Australian Chiropractic College

MANAGING SPONSORSHIP/SUPPORTER/STUDENT CREDIT/DEBIT CARD DATA

Procedure

DEFINITIONS

Terms in this document, for which definitions are not provided in the text or may not be self-evident or for which usage at ACC may differ to that in other higher education institutions are as follows:

CCV: The Credit Card Verification number on each payment card, as follows:
CVC2: Card Verification Code (MasterCard) on signature panel
CVV2: Card Verification Value (Visa) on signature panel

CID: Card Identification number (American Express) above logo on front of card.

Cardholder Data: Data consisting of the full PAN, or data in the form of the full PAN and any of the following: cardholder name, expiration date and/or the CCV number.

CDE: Cardholder Data Environment: a computer system or networked group of IT systems that processes, stores and/or transmits cardholder data or sensitive payment authentication data. A CDE also includes any component that directly connects to or supports this network.

EFTPOS: Electronic Funds Transfer Point of Sale. The College may use a variety of EFTPOS machines that accept American Express, MasterCard and Visa payment cards. These are sometimes referred to as Merchant Facilities.

Identity and Access Management (IAM): A framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. It is the means by which information technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include single sign-on systems, two factor authentication, multifactor authentication and privileged access management. These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared. IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model.

Instant message: Any form of online chat which offers real-time text transmission over the internet.

Multi-function device: A network-connected printer/scanner/copier/facsimile machine.

PAN: Primary Account Number: the unique payment card number that identifies the issuer and the particular cardholder account.

PCI DSS: Payment Card Industry Data Security Standards**:** a security standard with a set of requirements that must be followed by organisations that handle (accept, transmit, store) payment card data.

Review/Attestation of Compliance: A declaration by an organisation that handles payment card data (i.e. a service provider or third party vendor) that it is compliant with PCI DSS requirements.

SAQ: Self-Assessment Questionnaire: Reporting tool used to document self-assessment results from the College's PCI DSS assessment.

Service providers and third party vendors: Any organisation that processes, transmits or stores cardholder data on behalf of The College.

VoIP: Voice-over-Internet Protocol, i.e., communication received via the internet.

PURPOSE

The purpose of this procedure is to ensure the adoption of efficient and reliable business practices and benefits for persons or organisations making donations and/or payments to the Australian Chiropractic College Limited ('ACC', 'College') through the use of credit or debit cards (payment cards). Such persons or organisations include sponsors, supporters, staff and students.

SCOPE

This document and procedures apply across the College to all staff and their supervisors who:

a. handle or process payment card information or card transactions; or
b. are in a position where they may monitor or approve payment card information or requests for such information.

POLICY

The College and its third party service providers are committed to protecting sponsor/supporter/staff/student payment card data and preserving card provider relationships through compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Failure by the College or its service providers to comply with the PCI DSS may result in substantial fines, loss of the ability to accept payment cards, increased auditing, liability for fraudulent transactions, and damage to the College's reputation.

The College adopts generally accepted systems and procedures supporting its Financial Management and related Invoicing and Cash Receipting processes and ensures a robust approach to its risk management of Information Technology Services, inclusive of Identity and Access Management (IAM).

PROCEDURES

The procedures outlined below are based on the general principle that staff must only accept, transmit, use, retain and/or destroy payment card account data in a manner which protects the data from misuse or from unauthorised transactions.

1. Payment card processing

College professional staff members are responsible for ensuring that:

a) all payments to the College received by payment card are processed by a College approved PCI DSS-compliant third party internet gateway (e.g. any of the College's eCommerce online sales solutions) or an EFTPOS machine approved by the General Manager in accordance with the Invoicing and Cash Receipting

Procedures. (Only EFTPOS machines supplied and owned by the College aligned banking institution will be approved).

b) procedures are in place for all EFTPOS machines to be stored securely when not in use (e.g., when unattended or overnight).
c) procedures are in place to verify weekly that EFTPOS machines have not been tampered with.

Staff authorised to receive payments at Cash Receipting Locations will:

a) if payments are made when the card is **present** (i.e., usually because the cardholder is present in person), process the payment directly on an EFTPOS machine, and not via any other mechanism.
b) if payments are made via **telephone** without the physical card, key the cardholder data received (PAN, expiry date and CCV) directly into the EFTPOS machine and not write it down.
c) if the data is written down, or captured in any form of voice recording, destroy or delete it without delay when the transaction is processed: see Procedure 2.f).
d) if payment is received via a **dedicated analogue fax line**, key the cardholder data into an EFTPOS machine immediately on receipt of the paper fax, and destroy the fax without delay when the transaction is processed: see Procedure 2.f). Physical access to the fax machine must be restricted (e.g., in a locked cabinet or locked room) to staff who meet the requirements of Procedure C.
e) **not** accept or transmit payment details via an **email,** an **instant message,** a **facsimile on a multi-function device,** or a **VoIP fax**, as these forms of transmission are not secure.
f) if an email, instant message or non-complying facsimile is received from an account payer with their PAN:
    1. reply immediately – with the PAN deleted – with the statement "*Your transaction has not been processed. To better protect your identity, the College cannot accept your credit card number over email or facsimile as it is not a secure method of receiving and transmitting cardholder data. Please use an approved method such as telephone, mail, in-person or an online option (if applicable)*."
    2. ensure the email is deleted and the trash folder emptied; or the instant message is deleted; or the facsimile is securely destroyed: see Procedure 2.f).

