Payment Card Industry Data Security Standards (PCI DSS) Policy

Section 1 - Key Information

Policy Type and Approval Body	Administrative – Vice-Chancellor
Accountable Executive – Policy	Chief Financial Officer
Responsible Manager – Policy	Senior Manager, Business Support Services
Review Date	23 May 2028

Section 2 - Purpose

(1) The Payment Card Industry Data Security Standards (PCI DSS) are a set of industry standards designed to mitigate the risks associated with handling payment card data, including fraud and identity theft.

(2) PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. It promotes consistent security standards to protect cardholder data from fraud and security breaches by defining requirements for ICT systems, networks, and manual processes that handle payment card information.

Section 3 - Scope

(3) This Policy applies to all University staff, contractors or other parties who, in the course of doing business on behalf of the University, are involved in processing, storing or transmitting payment card data.

Section 4 - Key Decisions

Key Decisions	Role
Authorise users and areas to handle payment card data.	Senior Manager, Business Support Services
Determine notification requirements for any detected or suspected breaches of payment card data,	Chief Financial Officer

Section 5 - Policy Statement

(4) In accordance with its merchant agreements with credit card providers, the University is obligated to protect cardholder information during payment transactions. This obligation ensures the security and confidentiality of cardholder data throughout the entire payment process.

(5) The University is committed to safeguarding all payment card data it receives and ensuring compliance with PCI-

DSS requirements. This includes securely using, storing, transmitting, and destroying payment card data to protect against unauthorised access and fraudulent activities.

(6) To maintain PCI DSS compliance, the University must implement and uphold a comprehensive set of controls covering the twelve requirements, organised under six main categories within the entire Cardholder Data Environment (CDE):

Build and maintain a secure network and systems	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	Use and regularly update anti-virus software or programs Develop and maintain secure systems and applications
Implement strong access control measures	Restrict access to cardholder data by business need to know Assign a unique ID to each person with computer access Restrict physical access to cardholder data
Regularly monitor and test networks	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an information security policy	Maintain a policy that addresses information security for all personnel

Section 6 - Procedures

(7) Staff and connected third-parties must handle all cardholder data in a manner consistent with PCI DSS and this Policy. This includes adhering to the guidelines for the entire Cardholder Data Environment (CDE), which encompasses the people, processes, and technology involved in storing, processing, or transmitting cardholder data or sensitive authentication data.

Part A - Staff Handling Payment Card Data

(8) Only authorised and properly trained staff may accept and/or access payment card information.

(9) Staff accepting credit and debit card payments on behalf of La Trobe University must complete the online PCI Merchant (or similar) training module annually, with training records also retained locally.

(10) The Senior Manager, Business Support Services is responsible for maintaining a list of authorised and trained staff which is reviewed on an annual basis.

(11) All staff who complete training must agree to comply with all University policies and procedures as part of this training.

(12) All requests to become an authorised and trained user must be made via a ASK Finance Request and will be assessed and approved on a case by case basis by the Senior Manager, Business Support Services.

Part B - Accepting Payment Cards

(13) The capability to accept and process payment card information can only be established through Finance Operations, after approval from the Senior Manager – Business Support Services. A listing of all such areas shall be maintained by Finance Operations - Business Support Services.

Part C - Acceptable Payment Methods

(14) Payment card data will only be accepted by the University via the following methods:

a. EFTPOS machine
b. Online (via an approved payment system)
c. In-person
d. Telephone

(15) Payments must not be accepted or processed if the cardholder provides payment card information via email. If such information is received:

a. Respond to the cardholder, deleting the payment data from the reply, and state: "La Trobe University does not accept payment card information via email as this transmission method is not secure. Please use one of the acceptable payment methods listed on our website."
b. Permanently delete the email (including from the Deleted Items folder).

(16) Cardholder data received via telephone must be processed whilst the customer is on the line. Writing down a customer's payment card information to process later is prohibited and any calls that are recorded must be paused if a customer needs to provide their cardholder details.

(17) The University does not condone receiving cardholder data on voicemail. In such instances:

a. Staff must enter the cardholder data directly into an EFTPOS pinpad, a virtual terminal, or any other PCI-compliant secure device immediately and then delete the message.
b. Inform the cardholder that La Trobe University will not process future payment card information left on voicemail and advise them of acceptable payment methods under this Policy.

