

# Payment Card Industry Data Security Standards (PCI DSS) Procedure

## Section 1 - Purpose

- (1) Payment Card Industry Data Security Standards (PCI DSS) is the global data security standard to which all businesses must adhere in order to accept payment by cards, and to store, process, and/or transmit cardholder data. PCI DSS provides guidelines to assist merchants in preventing payment card fraud and to improve security around processing and storage of payment card details. The University of Canberra as part of its merchant agreements is required to be compliant with the PCI DSS.
- (2) The University is committed to safeguarding all payment card data it receives, and complying with PCI DSS requirements. To support this commitment, the University will use, store, transmit and destroy cardholder data (CHD) in a manner which protects the CHD from misuse or unauthorised transactions.
- (3) These procedures support the University's Finance Governance Policy.

## Section 2 - Scope

- (4) These procedures apply to all University staff, contractors or other parties who, while doing business on behalf of the University, are involved in processing, storing or transmitting payment card data.

## Section 3 - Procedures

- (5) These procedures are based on the general principle that staff must only handle payment card account data in a manner which protects the data from misuse or from unauthorised transactions.

### Accepting payment cards

- (6) Capabilities to accept and process payment card information can only be established through Finance, after approval from the Chief Financial Officer. A listing of all such areas shall be maintained by Finance.

### Acceptable payment methods

- (7) Payment card data will only be accepted by the University via these payment methods:
  - a. an approved PCI DSS compliant third-party internet gateway (such as any of the University's eCommerce online sales solutions); or
  - b. an EFTPOS machine (includes payment terminals at parking boom gates).

- (8) Payments must not be accepted and processed if the cardholder provides payment card information via email. If such information is received from a cardholder:
  - a. A reply must be sent to the cardholder, with the payment data deleted from the reply, stating that the University does not accept payment card information via email as this transmission method is not secure. The customer must also be advised of the acceptable methods of payment, per these procedures.
  - b. The email must be permanently deleted (that is, deleted from the Deleted Items folder).
- (9) In exceptional circumstances, payment via Mail Order Telephone Order (MOTO) may be permitted, where approved by the Chief Financial Officer. Cardholder data received via telephone must be processed while the customer is on the line. Writing down a customer's payment card information to process later is prohibited.
- (10) If cardholder data is received via any other method (including but not limited to voicemail, fax, or mail), the message should be deleted/destroyed immediately. The cardholder should then be contacted and advised of the acceptable methods of payment per these procedures.

## Storing, processing and transmitting cardholder data

- (11) Cardholder data is not to be collected, stored, processed or transmitted in any form, except for:
  - a. The acceptable payment methods described above, where the cardholder data is encrypted either within a PCI DSS compliant third-party internet gateway or by an EFTPOS machine.
  - b. Information systems must only store the first six and last four digits of a cardholder Primary Account Number (PAN), the cardholder's name and card expiry date.
- (12) After a payment card transaction is authorised, the following types of data must never be stored in electronic or non-electronic form at a UC facility:
  - a. Magnetic stripe data;
  - b. CVC2/CVV2/CID/CAV2; or
  - c. PIN/PIN block.
- (13) Unless otherwise authorised, credit card PANs on information systems must be masked. The first six and the last four digits of the PAN are the maximum that can be displayed.

## Cardholder data collected through EFTPOS machines

- (14) If not on a tamper proof stand, EFTPOS machines and other such devices used to collect cardholder data must be stored in a safe or locked filing cabinet overnight; or when unattended, locked with a PIN and kept in a secure environment.
- (15) Any suspected or perceived tampering or substitution of EFTPOS devices must be immediately reported to the Chief Financial Officer.

## Service providers and third-party vendors

- (16) All service providers and third-party vendors providing payment card related services for the University must:
- a. Be PCI DSS compliant and provide proof of compliance annually.
  - b. Acknowledge in writing their responsibility for the security of cardholder data in their possession.
  - c. Advise the University immediately in writing if they become aware of a PCI DSS breach.

## Staff access to cardholder data and training

- (17) Managers of business areas processing card payments must ensure that:
- a. Only authorised and properly trained staff with a legitimate business need may process card payments.
  - b. Training in payment card processing is successfully completed before any staff member is permitted to process payment card payments, and that training is successfully completed annually thereafter. Personnel with access to EFTPOS devices are to be trained to be aware of attempted tampering or replacement of devices, to include the following:
    - i. Verify the identity of any third-parties claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
    - ii. Do not install, replace, or return devices without verification.
    - iii. Be aware of suspicious behaviour around devices (for example, attempts by unknown personnel to unplug or open devices).
    - iv. Report suspicious behaviour and indications of device tampering or substitution to the Chief Financial Officer.
  - c. All staff with access to cardholder data have signed an acknowledgement that they understand and will comply with these procedures before being given access to cardholder data.
  - d. A record is maintained of all training and the signed acknowledgements.
  - e. Devices that capture payment card data via direct physical interaction with the card must be protected against tampering and substitution as follows:
    - i. An inventory of all devices is maintained that contains the device make and model, location, serial number, date installed, and date of device inspection. The list must be updated when devices are added, relocated, decommissioned and so on.
    - ii. Devices are periodically inspected for tampering (for example, addition of card skimmers to devices) or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).
    - iii. Inventory is to be audited periodically to ensure accuracy.

## On-going compliance requirements

(18) Finance will:

- a. Maintain a list of authorised third-party credit card processing vendors and service providers.
- b. Maintain a current list of EFTPOS machines.
- c. Perform an annual self-assessment to demonstrate the University's compliance with the PCI DSS.

## Breaches

(19) Any suspected or perceived breach that payment card information has been disclosed, stolen, or misused must be immediately reported to the Chief Financial Officer. Based on the investigative findings, the Chief Financial Officer will decide if other entities are required to be notified of the breach (for example, card associations, merchant bank, cardholders).

## Section 4 – Definitions

TERM	DEFINITION
CDE	Cardholder Data Environment: the system components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and system components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.
CHD	Cardholder Data: at a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.
CVV/CVC	Card Verification Value/Card Verification Code: This is the three-digit security code on the back of a credit card, referred to as CVV2 (Visa) and CVC2 (Mastercard).
EFTPOS	Electronic Funds Transfer Point of Sale: EFTPOS terminals facilitate payments by debit and credit payment cards issued by card schemes, such as Visa and MasterCard.
Merchant	Any person or entity (such as a school/unit) that accepts payment cards as payment for goods and/or services

TERM	DEFINITION
PAN	Primary Account Number: typically a 14- to 19-digit number that serves as a unique identifier on credit and debit cards.
Payment card	Any credit or debit card accepted by the University.
PCI DSS	Payment Card Industry Data Security Standards: an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data.
PIN	Personal Identification Number: secret numeric password known only to the user and a system to authenticate the user to the system.
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.
SAD	Sensitive Authentication Data: Security-related information used to authenticate cardholders and/or authorise payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.
Service Code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things, such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

## Status and Details

<b>Effective Date</b>	28 July 2025
<b>Review Date</b>	28 July 2030
<b>Approval Authority</b>	Geoff Drummond   Chief Financial Officer
<b>Approval Date</b>	24 July 2025
<b>Custodian</b>	Geoff Drummond   Chief Financial Officer

<b>Responsible Manager</b>	Dave Hughes   Treasury & Cash Flow Specialist
<b>Enquiries Contact</b>	<a href="mailto:Policy@canberra.edu.au">Policy@canberra.edu.au</a>