Payment Card Policy

Finance Department

October 2019

Please consider the environment before printing

Consider carefully how the information in this document is transmitted

Payment Card Policy

Responsible officer:

Coordinator Financial Accounting & Services

Authorised by:

Executive Leadership Team

Content Manager file #:

Approval date:

14th October 2019

Annual Desktop Review date:

October 2020

Review date:

Oct 2022

Expiry date:

October 2023

Version number:

1.1

Associated to Strategic Direction #:

Direction 6: Our Commitment to You

Sustainabilty Review:

Contents

1. Purpose

This document and additional supporting documents represents City of Port Phillip's policy to prevent loss or disclosure of sensitive customer information, specifically payment card data.

Failure to protect customer information may result in the following:

- Financial loss for customers,
- Suspension of credit card processing privileges,
- Damage to the reputation of the Council and
- Fines imposed due to failure to comply with the Payment Card Industry Data Security Standards (PCI DSS).

2. Scope

The City of Port Phillip Payment Card Policy applies to all staff, organisations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Council.

3. Definitions

Term	Definition
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Card Holder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Cardholder Name	The name of the Cardholder to whom the card has been issued.
CAV2, CVC2, CID, or CVV2 data	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.
CBA	Commonwealth Bank of Australia
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices. Computer drives should be sanitised in accordance with the relevant ICT Policies. The approved disposal methods are: Cross-cut shredding, incineration, approved shredding or disposal services.
DTS	Digital & Technology Services Department
ERP System	Enterprise Resource Planning System
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorisation during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorisation.
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the Finance department to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions.
Payment Cards	The following cards are accepted at the city of Port Phillip: • Mastercard and Visa Credit • Mastercard and Visa Debit • American Express (Amex) • Eftpos Card
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the major Credit Card Brands: Visa, MasterCard and American Express.

PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit 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.
Sensitive Authentication Data	Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Service Code	The service code that permits where the card is used and for what.

4. Responsibilities

4.1 Financial Accounting Team

Responsible for:

- Ownership and issuing the Payment Card Policy and a Payment Card Procedures
- Ensuring the policy and procedures are regularly reviewed and updated (where required) on an annual basis.
- Any reference to the Finance Department should be read as referring to the Financial Accounting Team, Chief Financial Officer or the Coordinator Financial Accounting & Services
- Processing requests from business units wishing to accept payments by card
- Administering monitoring and storing signed agreements by business units acknowledging their responsibilities
- Maintaining register of Eftpos terminals for tracking
- Liaising with Council's operational banker
- Requesting and issuing payment processing equipment to business units
- Reconciliation and receipt of payments received into Councils bank account

4.2 Coordinator Financial Accounting & Services

Responsible for:

- Ensuring the policy and procedures are regularly reviewed and updated (where required) on an annual basis.
- Reviewing and approving requests from business units to accept payments by card

4.3 Chief Financial Officer

Responsible for:

- Final approval of requests from business units to accept payments by card
- Review and approval of any exceptions to this policy eg alternate payment equipment requests

4.4 Digital Technology Services

Responsible for:

- Reviewing requests from business for external websites to accept card payment
- Approving these in conjunction with Finance

4.5 ASSIST/ Staff processing card payments

Responsible for:

- Adhering to the Payment Card Policy and Payment Card Procedures in the course of their work
- Undertaking the mandatory training as required in order to complete their job in a complaint manner

4.6 PCI Compliance Team

Responsible for:

- Compliance monitoring
- Management of Councils PCI DSS compliant status
- Team comprises the following representatives from Council:
    - Coordinator Financial Accounting & Services
    - Senior Financial Accountant
    - Financial Accountant
    - Coordinator ASSIST
    - ICT Governance and Risk Officer
    - Risk & Compliance Advisor
    - Coordinator Planning Business Support

5. Policy

It is the policy of City of Port Phillip to allow acceptance of payment cards as a form of payment for goods and services. Council requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this policy document, the City of Port Phillip payment card procedures, and other supporting documents.

5.1 PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the major credit card companies including VISA, MasterCard and American Express. These security requirements apply to all transactions surrounding the payment card industry and the merchants/ organisations that accept these cards as forms of payment.

To accept credit card payments, City of Port Phillip must prove and maintain compliance with the Payment Card Industry Data Security Standards. City of Port Phillip's Payment Card Policy and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done in order to reduce the organisational risk associated with the administration of credit card payments by individual departments and to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI DSS).

5.2 Card Acceptance and Approval

All business units that receive or expect to receive payments electronically must comply with the guidelines and procedures issued by Finance.

All business units who wish to take payments via payment cards must be approved by the Coordinator Financial Accounting & Services. All merchants (business units) should submit their requests for approval to the appropriate Level 3 Manager and then forward the signed form to the Financial Accounting Team (email: Helpdesk- Finance). The form 'New Payment Card Merchant Application is available on the intranet at the following location http://intranet.portphillip.vic.gov.au/secured/receipting.htm .

