THE CORPORATION OF THE CITY OF WINDSOR
POLICY

Primary Owner:	Financial Acctg & Corp Controls	Policy No.:	FI.A1.22
Secondary Owner:	Taxation & Financial Projects and	Approval Date:	July 11, 2022
	Information Technology	Approved By:	CR285/2022
Subject:	**PAYMENT CARD DATA**	Effective Date:	**IMMEDIATE**
	SECURITY POLICY	Procedure Ref.:	n/a
Review Date:	July 2027	Pages: 7	Date:
Prepared By:	Marco Aquino, Jocelyn De Luna		Replaces:

1. POLICY

1.1. To reduce the risk of credit card fraud, the Payment Card Industry (**PCI**), which consists of the five major credit card brands including VISA and MasterCard, requires its merchants to meet certain conditions when handling credit card data. These conditions are referred to as PCI Data Security Standards (**DSS**).

1.2. The Corporation of the City of Windsor ("the City") is considered a merchant, because it processes credit card transactions through the course of normal business and thus is required to comply with PCI DSS.

1.3. The City is committed to safeguarding cardholder information when storing, transmitting, and/or processing credit/debit card transactions and will comply with the PCI DSS as established and revised by the PCI Security Standards Council.

2. PURPOSE

2.1. To communicate the rules and expectations necessary to facilitate compliance with PCI DSS.

3. SCOPE

3.1. This policy applies to all of the City Departments funded by the City, in whole or part, or whose governing body contains the City's representation **AND** whose financial transactions are accounted for within the City's financial systems **OR** accept credit cards using a City of Windsor merchant identification number (MID).

3.2. Agencies, Boards and Commissions (ABCs) and wholly owned corporations incorporated by the City under Section 203 of the Municipal Act 2001, are encouraged to have a similar policy in the establishment of their respective policies.

3.3. This policy also applies to all of the City employees (including permanent, part-time, temporary, contractual, or seasonal staff) who are involved in accepting or processing credit card payments, including those that have access to cardholder data or cardholder data systems (e.g. network, applications, etc.).

4. DEFINITIONS

4.1. **Attestation of Compliance (AOC)** – a document completed by the company itself or a Qualified Security Assessor that states the company's PCI DSS compliance status.

4.2. **Card Verification Value (CVV**) or **Card Verification Number (CVN**) – the 3 digit security code that is printed on the back of a credit card.

4.3. Cardholder Data (CHD) – the full primary debit/credit account number including any of the following: Cardholder name, expiration date, and/or 3 digit security code, that is printed on front/back of the card.

4.4. Payment Card – for the purposes of this policy, a debit/credit payment card/device that bears the logo of a member of the PCI Security Standards Council.

4.5. Payment Channel – for the purpose of this policy, the methods (e.g. in person, over the phone) by which the public will be able to use a credit card to purchase goods or services from the City.

4.6. Payment Terminal – the device used to take customer card payments via swipe, dip, insert, tap, or manual entry of the card number. Point of Sale (POS) terminal, PIN pad, and credit card machine are also names used to describe these devices.

4.7. PCI Executive Committee – the governance group for the City's PCI efforts. The group consists of a representative from each Department/Board that processes credit card transactions.

4.8. PCI Security Standards Council – the governance body representing the major credit card brands. The "Council's mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders."

4.9. PCI Working Group – a group comprised of representatives from the City's Finance and Information Technology Departments.

4.10. Primary Account Number (PAN) – the 16-digit numeric code (typically for credit or debit cards) located on the front of the card that identifies the issuer and the cardholder account.

4.11. Qualified Security Assessor (QSA) – independent security organization or individual that has been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS.

4.12. Self-Assessment Questionnaires (SAQs) – validation tools intended to assist merchants and service providers to report their compliance with PCI DSS.

4.13. Third-Party Service Providers – any entity directly involved in the processing, storage, or transmission of cardholder data on behalf of the City. This also includes companies that provide services that control or could impact the security of cardholder data.

5. RESPONSIBILITY

5.1. The **Chief Administrative Officer (CAO)** has the following responsibilities:

5.1.1. Ensure that PCI compliance is made a priority at the City by assigning the necessary resources to work on PCI-related matters.

5.1.2. Completion of annual documentation with regards to PCI Compliance.

5.2. The **Chief Financial Officer (CFO)/City Treasurer** or designate has the following responsibilities:

5.2.1. Communicate this policy to all stakeholders

5.2.2. Ensure stakeholder compliance to this policy.

5.2.3. Direct the review of this Policy, at a minimum every five (5) years, or sooner if required, and recommend updates when necessary.

5.3. The **Deputy Treasurer – Taxation, Treasury, and Financial Projects or** designate has the following responsibilities:

5.3.1. Coordination of annual review to facilitate ongoing certification with respect to compliance to PCI DSS.

5.3.2. Coordinate any new installation, removal, returns or replacement of any credit card payment solutions/processes.

5.3.3. Maintain a master list of third-party service providers that accept and/or process online payments, including PCI DSS compliance status (e.g. via an Attestation of Compliance).

