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

# Section 1 - Background and Purpose

(1) PCI DSS – Payment Card Industry Data Security Standards 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. La Trobe University as part of its merchant agreements is required to be compliant with the PCI-DSS.

(2) Under PCI DSS requirements, La Trobe University is required to use, store and destroy CHD (cardholder data) in a manner which protects the CHD from misuse or unauthorised transactions.

(3) To ensure staff follow the Payment Card Industry Data Security Standards (PCI DSS) Procedures which provide a set of guidelines in preventing payment card fraud and to improve security around processing and storing of customers' payment card details.

# Section 2 - Scope

(4) Applies to:

a. all campuses
b. all staff
c. any staff taking payments on behalf of LTU
d. any service providers/vendors providing payment card related services to LTU must be PCI DSS compliant

# Section 3 - Policy Statement

(5) The University has entered into merchant agreements with credit card providers and is obligated to protect cardholder information received with any payment transaction.

(6) To ensure the University maintains compliance with the Payment Card Industry Data Security Standards (PCI DSS), which provide a set of requirements for processing, transmission, storage and disposal of cardholder data of payment card transactions, and preventing payment card fraud.

(7) Controls that are required include:

a. the acceptable use of computer equipment within the university;
b. the physical constraints required to protect data and facilities in the Card Data Environments (CDE);
c. security configuration policy for all payment CDE owned, operated, or managed by the University;
d. the security and requirements for any development of payment application software or Web based applications that transmit, process, or store credit card information;

e. the storage and disposal procedure for all confidential or sensitive data, when no longer needed for card processing requirements;
f. the process for logging all actions that occur in the CDE;
g. the control of all backup subsystems and the data therein involved in the CDE;
h. the operating and contractual procedure for sharing all confidential or sensitive data with a 3rd party;
i. the requirements for using wireless communications to transmit sensitive credit card information;
j. all confidential or sensitive electronic data within the University CDE must be protected by approved encryption techniques.

# Section 4 - Procedures

## Part A - Storage of Cardholder Data

(8) CHD should be treated the same as cash, it must be locked in a safe/secure cabinet/lockable office. Scanning of documents containing CHD into TRIM or any other document management system is prohibited. CHD is not to be stored, processed, or transmitted on La Trobe University computers in any form. Access to any physical media (such as paper forms) containing CHD must be limited to only those staff who require it as a part of their job function.

## Part B - Email

(9) Receipt or transmission of emails containing CHD is prohibited. If emails containing CHD are received, do not print or save the email and do not process the transaction. Instead, reply to the email with the CHD removed stating that the university does not accept payment by this method (specify alternative, allowable options). Delete the email and empty the trash folder as well.

## Part C - Paper Forms

(10) Determine whether or not the CHD is actually required to be stored. It is permissible to retain the forms securely for up to 90 days.

(11) If not required to be stored CHD must be destroyed after the payment has been authorised. Ensure documents containing CHD destined for destruction are secured at all times. Appropriate methods to destroy CHD are cross-cut shredding, incinerating, pulping. Shred service containers must be anchored to the wall or located in a secure room with limited access, the key should be controlled at all times. The staff of the contracted company handling the containers must be validated prior to being provided access. The company contracted to shred documents must be PCI-DSS compliant.

(12) If CHD is required to be kept ensure documents are stored in a secure location, such as a locked filing cabinet or safe in a locked office.

(13) Concealing CHD using a permanent marker does not meet minimum requirements for destroying CHD. All CHD must be secured at all times; if staff leave their desk, CHD must be secured.

## Part D - EFT POS devices

(14) All areas that have access to an EFTPOS machine, must adopt a procedure to verify that the EFTPOS has not been tampered with. This must be verified daily (check of serial number and condition of tamper proof seals).

## Part E - Fax Machine

(15) If fax is provided as an option for receipt of CHD, use a specific/dedicated fax machine for the receipt of payments. This fax must be setup to ensure it does not print or display incoming faxes unless a code is entered. Provide the code to only those staff authorised for receipt of cardholder data.

## Part F - Forms With CHD Taken to Cashier

(16) Only PCI-DSS trained LTU staff should hand/carry forms to the cashiers for processing. Any form containing CHD should be treated the same as cash. Cash-handling procedures should reflect the secure transport of all monies, including CHD, Cash and Cheques. A locking bank bag should be used and all monies hand carried to and from destinations. Do not use internal mail for forwarding CHD forms to cashiers.

## Part G - Recording CHD

(17) Typing of the full PAN into a spreadsheet or other type of document is prohibited. CHD must not be recorded in University receipt books.

## Part H - Card Security Codes

(18) Sensitive Authentication Data (magnetic stripe / track, card validation code or value (CCV2, CVC2), PIN data) cannot be stored or recorded under any circumstances once a transaction has been processed.

## Part I - Training

(19) Staff handling CHD are required to complete training on an annual basis. New staff will complete the training upon commencement and annually thereafter. A record of training and the users' acknowledgement of understanding and compliance with all policies and procedures will be recorded.

# Section 5 - Definitions

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

a. Cardholder Data(CHD): Full magnetic stripe or the PAN plus either of the following: Cardholder name, Expiry date, Service Code.
b. Cardholder Data Environment (CDE): Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing storage or transmission.
c. Credit Card Verification (CCV): The 3-digit number on the signature panel of a Visa or Mastercard. These are referred to as CAV2, CVC2, CVV2, or CID depending on payment card brand. The following list provides the terms for each card brand.
    i. CVC2: Card Validation Code 2 (Mastercard) on signature panel;
    ii. CVV2: Card Verification Value 2 (VISA) on signature panel.
d. Electronic Funds Transfer Point of Sale (EFTPOS): Business Units have terminals / machines that facilitate payments by electronic funds transfers based on the use of payment cards, such as debit or credit cards (Visa, MasterCard).
e. Payment Card: Any credit or debit card that bears the logo of Visa, Mastercard.
f. Payment Card Industry Data Security Standards (PCI DSS); is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS

cards defined by the Payment Card Industry Security Standards Council.

g. 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.

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 22nd November 2016 |
| **Review Date** | 30th June 2020 |
| **Approval Authority** | Vice-Chancellor |
| **Approval Date** | 20th November 2016 |
| **Expiry Date** | Not Applicable |
| **Responsible Policy Officer** | Jodie Banfield<br>Chief Financial Officer |
| **Author** | Chuan Tan<br><br>+61 3 9479 6602 |
| **Enquiries Contact** | Finance |