Once approved, the request should be forwarded to the Chief Financial Officer for final approval before implementation.

5.3 Implementation of Payment Card Processing

Business units accepting payment cards will sign an agreement with the Financial Accounting Team that details their responsibilities, as well as the security requirements (Payment Card Industry Data Security Standard and institutional Data Security Policies) that must be followed. This agreement may be updated from time to time as requirements change. Failure to follow the requirements of the agreement may result in the revocation of your ability to accept card payments.

Business units must accept only authorised payment cards and agree to operate in accordance with the contracts the Council holds with its service providers.

5.4 Training

All staff responsible for the handling of credit card information and payment card data must complete mandatory PCI DSS training as detailed in the Payment Card Procedures. Business units will be unable to process payments if staff training is not completed or up to date.

5.5 Acceptable Payment Card Format

Payment card information can only be received via the following channels:

- **In person**- for processing on an approved Commonwealth Bank Eftpos terminal, as allocated by the Financial Accounting Team. All Eftpos terminals must be included on a register that is maintained by Finance.
- **Online**- through approved CoPP websites that comply with PCI DSS requirements which have been pre-approved by Finance- in consultation with Digital Technology Services. e.g. e-Services, St Kilda Festival, South Melbourne Market, BPoint.
- **Over the phone**- through BPoint IVR (Interactive Voice Recognition) – applicable to Rates, Debtors and Animal renewal payments
- **Card not present**- where a payment is processed directly onto an Eftpos terminal using card number information provided by a customer on the telephone while the customer waits. Also known as MOTO (Mail Order/Telephone Order).

Cardholder information received on mailed in forms should be phased out by all business units and will no longer be accepted after the implementation of the Technology One enterprise reporting platform. Refer to Payment Card Guidelines for the procedures on processing these payments.

Email is not permitted:

Cardholder data (CHD) received via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. See below for the appropriate method of responding to and securely destroying the cardholder data.

5.6 Payment Processing Requirements

All processing equipment must be obtained through the Financial Accounting Team (Helpdesk-Finance) and integrate with Councils operational banking provider (CBA).

Exceptions to this policy will be limited and will require a business plan (including reason why the available central processing systems will not work for your area) to be submitted and approved by the Chief Financial Officer in advance of any equipment or system purchase.

All payments received must be directed into a CBA approved bank account. The type and nature of the electronic transaction will dictate where the transaction will be deposited, and is managed by the Financial Accounting Team.

Accounting entries to record the receipt of the payment will be linked directly into the Council's Financial System, whenever possible, to ensure timely recording of transactions and expedite the prompt reconcilement of general ledger and bank accounts.

5.7 Data Retention

As a rule, cardholder data storage should be kept to a minimum in order to reduce risk. The following rules apply for the storage and retention of cardholder data:

- Data storage amount and retention time should not exceed 12 months.
- All paperwork containing credit card information that is to be retained must only display the truncated card number. The maximum number of digits that can be displayed to mask the customer PAN (Primary Account Number) is the first 6 and last 4 digits of the card number e.g. 5163 22XX XXXX 1234.
- All Eftpos terminal receipts only print out the truncated number in order to comply with PCI DSS requirements.
- Scanned documents containing cardholder information are to be stored in secure folders within Record Manager with the PAN truncated as above and access restricted to staff within the relevant business unit as required.
- Paper documents must be kept in a secure location within the business unit, with access restricted to staff with a need to know *Note that provided the cardholder information and PAN is correctly masked, the retention of this paperwork is compliant with PCI DSS standards.
- All data will be treated as confidential.
- Files stored on the network containing card numbers and information are required to be encrypted and password protected with network scans conducted on a quarterly basis to identify those which are not secure for this to be rectified immediately. Refer to the Information Security Policy.

5.8 Disposal of Data

Data that is not necessary in order to conduct business will not be retained in any format.

- Cardholder data that is securely stored on the network will be deleted in accordance with the relevant retention and disposal schedule within Content Manager and the Information Security Policy**.**
- Cardholder data that is correctly truncated and stored on Content Manager will be deleted accordance with the relevant retention and disposal schedule within Content Manager.
- Hard copy physical data is to be securely shredded after 12 months.

6. Compliance Monitoring

The PCI Compliance Team has been established with representation from Finance, Digital and Technology Services, Risk & Assurance, and ASSIST.

The team will meet quarterly or earlier if issues arise.

Standard items will be discussed and addressed by the team as follows:

- Breaches and issues reported to the team
- Review of PCI statistics and tracking
- Monitoring of training registers

7. Relevant Policy, Regulations or Legislation

- Payment Card Industry Data Security Standards (PCI DSS)
- Payment Card Guidelines October 2019
- ICT Policies
- Privacy Policy
- Annual Merchant Survey Renewal