City of Bothell™

Information Services Division
STANDARD OPERATING PROCEDURES (SOP)

6.9 SECURITY: USER RESPONSIBILITIES

6.9.1 Credit Card Handling Procedures

A. **PURPOSE**: The City of Bothell has developed the below strategy ensure that users accepting credit cards perform the function in alignment with required Banking Industry Security Standards.

B. **REFERENCES**: Information Security Administrative Order.

C. **DEFINITION:**

1) In order for the City of Bothell to accept credit card transactions, we must be compliant with Payment Card Industry Standards. The processes below are in place to ensure credit card transactions are handled correctly.

D. **APPROVED CREDIT CARD TRANSACTION METHODS:**

1) Credit card and cardholder data may be accepted only in person, by phone, or through a City Online application.

E. **PROHIBITED CREDIT CARD TRANSACTION METHODS:**

1) Credit card and cardholder data cannot be accepted or transmitted by email.
2) Credit card and cardholder data cannot be accepted or transmitted by fax, unless fax machine is located in secure location inaccessible to staff not authorized to accept credit card.
3) If credit card information is received by fax or email, alert the customer that credit card information cannot be accepted by these methods and destroy the information.

F. **CARDHOLDER CONFIRMATION:**

1) When accepting a credit card payment and entering it into a City application (online or onsite), staff are required to confirm name on card and cardholder address before processing the payment.
2) When accepting a credit card payment in person, staff are required to confirm cardholder identity against valid identification, like driver's license.
3) When accepting a credit card payment via phone, staff are required to ask the name on the credit card, card billing address, card billing zip code, expiration date and security code. Staff are also required to enter all of this information into credit machine.

10 CREDIT CARD HANDLING AREAS:

1) Work areas containing hard copy or electronic credit card data must be securely locked when staff are not present.
2) Credit card or cardholder data is to be kept out of 'plain site' at all times.
3) Swipe machines are required to be removed from public access spaces and secured when staff are not present.
4) Changes to credit card handling areas, credit card machines, procedures, etc must be reviewed and approved by Information Services and Finance.

11 CREDIT CARD AND CARDHOLDER HANDLING METHODS:

1) Daily transaction information must remain in a locked drawer, locked cash drawer or lock box during business hours. Refer to the Finance Cash Handling Procedures for more information on cash drawers and key management.
2) All daily credit card records/receipts must be secured appropriately at the end of business day per The Finance Cash Handling Procedures. All daily credit card receipts must be delivered to the Finance Department in person and are not permitted to be sent through inter-office mail.
3) Accepting credit cards on behalf of the city, via an approved credit card processing site, is permitted only on a city computer AND through the VPN (if VPN access is available).

12 SECURITY:

1) Only authorized personal are permitted to handle credit card information and training is required. Refer to the Finance Cash Handling Procedures.
2) Any security incident or loss of credit card information must be reported to a supervisor and to Finance Immediately.