CITY OF BELLE ISLE, FLORIDA

CREDIT CARD PROCESSING, REFUND AND SECURITY POLICY

APPROVED DATE: _____

EFFECTIVE DATE: _____

RESOLUTION NO: N/A

Policy is approved and effective as indicated.

_____

Rick Rudometkin, City Manager

A. Purpose

This policy defines the guidelines for accepting and processing credit cards and storing personal cardholder information. It will help ensure that cardholder information supplied to the City of Belle Isle (the City) is secure and protected. Additionally, it helps the City comply with credit card company requirements and the Payment Card Industry (PCI) Data Security Standard.

B. Scope

This policy applies to all City of Belle Isle employees receiving credit card transactions. It pertains to all departments that process, transmit, or handle cardholder information, which may be in a physical or electronic format.

C. Refund Policy

City staff reviews refund requests individually to determine eligibility. If a citation has been dismissed in Court or an overpayment has been made, a refund may be determined appropriate. All valid refunds will be credited to the customer's credit card account within two (2) weeks, or a check may be issued within 30 days of request.

D. Security Policy

All credit card transactions that the City processes must meet the following standards:

1. An installed and maintained firewall configuration protects cardholder data, and transmission of cardholder data is encrypted over public networks. Regularly updated anti-virus software is used. Vendor-supplied defaults for system passwords are not used. Individuals processing payments use unique computer IDs.
2. The city does not transmit electronic credit card numbers or store them on a personal computer or personal e-mail account. Electronic lists of customers' credit card numbers have not been created. Credit card information is only accepted by e-mail, telephone, mail, fax, or in person. E-mail credit files are not subject to Public Records.
3. Physical cardholder data is locked in a secure area with limited access to individuals that require the use of the data. Access is restricted on a 'need to know' basis.
4. Only essential information is stored. The Card Validation Code (also known as the Security Digits, V Code, or CID) is not stored. User PINs or the full data from a card's magnetic stripe are not retained.
5. Credit card information is retained for only the time needed to process and reconcile.

6. Credit card information that does not need to be retained is destroyed. Information is destroyed by shredding (cross-cut) immediately after processing or immediately after it no longer needs to be retained.
7. All terminals used by the City produce credit card receipts which only show up to the last five digits of the credit card number.
8. The individual presenting the payment card must be the cardholder.
9. All departments must comply with the Payment Card Industry Data Security Standard summarized in this policy.
10. If the policy requirements are not followed, the City could be suspended from physical and/or electronic payment options for violating the Payment Card Industry Data Security Standard.

E. Procedures

- Departments that need to accept credit/debit cards and obtain a physical terminal to swipe or key transactions need to contact the Finance Department to execute the required paperwork, obtain a login and PIN, and be given direction on how to process those transactions for accounting purposes and to comply with the proper security measures needed to secure credit card information.
- All servers and computers used for electronic transactions will be secure and Payment Card Industry compliant.
- Employees are expected to regularly check equipment for suspicious behavior, evidence of tampering, or substitution of devices. If unusual conditions exist, employees must contact Finance immediately.
- Employees suspected of possible fraudulent use, misuse, or negligence shall have their login suspended without exception. The Login will only be reactivated after a full audit has been completed and it has been determined that fraudulent use, misuse, or negligence did not occur.
- Employees having been investigated and found to have violated this policy will be disciplined in accordance with the City's Personnel manual.
- Employees verify with the Finance Department on unsolicited third-party persons claiming to be repair or maintenance personnel prior to engaging services.

F. Events

- A city employee shall be designated to accept and process all credit card transactions, not limited to city and non-sponsored events, on-site and off-site events.
- Departments that need to accept credit/debit cards and obtain a physical terminal to swipe or key transactions need to contact the Finance Department to obtain the equipment and the required paperwork, login credentials, and be given direction on how to process those transactions for accounting purposes and to comply with the proper security measures needed to secure credit card information.

G. Training

All employees who process, transmit, or handle cardholder information are required to adhere to its requirements. Department supervisors are responsible for providing this policy to their card-handling employees and providing training on the use of devices and security as it relates to credit cards and related physical cardholder data.

H. Compromised Credit Cards

If the City becomes aware that a customer's credit card number or card processing device has been compromised, it will notify the individuals involved immediately. The City will also contact its service provider, the City Police Department, and other involved associations as necessary to remediate the loss of important information.

I. Service Providers

The City's service providers related to the credit card processing environment include:
Point and Pay LLC (PNP)