Payment Card Data Handling Guidelines

November 2023

#### City of Port Phillip logo

#### City of Port Phillip

99a Carlisle Street

St Kilda VIC 3182

Phone: ASSIST 03 9209 6777

Email: [portphillip.vic.gov.au/contact-us](mailto:portphillip.vic.gov.au/contact-us)

Website: [portphillip.vic.gov.au](https://www.portphillip.vic.gov.au/)

##### Divercity

Receive the latest news from your City and Council [portphillip.vic.gov.au/divercity](https://www.portphillip.vic.gov.au/about-the-council/divercity-enews-and-local-media)



##### National Relay Service

If you are deaf or have a hearing or speech impairment, you can phone us through the National Relay Service (NRS):

TTY users, dial 133677, ask for 03 9209 6777

Voice Relay users, phone 1300 555 727,

then ask for 03 9209 6777.

[relayservice.gov.au](https://www.infrastructure.gov.au/media-communications-arts/phone/services-people-disability/accesshub" \o "relayservice.gov.au)



## Guidelines

Responsible Service / Department:

Financial Accounting, Finance

Adoption authorised:

ELT

Date of adoption:

20th November 2023

Date effective from:

20th November 2023

Document Set ID (ECM):

[Insert Text]

Subject (Index name in ECM):

[Insert Text]

Endorsed CEO or ELT member or department manager to make and approve document editorial amendments:

Chief Financial Officer

Annual desktop review date:

September

Review date:

October 2025

Completion date:

30 September 2027

Associated Strategic Direction #:

Well-Governed Port Phillip

Associated instruments:

Payment Card Compliance Policy 2023

Supersedes:

Payment Card Guidelines October 2019

Contents

[Guidelines 3](#_Toc149487680)

[Purpose 6](#_Toc149487681)

[Definitions 6](#_Toc149487682)

[Scope 7](#_Toc149487683)

[Overview 8](#_Toc149487684)

[Authorised Personnel 8](#_Toc149487685)

[Police Checks and Approvals 8](#_Toc149487686)

[Training and Reviews 8](#_Toc149487687)

[Internal Procedures- Business Unit 8](#_Toc149487688)

[Payment Card Procedures 9](#_Toc149487689)

[Card Present Transactions 9](#_Toc149487690)

[Procedures for Card Present Transactions 9](#_Toc149487691)

[Review Card Security 9](#_Toc149487692)

[POS Terminal Security 10](#_Toc149487693)

[Manually Keyed Transactions 10](#_Toc149487694)

[Report Suspected Card Fraud 10](#_Toc149487695)

[Card Not Present Transactions 11](#_Toc149487696)

[Procedures for Card Not Present Transactions 11](#_Toc149487697)

[Back Office Procedures 12](#_Toc149487698)

[Reconciliation process 12](#_Toc149487699)

[Refunds 12](#_Toc149487700)

[Chargebacks 14](#_Toc149487701)

[Responding to CHD sent through email 14](#_Toc149487702)

[Suspected breach of security or fraud 14](#_Toc149487703)

# Purpose

To require that all business units within Council who handle payment card information must have access to documented procedures that are consistent with Council policy and cover the processes for complying with the current version of the Payment Card Industry Data Security Standards (PCI DSS).

The intent of these procedures is to provide guidance to Council departments that are responsible for handling or processing payment card transactions from customers for goods or services provided. These procedures should supplement other internal procedures that are in place to minimise the potential for loss of sensitive data belonging to either Council or our customers.

# 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 Electronic Data Disposal |
| **DTS** | Digital & Technology Services Department |
| **ERP System** | OneCouncil |
| **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. |
| **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/Debit 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, 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. |

# Scope

This document applies to all individuals with responsibility, authority, and stewardship over payment card transactions on behalf of Council. All persons who handle payment card transactions assume the responsibility for following the procedures outlined below. This encompasses payment received in all Council systems.

# Overview

## Authorised Personnel

Any department or business units accepting payment cards on behalf of City of Port Phillip for goods or services should designate a full-time employee within that area who will have primary authority and responsibility for payment card and/or ecommerce transaction processing. This should be the Head, Coordinator or Team Leader of the relevant area.

This individual will be responsible for the department complying with the security measures established by the Payment Card Industry and Council policies. In addition, they are responsible for ensuring that any employee or contractor who handles payment card transactions takes the annual PCI training, which will be undertaken through MyPath to ensure staff have received up to date training.

