Payment Card Security policy

Section 1 - Preamble

(1) This Policy is effective from 2 July 2020.

Section 2 - Purpose

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

(3) The PCI DSS applies to all entities (including merchants, processors, acquirers, issuers and service providers). It focuses on the promotion of consistent security standards to protect cardholder data from fraud and security breaches by defining requirements for ICT systems, networks and manual processes which handle payment card details.

Section 3 - Scope

(4) 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 - Policy

(5) 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 payment card data in a manner which protects such data from misuse and from unauthorised transactions.

Section 5 - Procedure

Staff that can handle payment card data

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

(7) Staff accepting credit and debit card payments on behalf of Deakin University must on an annual basis complete the on-line PCI Merchant training module.

(8) All relevant staff must complete the on-line PCI Merchant training module upon commencement at Deakin University.

(9) All staff who complete training will agree to comply with all University's policies and procedures as a part of this training. These records will be retained in the University's Learning Management System (LMS).

Accepting payment cards

(10) Capabilities to accept and process payment card information can only be established through Corporate Finance,

after approval from the Director, Corporate Finance. A listing of all such areas shall be maintained by Corporate Finance.

Acceptable payment methods

(11) Payment card data will only be accepted by the University via these payment methods:

a. EFTPOS machine
b. online (via an approved payment system)
c. in-person
d. telephone
e. mail-in.

(12) 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 'Deakin 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 this Policy'
b. the email must be permanently deleted (that is, deleted from the Deleted Items folder).

(13) 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 at a later time is prohibited.

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

a. staff must enter the cardholder data directly into the (EFTPOS) pinpad and then immediately delete the message. If the number is written down, the paper on which the card number has been written should be securely destroyed using a cross-cut shredder immediately after processing the payment, and
b. the cardholder should then be contacted and informed that Deakin University will not process future payment card information left on voicemail. The customer must also be advised of the acceptable methods of payment under this Policy.

(15) Cardholder data received via mail must be transferred securely. No cardholder data is to be emailed internally or externally between staff or customers. No cardholder data is to be despatched via internal mail.

Processing or transmitting cardholder data on Deakin University computers

(16) Cardholder data is not to be entered on a keyboard or stored, processed or transmitted on Deakin University computers including onto any portable devices as USB flash drives, compact disks, personal digital assistants, tablets or phones, in any form unless an exemption has been approved in writing by the Director, Corporate Finance (informed by the Manager Information Systems - Security and Risk) and the appropriate security measures are taken in accordance with PCI DSS.

Storing cardholder data

(17) Hardcopy cardholder data must be stored in a highly secure and protected manner, in a safe or locked filing cabinet that is located in a locked office, and securely destroyed as soon as is practicable for business purposes, using a cross-cut shredder.

(18) Credit card security codes (CVV2, CVC2 and CID) are not to be stored or recorded under any circumstances once a transaction has been processed.

(19) Where (hard copy) cardholder data is required to be retained for business purposes, the data is not to be retained for longer than six months after the date of transaction processing.

(20) Each area that retains cardholder data, must institute a process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements.

(21) Cardholder data is not to be stored for chargeback purposes. Storing the first four and last four digits of a cardholder number, along with time, date, transaction identification and amount is sufficient for chargeback.

Disposing cardholder data

(22) All hardcopy shred bins must remain locked at all times (until shredding). Staff should make every effort to immediately destroy any printed material containing cardholder data using a cross-cut shredder where available.

Cardholder data collected through EFTPOS machines

(23) EFTPOS machines and other such devices used to collect cardholder data if not on a tamper proof stand must be stored in a safe or locked filing cabinet overnight or when unattended, or locked with a PIN, and kept in a secure environment. Tamper evident stickers across the seams of the EFTPOS terminals should also be used if available.

(24) Any suspected or perceived tampering or substitution of EFTPOS devices must be immediately reported to the Director, Corporate Finance.

Service providers and third party vendors

(25) All service providers and third party vendors that provide payment card services on behalf of the University, including processing, storage or transmission of payment card information, must be PCI DSS compliant.

(26) General Counsel will ensure contracts with service providers and third party vendors (who provide payment card services on behalf of the University) contain a statement that the vendor will maintain their PCI DSS compliance and provide proof of compliance annually and advise the University immediately in writing if they become aware of a PCI DSS breach.

(27) Local area contacts with service providers will ensure proof of compliance documents are forwarded to the Director, Corporate Finance annually and retained on the Deakin records management system.

Incident response

(28) The Director, Corporate Finance must maintain security incident response procedures.

On-going compliance requirements

(29) The Director, Corporate Finance is responsible for ensuring the University's compliance with the PCI DSS and will:

a. Maintain a list of authorised third-party credit card processing vendors and service providers with key business and technical contacts.
b. Maintain a current list of EFTPOS machines and computer systems (e.g., workstations, kiosks, web servers, database servers) involved in the storage, processing, and/or transmission of cardholder data as required by PCI DSS or other applicable policies and standards.
c. If required, coordinate quarterly internal network vulnerability scanning of the CDE by eSolutions.
d. If required, coordinate quarterly external vulnerability scanning by a PCI approved scanning vendor.
e. Perform an annual self-assessment to demonstrate the University's compliance with the PCI DSS in consultation with eSolutions.

f. Test the incident response plan, annually.
g. Provide annual awareness and training program to staff commensurate with staff's responsibilities.
h. In consultation with other relevant organisational units of the University, develop and implement remediation plans for vulnerabilities found in the quarterly scans and for any other areas where the business unit is not PCI DSS compliant or compliant with this Policy. Remediation plans should be fully implemented within one month of identification or earlier based on risk assessment.

Breaches

(30) Any suspected or perceived breach that payment card information has been disclosed, stolen, or misused must be immediately reported to the Director, Corporate Finance. Based on the investigative findings the Director, Corporate Finance will decide if other entities are required to be notified of the breach (e.g. card associations, merchant bank, cardholders).

Exemptions

(31) Any request for an exemption from this Policy should be referred to the Director, Corporate Finance for review and recommendation to the Chief Financial Officer for approval. Any such exemptions are to be fully documented and retained on Deakin's record management system.

Section 6 - Definitions

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

a. CVC2: Card Validation Code. This is the three digit security code on the back of a credit card issued by MasterCard.
b. CVV2: Card Verification Value. This is the three digit security code on the back of a credit card issued by Visa and Discover.
c. CDE: Cardholder Data Environment.
d. CID: The Amex Card Identification number is the 4 digit, non-embossed number printed above the account number of the face of the card.
e. EFTPOS: Electronic Funds Transfer Point of Sale.
f. Payment card: Any credit or debit card accepted by the University.
g. PCI DSS: is a proprietary information security standard for organisations 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.
h. VoIP: Voice over Internet Protocol.
i. Merchant: Any person or entity (such as a school/unit) that accepts payment cards as payment for goods and/or services.
j. Payment card: Any credit or debit card accepted by the University.
k. PCI DSS: Payment Card Industry Data Security Standards, developed by the PCI Security Standards Council.

Status and Details

Status	Current
Effective Date	2nd July 2020
Review Date	2nd July 2023
Approval Authority	Vice-Chancellor
Approval Date	1st July 2020
Expiry Date	To Be Advised
Responsible Executive	Kerrie Parker Chief Financial Officer +61 3 92468110
Implementation Officer	Robin Donohue Director, Corporate Finance 924 46755
Enquiries Contact	Robin Donohue Director, Corporate Finance 924 46755