receipt or, if requested, emailed a receipt.

5.3 A duplicate receipt is printed, initialed by the Municipal employee, and attached to the invoice or statement documentation provided by the customer.

5.4 All transaction documentation is submitted to the Borough Tax Clerk to enter into the accounting system.

5.5 Once recorded in the accounting system, the Borough Tax Clerk files the credit card payment receipts & related documentation with the daily deposits.

Revision History:

Revision	Date	Resolution #	Description of changes	Requested By
0	12/06/12	RES#13-01R	Initial Release	Heather Rodig
1	03/01/18	RES#18-03R	Review & remove transaction limits	Heather Rodig
2	06/17/21	RES#21-20R	Review & update language	Heather Rodig
3	12/07/23	RES#23-33R	Review & update language	Heather Rodig

[This page intentionally left blank]

CSH109 Ex1 TEMPLATE RESPONSE* FOR CREDIT CARD NUMBER RECEIVED IN EMAIL

Thank you for your recent communication regarding payment for [item or service]. For your protection, we cannot accept credit card information via email. Email is an unsecure means of transmitting information and you should never use it to send your credit card number or other sensitive personal information (passwords, Social Security Number, etc). Please call our office at 907-983-2297 during regular business hours to complete the transaction. Thank you.

Delete the cardholder data from your response and delete the original message after replying.