Category: Administration Policy

Policy Title:	**Protecting Card Holder Data**
Report Number:	**ALT2011-048**
Adopted by:	**Executive Leadership Team**
Effective Date:	**2011/06/22**
Last Amended:	**2021/09/21**
Policy Owner(s):	**CFO's Department / Finance & Supply (Treasury)**

1. PURPOSE

1.1. *The purpose of this policy is to*:

a. Set out the requirements, roles and responsibilities for the secure processing, transmission, storage, and disposal of data relating to payment card transactions to ensure compliance to the Payment Card Data Security Standard (PCI DSS); and

b. Identify required internal controls to reduce the institutional risk associated with the administration and processing of payment cards.

2. POLICY STATEMENT

2.1. The City shall comply with the PCI DSS regardless of where payment card transaction data is processed or stored, through the lifecycle of that data.

2.1.1. Where individual card brands have a rule that exceeds that of PCI DSS, The City will follow the individual card brand's rule.

2.2. Any application, service or solution involved in the processing or transmission of Card holder Data will be implemented and maintained in a manner compliant with PCI DSS and this policy.

2.2.1. Applications, services or solutions that could affect the PCI compliance of The City cannot be procured, developed or implemented without prior approval from the PCI Team and Information Technology.

2.3. The City will ensure applications, services or solutions do not store non-truncated Primary Account Numbers or Sensitive Authentication Data in physical or digital form.

2.4. The City must complete and pass an annual assessment based on the requirements set forth by the Payment Card Brands and defined by Merchant Level. The City must provide an annual Attestation of Compliance to The City's Merchant Service Provider(s) certifying compliance with the PCI DSS.

2.5. Any application, service or solution (internal or external) involved in payment processing must be evaluated for security and compliance risk prior to procurement and again prior to use through an established risk process (e.g. Threat Risk Assessment Questionnaire, Cloud Risk Value assessment or equivalent). The risk assessment will include at minimum:

a. Review of the service providers' policies and certifications that demonstrate their compliance with PCI DSS standards;

b. Identification of any information security risk which may pose a risk to card holder data at rest or in transit; and

c. Review of proposed data flow and architectural diagrams to validate PCI compliance.

2.6. City staff will not directly contract or engage a service provider in any activity that involves possessing Card holder Data, storing, or processing payment cards on behalf of The City without the prior approval of the PCI Team.

2.7. All agreements and contracts with service providers involved in processing payment must include provisions that the service providers are responsible for the security of Card holder Data that they process, store or transmit on behalf of The City.

2.8. The City must maintain up to date and accurate data flow and architectural diagrams showing the implementation of systems and solutions involved in the processing of payment card transactions.

2.9. The City will complete regular vulnerability scanning and penetration testing as required by the PCI DSS, at the request of the PCI Team or after any change or upgrade to a PCI in scope system or service.

3. DEFINITIONS

3.1. In this administration policy:

a. **Attestation of Compliance (AOC)** means a document that serves as a declaration of the merchant's compliance status with the PCI DSS.

b. **Business Unit Technical Resources** means Business Unit technical staff who are not members of IT but who have responsibility for technology and related processes that are related to transmitting, processing, storing or accessing card holder data to process payments;

c. **Card holder** means individual who owns and benefits from the use of a membership card, particularly a payment card;

d. **Card holder Data (CHD)** means elements of payment card information that must be protected, including primary account number (PAN), card holder name, expiration date, and the service code;

e. **Card holder Name** means the name of the individual to whom the card is issued;

f. **CAV2, CVC2, CID, or CVV2 data** means the three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions;

g. **Expiration Date** means the date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card;

h. **Frontline Staff** means individuals responsible for handling and processing payment card payments on behalf of The City;

i. **Internal Security Assessor (ISA)** means a designation given by the PCI Security Standards Council to eligible internal security audit professionals working for a qualifying organization;

j. **Magnetic Stripe (i.e., track) data** means data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction;

k. **Merchant** means a business unit or business line that is approved to accept payment cards and assigned a merchant identification number;

l. **Merchant Level** means a level defined by the volume of transactions processed by a merchant. This level is set by the card brands. The level defines the assessment process the merchant must follow and governs the annual PCI reporting requirements to the card brands;

m. **Payment Card Industry Data Security Standards (PCI DSS)** means the security requirements defined by the Payment Card Industry Data Security Standards Council and the major payment card brands including Visa, MasterCard, Discover, American Express, and JCB;

n. **PCI Team** means the PCI Program Lead and PCI Analyst(s), who are certified by The PCI Council as Internal Security Assessors for The City of Calgary;