5.3.4. Review and approve Third-Party Service Providers' contracts/agreements, and ensure they include an acknowledgement that the Third-Party Service Providers will maintain all applicable PCI DSS requirements and will protect all customers' cardholder data and the Cardholder Data Environment.

5.3.5. Maintain a master list of payment terminals (e.g. PIN Pads, Point of Sale Terminals, and credit card machines).

5.3.6. Develop, implement, and maintain procedures for the use of payment terminals, and provide training regarding those procedures to the users of that technology.

5.4. The **Chief Information Officer/Executive Director of Information Technology** or designate has the following responsibilities:

5.4.1. Coordination of annual review to facilitate ongoing certification with respect to compliance to PCI DSS.

5.4.2. Develop, implement, and maintain procedures, documentation, practices, and standards to address the PCI DSS requirements that pertain to the cardholder data technology being managed by Information Technology Department staff.

5.4.3. Maintain an inventory of system components (software, networking, and hardware (with the exception of PIN Pads and Third-Party Service Providers)) that are in scope for PCI DSS, including all components sourced from a third party.

5.4.4. Implement a formal security awareness program/training for all Information Technology Department staff handling cardholder data and those who support the processes, systems, and applications within the cardholder data environment.

5.5. The **Executive Directors** (or ABC equivalents) or designates have the following responsibilities:

5.5.1. Notify the Deputy Treasurer-Taxation, Treasury and Financial Projects and Chief Information Officer/Executive Director of Information Technology:

5.5.1.1. Prior to adding, removing, or changing any Payment Channel.

5.5.1.2. If any Cardholder Data is being stored and the process being used to store and secure it**.**

5.5.1.3. Of any processes the respective department uses for transmitting cardholder data, so the Deputy Treasurer-Taxation, Treasury and Financial Projects and Chief Information Officer/Executive Director of Information Technology can verify whether those transmissions are secure**.**

5.5.2. Develop, implement, and maintain procedures for the use of the Payment Channels and the security of the Cardholder Data in their respective department.

5.5.3. Ensure all individuals involved in handling cardholder data transactions complete the PCI Security Awareness Program/Training and any other specific PCI training required.

5.5.4. Participate or have a designate participate in the PCI Executive Committee if their department processes credit card transactions.

5.5.5. Ensure employees comply with the provisions of this policy.

5.6. **Department Employees** who are involved in the storing, processing, or transmitting or have access to cardholder data have the following responsibilities:

5.6.1. Complete the PCI Security Awareness Program/Training and any other specific PCI training required.

5.6.2. Maintain confidentiality of the cardholder data.

5.6.3. Ensure adherence with this policy, procedures and directives to facilitate compliance with PCI DSS.

6. <u>GOVERNING RULES AND REGULATIONS</u>

6.1. PAYMENT CARDS

The City only accepts the following Payment Cards for the payment of goods, services, or donations: Visa, Visa Debit, MasterCard, and MasterCard Debit.

6.2. PAYMENT CHANNELS

The City accepts payment card transactions only via the following payment channels with the restrictions noted below: In Person, Postal Mail, Online, and via Phone. Regardless of the Payment Channel, all credit card transactions will be processed directly into a PIN pad or via a Third-Party Service Provider that has been approved by the Deputy Treasurer – Taxation, Treasury, and Financial Projects and the Chief Information Officer/Executive Director of Information Technology.

6.2.1. In Person

- Credit card payments should be completed using an authorized payment solution.

6.2.2. Postal Mail

- Credit card payments should be completed using an authorized payment solution. Cardholder data that is provided in paper format must be treated as confidential and protected against unauthorized access.

6.2.3. Online

- All on-line payments must be processed using a PCI compliant third-party service provider.

6.2.4. Phone

- The use of phones for the collection of cardholder data is only permitted when using technology that has been approved for that purpose by the Chief Information Officer/Executive Director of Information Technology.
- The employee must enter the cardholder data directly into a payment terminal.
- The phone conversation with the customer must not be recorded during the time that the customer is providing credit card information.

6.2.5. Other Payment Channels

- Other than the Payment Channels listed above, no other Payment Channels will be permitted. Under **NO** circumstances will the cardholder data be transmitted/received or accepted via e-mail, fax, voicemail, instant/text messaging or chat.

6.3. CARDHOLDER DATA ACCESS

6.3.1. Each Department must maintain an up-to-date list of individuals (i.e. managers, supervisors, and other staff) who may accept or access cardholder data.

6.3.2. Access to system components and cardholder data must be restricted appropriately based on individual job classification and functions.