2. Storing and destroying cardholder data

Any staff member with access to cardholder data will:

a) not store cardholder data (PAN, cardholder name and expiry date with the exception of CCV) unless there is a legitimate business need (e.g. chargeback or refunds) AND a documented storage procedure is approved by the General Manager.
b) once a transaction has been processed, not store or record CCV numbers under any circumstances, nor store other sensitive authentication data, such as data on the magnetic stripe or chip and PINs. (*The College is required to comply with State and Commonwealth legislation related to recordkeeping).*
c) destroy cardholder data as soon as the business need for the storage is no longer relevant, or within six months of the date of the transaction, whichever is shorter. (*The College is required to comply with State and Commonwealth legislation related to recordkeeping).*
d) only store the first six and last four digits of a cardholder PAN, the cardholder name and card expiry date.
e) Ensure any cardholder data in **hard copy** retained under Procedure 2.a. is stored in a secure and protected manner within a locked filing cabinet or safe within a locked office; and that access is restricted to staff with a legitimate business need for such data.
f) In destroying **hard copy** cardholder data, use at least one of the following methods: crosscut shredding, incinerating, or a secure disposal service.
   (For further information on ways to securely destroy cardholder data, including advice on the design of payment forms so that the relevant data can be easily removed, staff are advised to contact the General Manager, who is responsible for PCI DSS Compliance).
g) not store cardholder data on spreadsheets, in College receipt books or in any removable storage medium such as DVDs, CDs or USB flash drives.
h) not store, process or transmit **electronic** cardholder data on College computers (including laptops, tablets or smartphones, hard drive of any computer servers or network storage devices) in any form unless an exception has been approved by the General Manager and a documented procedure has been put in place.

3. Staff access to cardholder data and training

College Professional Staff with authority designated by the General Manager will ensure that:

a) only staff with a legitimate business need for cardholder data are provided with access to such data;
b) training in payment card processing and the PCI DSS is successfully completed before any staff member is permitted to process payment card payments, and that training is successfully completed annually thereafter;
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; and
d) a record of all training and the signed acknowledgements is maintained.

4. Secure data transmittal

All staff with access to cardholder data will ensure that:

a) cardholder data is not transmitted unless the means of transmittal is secure. In general, the only secure method for intra-College cardholder data transmittal is hand delivery or telephone (voice recordings must be deleted without delay when the transaction is processed);
b) no cardholder data is emailed or transmitted as an instant message or text message.
c) no cardholder data is faxed, either internally or externally between staff or sponsors/students, unless both the sending and receiving facsimile machines are directly linked to an analogue line specifically installed for this purpose. PCI DSS compliance by service providers and third party vendors.

5. Service Providers

All service providers and third party vendors providing payment card related services for the College must be PCI DSS compliant;

Any staff engaged in negotiation with service providers and third party vendors for payment card related services will ensure that all service providers and third party vendors have their PCI DSS compliance reviewed annually.

Any payment card data storage in contravention of this procedure will be reported immediately to the General Manager, who will ensure that the data is removed in accordance with these procedures and the PCI DSS.

RESPONSIBILITIES

The College's General Manager is responsible for ensuring that all card payment processes and systems within the College are compliant with these procedures. This involves:

a) allocating responsibilities to suitable staff within the College under these procedures;

b) monitoring PCI compliance and co-ordinating an annual College Review of PCI Compliance and identification of any aspects of the College's card payment processes and systems that need strengthening;

c) periodically arranging random audits for all College business areas in order to verify compliance with these procedures;

d) annual review and update of the Merchant Facilities (EFTPOS) register to facilitate review and monitoring of compliance with these procedures; and

e) coordinating the management of suspected or actual breaches in security of payment card data.

More specifically, in terms of IT Controls, the General Manager is responsible for:

a) Maintaining a documented list of assets, collectively referred to as cardholder data environment (CDE), including servers, network devices and end points, that are considered "in scope" for compliance with PCI

DSS, as well as a network diagram describing the flow of cardholder data.

b) Ensuring that necessary policies and standards as required by PCI DSS are developed, maintained and promulgated to staff responsible for the maintenance of assets that reside within the College CDE.

c) Ensuring that technical controls as required by PCI DSS are in place for all assets within the College CDE. Where it is not practical to implement such PCI DSS controls, then it is the responsibility of the General Manager to consider and develop sufficient mitigating controls.

RELATED DOCUMENTS

- Privacy Policy
- Privacy Procedure
- Privacy Statements for students and staff
- Grievance Management Non-Academic (Students) Policy and Procedures

LEGISLATION

- Financial Management Act 1994
- Collections for Charitable Purposes Act 1939 (SA)
- Privacy Act 1988 (Cth)

VERSION CONTROL

Document: C005 Managing Sponsorship/Supporter/Student Credit/Debit Card Data Procedure		
Responsible Officer: General Manager		
Initially Approved by: Board of Directors		**Date:** October 2016
Reviewed and endorsed by: Finance Audit and Risk Committee		**Date:** 14 July 2021
Reviewed and approved by: Board of Directors		**Date:** 27 July 2021
Version: V1.1	**Replaces Version(s)**: V1.0	**Next Review:** July 2024
Nature of Change	July 2021: • Minor text adjustments, including to 'purpose' and 'policy' sections, and generally up-dating in line responsibilities in the revised Organisational structure.	