o. **PIN or PIN block** means personal identification number entered by the card holder during a card-present transaction, or encrypted PIN block present within the transaction message;

p. **Primary Account Number (PAN)** means a number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device;

q. **Qualified Security Assessor (QSA)** means a person who has been certified by the PCI Security Standards Council to audit merchants for Payment Card Industry Data Security Standard (PCI DSS) compliance;

r. **Self-Assessment Questionnaire (SAQ)** means a validation tools to assist merchants and service providers report the results of their PCI DSS self-assessment;

s. **Sensitive Authentication Data** means additional elements of payment card information required to be protected but never stored. These include magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN or PIN block; and

t. **Service Provider** means a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of card holder data. This also includes companies that provide services that control or could impact the security of card holder data.

4. APPLICABILITY

4.1. This policy and associated standards and procedures apply to all digital or physical assets that connect to or facilitate the transmission, processing, storing or accessing of payment data. The PCI Team will determine what is considered an in-scope PCI asset based on the PCI DSS and scoping exercises which rely on accurate data flow and architectural diagrams. The City will ensure all policies and associated standards related to PCI adhere to this policy.

4.2. This policy applies to all City staff and contractors who have access to payment card information and payment systems, including but not limited to:

a. Every employee that physically accesses areas when payment card information is handled or processed;

b. Employees who contract with service providers (third-party vendors) who process payment card payments on behalf of The City;

c. Employees who manage events and require payment processing capabilities;

d. Information Technology staff and contractors who are responsible for maintaining, designing, supporting and upgrading systems which relate to the processing of payment for The City; and

e. Information Security and Information Technology staff engaged in Incident Response for incidents involving Card holder Data or in scope PCI Assets.

5. LEGISLATIVE AUTHORITY

5.1. The City is subject to the rules and regulations of the PCI Council to maintain annual compliance certification. Failure to maintain compliance can lead to the PCI

Council instituting fines and penalties against The City up to, and including, rescinding the ability to process payment cards.

6. ROLES AND RESPONSIBILITIES

6.1. The PCI Team is responsible for:

a. Providing overall strategic direction for the PCI program at The City;

b. Engaging external QSAs and internal stakeholders for annual PCI assessments;

c. Evaluating and approving all proposed and existing projects which involve the use of payment cards for payment to ensure compliance with PCI DSS;

d. Creating a remediation plan for all additional findings from annual assessments and communicating remediation expectations and timelines to the Merchant;

e. Validating that all systems, services and solutions with identified vulnerabilities or compliance deficiencies are brought into compliance;

f. Executing monthly external vulnerability scans using an Approved Scanning Vendor (ASV):

   i. Notifying responsible parties of the findings of those scans and ensuring responsible parties remediate vulnerabilities; and

   ii. Certifying those results quarterly and submitting to Card Brands as required;

g. Proactively engaging Business Units to review business processes, documentation and other related PCI activities to ensure the Business Unit is in compliance with PCI DSS;

h. Collaborating with Information Technology to review and approve all modifications, exemptions and compensating controls implemented on payment systems and processes impacting card holder data;

i. Providing direction and support to the Business Unit, in conjunction with Information Technology and Corporate Security to define technologies and processes that achieve overall PCI DSS compliance and security best practices;

j. Promoting PCI and Information Security education and awareness throughout The City;

k. Being engaged as a stakeholder in all incidents involving, or suspected of involving, Card holder Data;

l. Notifying Merchant Services Provider and/or PCI brands of suspected or confirmed incidents involving Card holder Data; and

m. Reviewing the list of payment systems and service providers at least annually, or at time of a significant change, to confirm that the providers are compliant with all applicable PCI DSS standards.

6.2. The Chief Financial Officer is responsible for:

a. Reviewing the annual PCI assessment facilitated or completed by the PCI Team which covers:

   i. The scope of the assessment;

   ii. The findings of the Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC); and

   iii. Current compliance status; and

b. Signing Attestation of Compliance on behalf of The City.