(18) To ensure maximum security during transmission, staff should use devices and systems that employ Point-to-Point Encryption (P2PE) or End-to-End Encryption (E2EE).

Part D - Processing or Transmitting Cardholder Data using La Trobe

(19) Cardholder data, including the Primary Account Number (PAN), must not be entered via a laptop or computer keyboard, or stored, processed, or transmitted on La Trobe University computers, including any portable devices such as USB flash drives, compact disks, personal digital assistants, tablets, or phones.

Part E - Storing Cardholder Data

(20) Hardcopy cardholder data must not be collected or stored in any format, including the Primary Account Number (PAN), expiry date, and credit card security codes (CVV, including CVV2, CVC2, and CID). Any digital storage of cardholder data must use strong encryption or tokenization methods to protect the data. Storing a partial PAN, such as the last four digits, is permitted but must still be handled securely to prevent unauthorised access.

Part F - Cardholder Data Collected Through EFTPOS Machines

(21) EFTPOS machines and other devices used to collect cardholder data must be stored securely when not in use, either in a safe, locked filing cabinet, or with a PIN lock, and kept in a secure environment. Use tamper-evident stickers across the seams of the EFTPOS terminals if available.

(22) Any suspected or perceived tampering or substitution of EFTPOS devices must be immediately reported to the

Senior Manager – Business Support Services or other Finance Director.

Part G - Service Providers and Third-Party Vendors

(23) All service providers and third-party vendors that provide payment card services on behalf of the University must be PCI DSS compliant.

(24) Contracts with service providers and third-party vendors should include a statement requiring the vendor to maintain PCI DSS compliance, provide annual proof of compliance, and immediately notify the University in writing of any PCI DSS breach.

Part H - Incident Response

(25) All suspected breaches must immediately be reported to the IS Service Desk via ASK IS or on telephone number (03) 9479 1500. The IS Service Desk will report all actual or suspected incidents to Finance. Finance, in coordination with IS, will assess the incident, initiate an appropriate investigation, and determine any remedial or corrective actions required in accordance with applicable policies and procedures.

Part I - Ongoing Compliance Requirements

(26) The Chief Financial Officer (or their nominee) is responsible for:

a. maintaining a register of authorised third-party credit card processing vendors, service providers, and EFTPOS terminals;
b. ensuring that, in collaboration with IS and/or Data & Analytics, all system components involved in cardholder data storage, processing, or transmission are appropriately captured and secure;
c. ensuring all financial transactions and payment processing activities are compliant with PCI DSS requirements and University policies, in coordination with relevant business units and Information Services;
d. regularly reviewing financial processes to ensure PCI DSS compliance, identifying any gaps or vulnerabilities, and supporting the development and implementation of remediation plans as needed;
e. ensuring that all University staff involved in payment processing complete the required PCI DSS training and understand their responsibilities;
f. coordinating with the designated Finance and IS contacts to ensure that all financial implications of a security incident are fully assessed, appropriately addressed, and accurately documented in accordance with relevant policies and procedures; and
g. completing and submitting the annual Self-Assessment Questionnaire (SAQ) to demonstrate the University's compliance with PCI DSS, with support and assistance from the University’s PCI DSS compliance partner as required.

(27) The Chief Information Officer (or their nominee) is responsible for:

a. coordinating quarterly internal and external network vulnerability scanning as required;
b. performing an annual self-assessment to demonstrate the University's compliance with PCI DSS in consultation with Digital Service;
c. testing the incident response plan annually;
d. providing annual awareness and training programmes to staff commensurate with their responsibilities; and
e. developing and implement remediation plans for vulnerabilities identified in quarterly scans or other areas of non-compliance, to be fully implemented within one month of identification or sooner based on risk assessment.

Part J - Breaches

(28) Any suspected or perceived breach involving the disclosure, theft, or misuse of payment card information must be immediately reported to the Senior Manager – Business Support Services or other Finance Director. Based on investigative findings, the CFO will decide if other entities need to be notified of the breach (e.g., card associations, merchant bank, cardholders).

