DRAFT – For Discussion Only
Last revised 2022-01-21

City of St. John's Corporate and Operational Policy Manual

Procedure Title: Payment Card Industry Data Security Standard Procedures	
Authorizing Policy: Cash Handling and Petty Cash Policy	
Procedure #: 04-12-01-02	**Last Revision Date:** N/A
Procedure Sponsor: Manager, Budget and Treasury	

1. Procedure Statement

The purpose of these procedures is to identify the business rules, roles, and responsibilities to support the City's compliance with the Payment Card Industry Data Security Standard (PCI-DSS).

2. Definitions

"Cardholder Data" means the information about a cardholder that is collected for the purpose of processing of a credit or debit card transaction, and may include any of the following: contents of the magnetic stripe and/or chip, Primary Account Number (PAN), cardholder name, expiration date, or Card Verification Value (CVV) number.

"Credit Card Processing System" means any electronic system or service used for the completion of credit card transactions, collection or storage of Cardholder Data, creation of Cardholder Data receipts or reports, or analysis and/or disposal of Cardholder Data, for City Merchant accounts. This includes any software applications, hardware, or other electronic devices, including those provided by third-party vendors that process, transmit, store, or display Cardholder Data.

“Department Head” means any Employee reporting directly to the City Manager and/or Council.

“Employee” means any person employed by the City of St. John’s as a permanent, term, part-time, casual, contract, seasonal, temporary, or student worker.

“Payment Card Industry Data Security Standard” (PCI DSS) means the official published set of industry standards and requirements that all credit or debit card processing Merchants are expected to comply with, as set forth by the Payment Card Industry Security Standards Council.

“Merchant” means any department, division, or third-party provider acting on behalf of the City that accepts payment cards (credit or debit) as payment.

3. Procedure Requirements

3.1 General

a) All City credit card Merchant accounts shall be approved by the Department of Finance and Administration.
b) Any proposal for a new process related to the storage, transmission, or processing of Cardholder Data (including, but not limited to, changes to providers, equipment, or processes) shall be approved by the Department of Finance and Administration.
c) Access to the Cardholder Data environment shall be restricted to those Employees with a need to access such environments and appropriate physical and technical controls shall be in place to protect the Cardholder Data environment.
    i. Scanned and printed documents ideally shall not contain any Cardholder Data, and/or if they do, Employees shall redact Cardholder Data from those documents.

ii. Employees interacting with the public via phone shall exclude discussions of Cardholder data from any recordings.
iii. The City shall filter incoming emails to quarantine and secure any Cardholder Data.

d) The City shall require that third-party providers encrypt any Cardholder Data transmitted across open, public networks.
e) No Credit Card Processing Systems shall use vendor-supplied defaults for system passwords or other security parameters.
f) Employees shall comply with the Information Technology Policy and Privacy Management Policy, including, but not limited to, reporting any suspected or known breaches of Cardholder Data or personal information.
g) Employees requiring clarification shall contact the Manager, Budget and Treasury about the interpretation of these procedures.

3.2 Merchant Account Management

Departments with Merchant accounts shall:

a) identify and document all of the forms of card payment activities that occur in their department and maintain a list of Credit Card Processing Systems used to process these payments;
b) assign responsibility for the following tasks to Employee(s) in their department:
i. inspection of PIN pads, terminals, or payment processing workstations for signs of tampering, unauthorized new accounts, or card skimming devices on a weekly basis; and
ii. maintenance of up-to-date lists of (a) all Credit Card Processing Systems including, but not limited to, PIN pads, terminals, and payment processing workstations; and (b) of individuals, including Employees, volunteers, contractors, or consultants, who may access Cardholder Data or Credit Card Processing Systems.

3.3 Storage and Disposal

a) Cardholder Data shall not be stored on any electronic device, including network servers, workstations, laptops, mobile devices, or local or cloud storage.
b) Cardholder Data shall not be transmitted electronically outside of Credit Card Processing Systems, including, but not limited to, email, electronic messaging/meeting applications, voicemail, fax, text messaging, or any other method that may store or transmit electronically.
c) Web payments shall be processed using a PCI-compliant service provider approved by the Department of Finance and Administration.
d) Any paper documents containing Cardholder Data shall:
    i. be limited to only information required to transact business,
    ii. only be accessible to those Employees or third-party vendors who have a business need to have access,
    iii. be in a secure location with sufficient physical safeguards to protect against loss or theft, unauthorized access, disclosure, copying, use, and/or modification, and
    iv. be destroyed via secure records disposal methods (for example, placed in a secure shredding box and shredded by a commercial bonded shredding company) once business needs no longer require retention.
e) All Credit Card Processing Systems shall be programmed to print out only a maximum of the first six characters and the last four of a credit card number.
f) The full contents of any track for the magnetic strip and/or the three-digit card validation code, shall not be stored in a Credit Card Processing System.

3.4 Third-Party Vendors

a) The City shall contractually require that all third-party vendors and any of their subcontractors involved in credit card transactions meet all required PCI data security standards.
b) Third-party vendors shall provide evidence, to the sole satisfaction of the City, of PCI DSS compliance and their efforts at maintaining ongoing compliance.

4. Application

These procedures apply to (i) all City Employees and third-party service providers who have access to Cardholder Data or Credit Card Processing Systems, excluding the St. John's Transportation Commission (Metrobus); (ii) all Cardholder Data; and (iii) all Credit Card Processing Systems.

5. Responsibilities

5.1 The Department of Finance and Administration shall be responsible for:

a) overseeing the implementation of these procedures;
b) management and approval of third-party vendor compliance.

5.2 The Corporate Information Services Division shall be responsible for:

a) filtering incoming emails to quarantine and secure any Cardholder Data.

5.3 Employees involved in the handling or management of Cardholder Data shall be responsible for:

a) complying with these procedures.

5.4 Managers supervising Employees involved in the handling or management of Cardholder Data shall be responsible for:

a) communicating these procedures to applicable Employees in their departments; and
b) having any additional standard operating procedures used by their divisions comply with these procedures and related policies.

5.5 Department Heads shall be responsible for:

a) communicating these procedures to all applicable Employees in their departments; and
b) directing their departments to comply with these procedures.

6. References

01-04-02 Privacy Management Policy
04-12-01 Cash Handling and Petty Cash Policy
02-01-18 Information Technology Policy

7. Approval

- Procedure Sponsor: Manager, Budget and Treasury
- Procedure Writer: Policy Analyst / Manager, Budget and Treasury
- Date of Approval from:
  - Corporate Policy Committee: January 17, 2022
  - Senior Executive Committee:

8. Monitoring and Contravention

The Department of Finance and Administration shall monitor the application of these procedures.

Any contravention of the procedures shall be brought to the attention of the Department of Finance and Administration (including the Human Resources Division); the Office of the City Solicitor; the Office of the Internal Auditor; and/or the City Manager for further investigation and potential follow up disciplinary or legal action, up to and including dismissal.

9. Review Date

Review: Concurrent with the review of Cash Handling and Petty Cash Policy