6.3.3. Physical access rights granted based on individual function must be regularly reviewed and revoked immediately upon termination or job transfer.

6.4. PROTECTING PIN PADS

6.4.1. All of the City Departments using credit card devices for processing customer transactions must ensure that all devices are secured and protected from tampering and substitution.

6.4.2. Device surfaces must be regularly examined to detect tampering (e.g. addition of card skimmers to devices) or substitution (e.g. by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

6.4.3. The identity of third-party personnel requesting access to payment terminals for reasons such as repairs, inspections, equipment swapping, etc. must be verified prior to granting them access to modify devices. Employees must always verify with their manager that the third party personnel and their devices are legitimate and from a trusted source.

6.4.4. Any new installation, removal, returns, or replacement of any payment terminals from the City's premises must be documented and authorized by the Deputy Treasurer-Taxation, Treasury and Financial Projects or designate.

6.4.5. Departments must maintain an up-to-date inventory of payment terminals (e.g. PIN pads, Point of Sale terminals and Credit card machine) in coordination with the Deputy Treasurer of Taxation, Treasury, and Financial Projects. This inventory should be reviewed at a minimum annually for accuracy.

6.5. MANAGING THIRD PARTY SERVICE PROVIDERS

Third party service providers contracted by the City are an integral part of the City's business and may impact the City's PCI compliance, as well as the security of the cardholder data environment. Departments who work directly with third-party service providers are required to:

6.5.1. Ensure agreements or contracts include clauses that states annual provision of AOC, termination for non-compliance, and that the service provider will be responsible for the security of cardholder data in their possession on behalf of the City.

6.5.2. Consider to include in agreements or contracts clauses related to indemnification rights and special insurance provisions.

6.5.3. Maintain a list of service providers, including pertinent information such as business owner, address, contact information, term of contract, and renewal date, etc.

6.5.4. Annually monitor service providers' PCI DSS compliance status or request proof of PCI DSS compliance via an Attestation of Compliance.

6.6. RETENTION AND STORAGE

6.6.1. Cardholder data must **NOT** be entered/stored on any electronic device including network servers, workstations, laptops, tablets, and cell phones unless it is explicitly approved for use as part of the cardholder data environment.

6.6.2. Cardholder data must **NOT** be stored on any removable storage devices such as USB keys/drives and portable external hard drives. This includes **cardholder data that is contained within** Excel, Word, or PDF file formats.

6.6.3. Cardholder data storage should be kept to a minimum, and retention time should be limited to that which is required for business, legal, and/or regulatory requirements.

6.6.4. All paper records (e.g. receipts, forms) containing cardholder data may only be retained where it is necessary for business or legal purposes and must be kept in a locked cabinet in a secured area or a safe that is accessible only by authorized staff. When no longer needed, the paper record must be securely destroyed (cross-cut shredded) or placed in the designated confidential shred receptacles.

6.6.5. Sensitive authentication data should never be stored or retained after authorization. This includes the 3 digit security code (CVV or CVN) printed on the back of a payment card and personal identification numbers (PINs) entered by the cardholder.

6.6.6. Cardholder data must never be duplicated or scanned using a photocopier or multifunctional devices.

6.7. SECURITY AWARENESS PROGRAM/TRAINING

6.7.1. Employees involved in handling cardholder transactions, including those who support the processes, systems, and applications within the cardholder data environment, must annually complete the PCI Security Awareness Program/Training. That PCI Security Awareness Program/Training may include web-based, pre-recorded, or in-person formal training. Employees will acknowledge that they have read and understood the various information, security policies, and procedures described during that PCI Security Awareness Program/Training.

6.8. INCIDENT REPORTING

6.8.1. In the event of suspected theft or loss of cardholder data, potential cardholder data security breach, or suspected tampering or substitution of a payment terminal or payment card capture device (PIN pad), employees must immediately inform their manager/supervisor. The manager/supervisor will report to the following and assist with investigation of the suspected incident:

- Chief Information Officer/Executive Director of Information Technology
- Deputy Treasurer-Taxation, Treasury and Financial Projects

6.8.2. The Deputy Treasurer-Taxation, Treasury and Financial Projects and Chief Information Officer/Executive Director of Information Technology must report to the CAO all **confirmed** incidents.

6.9. CONSEQUENCE OF NON-COMPLIANCE

6.9.1. Failure to comply with PCI DSS can result in serious consequences for the City including substantial fines and penalties, litigation, reputational damage, revocation of the City's right to accept credit card payments, and other financial costs.

6.9.2. Any employees found to be in violation of their responsibilities under this policy are subject to disciplinary action up to, and including, dismissal.

7. REFERENCES AND RELATED DOCUMENTS

7.1. Information Security Policy

7.2. Acceptable Use Policy

7.3. Fraud and Misuse of Assets Policy

7.4. Accounts Receivable Collections Policy

7.5. Corporate Accounts Receivable Policy