6.3. Corporate Security is responsible for:

a. Information Security completes risk assessments of new and existing applications, systems, solutions and processes engaged in the processing of payments to identify potential threats and vulnerabilities and provide direction and guidance to ensure assets and infrastructure remain secure, accurate and available;

b. Providing information to the external QSA and/ or PCI Team as requested to facilitate the annual SAQ or ROC;

c. Complete regular internal vulnerability scanning of payment systems and

   i. Share the findings of those scans with the PCI team and Information Technology and Business Unit to facilitate remediation; and

   ii. Validate that vulnerabilities are remediated;

d. Maintaining and delivering an Information Security Awareness Training Program;

e. Leading the Information Incident Response process for all suspected or actual incidents involving payment processing and Card Holder Data including:

   i. Tampering or theft of hardware used for processing Payment Cards (e.g. Terminals, PIN Pads or card readers);

   ii. Information systems involved in processing of transactions; and

   iii. Loss, theft or unauthorized access or use of media containing Card Holder Data (physical or logical); and

f. Conducting physical risk assessments for new and existing areas where payment processing occurs or where payment data is stored, managed or transmitted (i.e. Data Centre's) including:

    i. Working with PCI Team to identify and implement appropriate physical and technical controls defined by PCI DSS to protect payment card processing, storage or transmission.

6.4. Information Technology is responsible for:

a. Implementing and supporting the infrastructure and applications that underpin The City's payment processing channels;

b. Implementing appropriate security controls to ensure PCI Compliance;

c. Collaborating with Information Security and PCI Team to facilitate risk assessment activities and implement corrective action as required to maintain PCI compliance;

d. Responding to requests from the external QSA and/ or PCI Team to facilitate the annual SAQ or ROC;

e. Advising the PCI Team of any material changes to in-scope PCI assets or processes (i.e. integrations, hardware or software)

f. Informing the PCI Team of any change that may impact PCI Compliance or necessitate additional testing to validate continued compliance with PCI DSS;

g. Remediating vulnerabilities identified through vulnerability scanning (internal and external) or security testing and assessments for payment systems;

h. Installing required security patches to ensure ongoing compliance with PCI DSS;

i. Ensuring an audit trail for all system components engaged in or connected to payment processing as defined by PCI DSS;

j. Creating and maintaining up to date architectural diagrams and data flow diagrams for systems and processes for all assets that connect to or related to the transmission, processing, storing or accessing of card holder data;

k. Documenting and maintaining an up to date asset inventory (including documentation on configuration and installation) for all assets that connect to or related to the transmission, processing, storing or accessing of card holder data;

l. Immediately notifying the Corporate Security of any incident or suspected breach within The City's payment processing channels; and

m. Maintaining a list of known applications that relate to The City's payment card acceptance process and a description of the service provided or application function.

6.5. *Business Unit Technical Resources are responsible for:*

a. Engaging the PCI Team and Information Technology on all new, modified or updated devices connected to the City's network that are involved in or connected to systems that transmit, process, store or access card holder data;

b. Engaging the PCI Team and Information Security for risk assessments and vulnerability scanning on all new, modified or updated devices connected to the City's network that are involved in or connected to systems that transmit, process, store or access card holder data;

c. Creating and maintaining up to date business processes documentation related to the processing, storing and security of card data;

d. Immediately notifying Corporate Security of any suspected breach or issue relating to Card holder Data; and

e. Maintaining a list of service providers that relate to The City's payment card acceptance process and a description of the service provided.

6.6. *Business Unit Leaders are responsible for:*

a. Ensuring that all staff and contractors review and comply with the requirements set forth in this policy;

b. Maintaining an inventory of all payment equipment (i.e. PIN Pads) and regularly inspecting for tampering and validating serial numbers against inventory;

c. Establishing and documenting PCC DSS-compliant business processes;

d. Serving as a point of contact for the PCI Team as it pertains to processing payment card transactions;

e. Ensuring all staff receive annual Information Security Awareness training in compliance with PCI DSS; and

f. Immediately notifying the Corporate Security of any suspected breach or issue relating to Card holder Data.

6.7. *Frontline Staff are responsible for:*

a. Completing annual Information Security Awareness training in compliance with PCI DSS;

b. Completing regular visual inspections of the PIN pads in accordance with the processes documented by the Business Unit;

c. Immediately notifying supervisors of any suspected breach of Card holder Data; and

d. Adhering to and following this policy, related policies, and PCI DSS-compliant processes set forth by the Business Unit to ensure that Card holder Data is properly secured.

7. CONSEQUENCES OF NON-COMPLIANCE

7.1. Failure to adhere to this Policy and its associated standards and procedures may result in disciplinary action in accordance with the Labour Relations Policy.

8. HISTORY

Policy Action	Date	Report Number	Description
New Policy	**2011/06/22**	**ALT2011-048**	**New Policy**
Update	**2013/04/29**		**Update to job title & update to Data Compromise form**
Amendment	**2021/09/21**	**ELT2021-1317**	**Expanded policy statements & roles and responsibilities**