(29) Any incidents also need to be reported to the University's Compliance Manager via compliance@latrobe.edu.

Part K - Exemptions

(30) Any request for an exemption from this Policy should be referred to the Senior Manager – Business Support Services or other Finance Director for review and recommendation to the Chief Financial Officer for approval. Any such exemptions are to be fully documented and retained in La Trobe's record management system.

Section 7 - Definitions

(31) For the purpose of this Policy and Procedure:

a. Access Control Measures: Security protocols that restrict access to cardholder data to authorised personnel only.
b. Acquirer: A financial institution that processes credit or debit card payments on behalf of a merchant.
c. Anti-virus Software: Programs designed to detect and remove viruses and other kinds of malicious software from computers and networks.
d. ASK IS: La Trobe University's Information Services help desk for reporting incidents and requesting IT support.
e. Cardholder Data Information: Information associated with a payment card, typically including the primary account number (PAN), cardholder name, expiration date, and service code.
f. Cardholder Data Environment (CDE): The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.
g. CID (Card Identification Number): The Amex Card Identification number is the four-digit, non-embossed number printed above the account number on the face of the card.
h. Critical Incident Management Strategic Framework: A set of procedures and protocols for managing critical incidents at the University.
i. CVC2 (Card Validation Code): The three-digit security code on the back of a credit card issued by MasterCard.
j. CVV (Card Verification Value): A security feature for credit and debit card transactions, providing an additional layer of verification, typically a three- or four-digit number.
k. CVV2 (Card Verification Value): The three-digit security code on the back of a credit card issued by Visa and Discover.
l. Encryption: The process of converting information or data into a code, especially to prevent unauthorised access.
m. EFTPOS (Electronic Funds Transfer Point of Sale): A payment system that allows the transfer of funds from a cardholder's account to a merchant's account at the point of sale.
n. Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
o. Incident Response Team: A group responsible for investigating and responding to security incidents involving cardholder data.
p. Issuer: A financial institution that issues payment cards to consumers.

q. Merchant: Any person or entity (such as a school/unit) that accepts payment cards as payment for goods and/or services.

r. PAN (Primary Account Number): The 14- or 16-digit number on a credit or debit card that identifies the issuer and the specific cardholder account.

s. P2PE (Point-to-Point Encryption): A secure payment technology that encrypts cardholder data from the point of entry to the payment processor, preventing unauthorised access during transmission.

t. Payment Card: Any credit or debit card accepted by the University.

u. PCI DSS (Payment Card Industry Data Security Standards): The Payment Card Industry Data Security Standards are a set of industry standards designed to mitigate the risks associated with handling payment card data, including fraud and identity theft.

v. Payment Card Incident Log: A log used to document actions taken in response to a suspected or actual security incident involving payment card data.

w. Processor: An entity that processes payment card transactions on behalf of a merchant.

x. Self Assessment Questionaire: A validation tool for merchants and service providers to demonstrate compliance with PCI DSS requirements.

y. Senior Manager, Business Support Services: The person responsible for overseeing the business support services at the University, including compliance with payment card processing standards.

z. Service Provider: A business entity that provides services related to processing, storing, or transmitting cardholder data on behalf of another entity.

aa. Tamper-evident stickers: Stickers used to indicate whether a device has been tampered with.

ab. Tokenization: The process of replacing sensitive card information with a unique identifier or token that cannot be reverse-engineered.

ac. Virtual Terminal: A web-based application that allows merchants to process card-not-present transactions securely.

ad. Primary Account Number (PAN): Unique payment card number (typically for credit or debit cards also called account number) that identifies the issuer and the particular cardholder account.

Section 8 - Authority and Associated Information

(32) This Policy is made under the La Trobe University Act 2009.

(33) Associated information includes:

a. PCI DSS Security Standards Council

Status and Details

Status	Current
Effective Date	23rd May 2025
Review Date	23rd May 2028
Approval Authority	Vice-Chancellor
Approval Date	23rd May 2025
Expiry Date	Not Applicable
Responsible Manager - Policy	Jodie Banfield Chief Financial Officer
Enquiries Contact	Finance