## Police Checks and Approvals

Staff will be required to have an up-to-date police check completed before access is granted to the OneCouncil ECR module by the CFO.

Departments or business units may only use the services of vendors which have been approved/ recommended by the Financial Accounting team to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order, or internet-based.

## Training and Reviews

The Financial Accounting Team will review these procedures annually as part of the compliance review cycle and in consultation with the PCI Compliance Team. All changes and/or revisions will be published on the intranet and will be effective when issued, with any major changes communicated to the Executive team.

Mandatory training on PCI Compliance will be provided to staff involved in card acceptance annually, and as new staff are hired. This training will be available on MyPath.

## Internal Procedures- Business Unit

Any internal procedures undertaken within a business unit which vary from these procedures must be reviewed and approved by the Financial Accounting Team and cannot supplement the requirements contained within this document.

These additional procedures must thoroughly describe the entire transaction process and will include, but are not limited to, the following:

* Segregation of duties
* Deposits
* Reconciliation procedures
* Physical security
* Information disposal
* Data retention
* Cash register/ POS procedures (if applicable)
* Incident response

# Payment Card Procedures

All departments should be using these guidelines for the processing of payment card data. Any additional internal procedures must be reviewed and approved by the Financial Accounting Team.

## Card Present Transactions

Card present transactions require the physical card to be presented at the time of the payment and the payment data entered by swiping, inserting (EMV), or tapping (NFC) the card. Transactions are considered “card present” if the CVV1 is submitted at the time of the transaction. The CVV1 is contained only on the magnetic stripe and is **not** the three-digit verification code (aka. CVV2, CVC2) that is more commonly known.

### Procedures for Card Present Transactions

Where in person payments are received, these procedures and guidelines must be followed:

* Attach any/all form(s) where payment card information is requested (if applicable) ie remittances, invoices, POS dockets
* Only approved staff who have undertaken appropriate training should be handling credit/debit card transactions.

### Review Card Security

* The card may not be used after the last day of the expiration month embossed on the card.
* Only the actual card/account holder should be using the card.
* Where a customer's signature is required, the card is swiped and they sign the back of the merchant copy. Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.
* Check the signature panel on the card to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.
* The account number on the front of the card must match the number on the back of the card and the terminal receipt display. If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.
* Retain the signed merchant copy of the swipe machine-generated receipt and return the other copy to the cardholder.
* Place the merchant copy of the receipt in the cashier drawer. The settlement printout together with all merchant copies form part of the end of day paperwork required to be kept. .

### POS Terminal Security

* POS terminals are checked by staff daily and information is logged into the Swipe Terminal Inventory Sheet as per the Cash Handling Policy.
  + These checks determine if the machine has been tampered with or exchanged (i.e. verify stickers have not been removed and re-affixed, same model, same serial number, etc.). (PCI DSS Requirement 9.9 requires that all swipe terminals must be periodically checked, and those checks must be logged).
* Report any tampering as a [security breach](#Breach) per the steps defined below.
* Keep the machine in a locked area when not in use or after hours.

### Manually Keyed Transactions

* Manually keying in the card account information carries a higher risk of fraud since many of the built-in card security features cannot be accessed. If the magnetic stripe on the back of the card is unreadable, or if you choose to process transactions manually, follow these steps:
  + Key the transaction and expiration date into the terminal.
  + Ask the cardholder to sign the paper receipt and compare the signature to the one on the back of the card to validate the person using the card. If the card is not signed, the card brands deem the card not valid to be used and the transaction can be denied.

### Report Suspected Card Fraud

* If you suspect the card is fraudulent the following process should be followed:
  + Notify your supervisor and the PCI team via email Helpdesk- Finance
  + Advise the customer as follows:

“*We are having issues processing your card and will need to contact the bank. Please take a seat while we look into this”*

* + Verify with your supervisor (or another staff member if Supervisor is unavailable) and the bank that the card is fraudulent. If yes- do not process the payment transaction. Staff member can destroy the card.
  + If the suspected activity involves computers (hacking, unauthorised access, etc.) contact Digital & Technology Services and immediately notify IT Security.

## Card Not Present Transactions

Transactions are considered “card not present” if the CVV1 is not submitted at the time of the transaction because the physical card is not presented. Payments made over the telephone or Internet or sent via mail or fax fall into this category.

Payments received by mail, fax or email are considered high risk for fraud and are subject to greater scrutiny under PCI DSS. These are not accepted by Council under any circumstances.

