Town of Clyde Park

Internal Payment Card Handling Policy

Effective Date: _____
Approved By: _____

Purpose

To protect residents' payment card information and reduce fraud risk, the Town of Clyde Park will handle all credit and debit card transactions in a secure and limited manner.

Scope

This policy applies to all elected officials, employees, contractors, and volunteers who may accept or process card payments on behalf of the Town.

Approved Payment Methods

Card payments may only be accepted through Town-approved secure systems, including:

- Authorized payment terminals
- Approved online payment portals
- Approved third-party processors
- Other systems specifically authorized by the Clerk/Treasurer

No unofficial apps, personal devices, or unapproved websites may be used.

Card Data Protection Rules

Town personnel shall **never**:

- Write down full card numbers
- Store card numbers in paper files, notebooks, spreadsheets, or computers
- Email card numbers
- Text card numbers
- Photocopy cards
- Retain CVV/security codes
- Share payment login credentials

If card information is accidentally received in writing, it must be immediately shredded or securely destroyed after reporting to the Clerk/Treasurer.

Processing Procedures

- Card payments should be entered directly into approved systems only.
- Residents should be encouraged to enter their own card information whenever possible.
- Printed receipts should not display full card numbers.
- Only authorized personnel may handle payment equipment.

Access Control

- Access to payment systems shall be limited to staff with business need.
- Passwords must be unique and kept confidential.
- Shared passwords are prohibited when individual logins are available.

Equipment & Security

- Payment terminals and office computers used for payments must be kept in secure locations.
- Suspicious tampering, damaged terminals, or unusual activity must be reported immediately.
- Computers should remain updated with security patches and antivirus protections.

Incident Reporting

Any suspected fraud, data exposure, lost receipts, phishing email, or unauthorized access involving payment information must be reported immediately to the Clerk/Treasurer and Mayor.

Annual Review

This policy should be reviewed annually and updated as payment systems change.

Employee Acknowledgment

I have read and understand this policy.

Name: _____
Signature: _____
Date: _____