### Procedures for Card Not Present Transactions

Where card not present payments are received, these procedures and guidelines must be followed:

#### Online Payments

All new online payments for services must be requested and approved by the Finance department and websites or links must be set up by the DTS department only.

Where your business unit accepts online payments via a website separate to Councils main website the following information must be provided to the Financial Accounting Team for review and approval in conjunction with DTS:

* Payment gateway provider
* Payment providers PCI DSS AOC Attestation of Compliance certification
* A copy of the contract with the payment gateway provider
* Web site host information
* Web administrator contact information

The following must be adhered to in the set up of new gateways:

* All new contract specifications should request an up-to-date AOC as part of their insurances and certifications.
* Financial Accounting must be consulted where new payment gateways are proposed and must review the tender or proposal with DTS to address all compliance matters.
* Information for payment settlement into Councils systems will not be provided until the payment gateway submits an up-to-date PCI DSS Attestation of Compliance certification.

**Annual attestation required by Payment Gateway Providers**

As part of the requirement to remain PCI compliant, all payment gateway providers must annually attest to their PCI status.

* Where the provider becomes non-compliant Finance and DTS will work together to transition to a compliant provider as quickly as possible
* Any delay in receiving this information will also result is a review of the service between Finance and DTS and sourcing another compliant solution quickly to ensure Council remain complaint.

#### BPoint IVR

New services for telephone payments using Interactive Voice Response must be requested in writing to the Finance, signed off by a Level 3 Manager for approval by the Chief Financial Officer.

#### Telephone Payments

Payments received via telephone can only be accepted where the payment is processed on an EFTPOS terminal and the cardholder data is not recorded or kept.

* All telephone payments should be entered directly into the payment terminal during the call if possible. Do not accept payment information via a voicemail/phone message.
* Payments should NOT be entered into the online payment applications by Council staff on City of Port Phillip hardware on behalf of the customer as this carries a high risk of fraud and is a breach of PCI DSS requirements.
* Payments should only be processed by authorised staff on approved equipment – in accordance with the Payment Card Compliance Policy (approved by the Financial Accounting Team).

#### Fax Payments

* Not accepted

#### Mailed in forms

* Not accepted

## Back Office Procedures

### Reconciliation process

All business units are required to:

* Close out and settle their payment card terminals daily and
* Reconcile transactions on their Daily Settlement Reports in accordance with the Cash Handling Policy and the ASSIST end of day processes.
* Payments received through web-based payment channels should be reconciled to the bank on a regular basis as agreed between the business unit and Finance Department.

### Refunds

Where a payment is processed through a POS terminal it can be refunded back on the card by the appropriate staff member if the card is present or the customer calls and provides the card number over the telephone so the card number is not stored. The following information must be kept on file for reconciliation and audit purposes:

* The original receipt/ transaction
* Reason for refund or refund request document
* Copy of the receipt reversal

Where a card payment was processed online (Bpoint, Optimo) the payment can be refunded online by the Financial Accounting team who have access to perform this function.

### Chargebacks

All chargeback documentation is received by the Financial Accounting team who will investigate the original transaction with assistance from the business unit to determine if the money should be returned.

## Responding to CHD sent through email

Any open communication system such as email or chat programs are not considered secure for the transmission of any payment card information. These will be blocked on Council servers under DTS policy.

Email and network drives are the property of Council. This includes H drives and desktop folders.

Information stored on these and transmitted by staff is the property of Council and therefore must comply with all policies.

### Repeated non-compliance by staff

Where a staff member repeatedly sends card information through email and is intercepted by DTS the following will occur:

* 1st non-compliance- email notification of blocking by DTS received as normal
* 2nd non-compliance- staff member will be contacted by Finance/PCI team with details of the policy (and their manager copied in)
* Non-compliance will be reported to ELT with repeat offenders highlighted and appropriate actions including PCI merchant training and privacy training.

# Suspected breach of security or fraud

In the event of a security breach/incident, or suspected breach or fraud follow formally assigned duties and responsibilities.

1. Notify your supervisor and the PCI Compliance team (via email Helpdesk- Finance)
2. If the suspected activity involves computers (hacking, unauthorised access, etc.) contact the DTS department immediately
3. Refer to the Incident Response plan located at
   1. [Payments from customers - Council Intranet (portphillip.vic.gov.au)](https://intranet.portphillip.vic.gov.au/guides-tasks-and-tools/finance/payments-from-customers)