Payment Card Industry Policy

POLICY STATEMENT

Palmer College of Chiropractic (College) supports the acceptance of credit cards as payment for goods and/or services and is committed to management of its payment card processes in a manner that protects customer information; complies with data security standards required by the payment card industry; and other applicable law(s). As such, the College requires all individuals who handle, process, support or manage payment card transactions received by the College to comply with current Payment Card Industry (PCI) Data Security Standards (DSS), this policy and associated processes.

PURPOSE

This Payment Card Policy (Policy) establishes and describes the College's expectations regarding the protection of customer cardholder data in order to protect the College from a cardholder breach in accordance with PCI (Payment Card Industry) DSS (Data Security Standards).

SCOPE

This Policy applies to the entire College community, which is defined as including the Davenport campus (Palmer College Foundation, d/b/a Palmer College of Chiropractic), West campus (Palmer College of Chiropractic West) and Florida campus (Palmer College Foundation, Inc., d/b/a Palmer College of Chiropractic Florida) and any other person(s), groups or organizations affiliated with any Palmer campus.

DEFINITIONS

For the purposes of this Policy, the following terms shall be defined as noted below:

1. The term **"College"** refers to Palmer College of Chiropractic, including operations on the Davenport campus, West campus and Florida campus.

2. The term **"Cardholder data"** refers to more than the last four digits of a customer's 16-digit payment card number, cardholder name, expiration date, CVV2/CVV or PIN.

3. The term **"Card-verification value" (CVV2 or CVV)** refers to a three-digit number on the back or four-digit number on the front of a payment card. PCI does not permit the CVV2/CVV to be stored on paper, electronically or by any other means.

4. The term **"Data-Security Standards"** (DSS) refers to standards established by the card brands and the PCI Security Standards Council for payment card security. Merchants must refer to the current and applicable provisions of the DSS: pcisecuritystandards.org/

5. The term **"e-Commerce"** refers to a method of processing electronic payments primarily on the Internet.

6. The term **"Merchant"** refers to the departments authorized by the PCI Committee to accept payment cards using the College's merchant processor(s) as payment for goods and/or services.

7. The term **"PCI Committee"** refers to persons authorized by the College to administer the College's PCI DSS program; monitor merchants' compliance with PCI DSS and the College's PCI Requirements; and review, authorize or deny merchant requests.

8. The term **"PCI Payment Application, PA-DSS-approved software"** refers to Payment Application Data Security Standards (PA-DSS)-approved software sold, distributed, or licensed that stores, processes, or transmits cardholder data as part of authorization or settlement. This includes customized, pre-installed, and "off-the-shelf" software.

9. The term **"Payment-Card Industry (PCI) Security Standards Council"** refers to the council formed by Visa, MasterCard, American Express and Discover to establish Data Security Standards (DSS) for account data protection in the payment-card industry.

10. The term **"Payment-Card Industry Data Security Standards"** refers to a set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.

11. The term **"Payment card(s)"** refers to credit and debit cards bearing the logo of Visa, MasterCard, American Express and Discover used to make a payment.

12. The term **"Third-party vendor"** refers to a business entity directly involved in transmitting, processing or storing of cardholder data, or which provides services that control or could impact the security of cardholder data.

13. The term **"Virtual payment terminal"** refers to Web-browser-based access to a third-party service provider website to authorize payment card transactions, when the

merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card.

POLICY DETAILS

Compliance with PCI DSS

All card payment processes, procedures, technologies, storage, access or other activities must comply with current Payment Card Industry (PCI) Data Security Standards (DSS) and the College's PCI requirements.

Required Pre-approvals

PAYMENT CARD PROCESSING

Only College-authorized merchants that are pre-approved by the PCI Committee can process card payments. Requests for merchant authorization may be made to the Financial Affairs Department. Authorized merchants will be assigned a merchant account number by the Financial Affairs Department.

PAYMENT CARD PROCESSING METHODS

All payment card processing methods must be preapproved by the College's PCI Committee and must comply with PCI DSS and the College's PCI Requirements.

THIRD-PARTY VENDORS

The College can authorize a merchant to use a third-party vendor to process payments only if the vendor provides written verification to the merchant that the vendor is PCI DSS-certified. It is the responsibility of the merchant to obtain written verification from the vendor. Such written verification must be provided to the PCI Committee for review for satisfactory assurance before authorization will be granted.

Additionally, the vendor may be required by the PCI Committee to sign a business associate agreement or service contract. Should a business associate agreement or service contract be required, such agreement or contract must be approved and signed by the College's Treasurer before authorization will be granted.

Transaction Types

This policy applies to merchants using a payment card terminal as well as merchants processing or sending transactions using e-Commerce.

TERMINAL TRANSACTIONS

Terminal transactions include:

a) Face-to-face transactions or transactions via phone line;

b) Cellular terminals;

c) In some cases, a terminal's keypad may be used to enter card-not-present transactions where cardholder data was received via postal mail or over the phone.

E-COMMERCE TRANSACTIONS

e-Commerce transactions include the following:

a) Links on College websites redirecting customers to another payment website;

b) IP-connected terminals processing payments on the Internet;

c) Point-of-sale transactions at a computer cash register using PCI payment applications. This includes point-of-sale software on a computer to transmit, process or store cardholder data;

d) Use of a third-party vendor's virtual payment terminal to transmit, process or store cardholder data; or

e) Transactions transmitted, processed and stored on the College network.

PCI Committee

The College's PCI Committee:

- Administers the College's PCI DSS program;
- Monitors compliance with PCI DSS;

- Monitors compliance with the College's PCI Requirements;
- Reviews requests for merchant authorization and authorizes or denies requests;
- Maintains a current list of PCI DSS standards; terminal locations, terminal IDs, devices that capture payment card data and all employees authorized to use the College's terminals; and
- Notifies the Office of Compliance should a breach or non-compliance with this policy occur.

REPORTING A SUSPECTED BREACH

A. Responsibility to Report

All employees, students and any other members of the College community are required to report any suspected or actual breaches that might involve the acquisition, access use or disclosure of unsecured payment card information **within 24 hours** of discovery.

Additionally, vendors must notify the College if a breach occurs at, or by, the vendor **within 24 hours** of discovery.

B. Who to Contact to Make a Report

Reports may be made to the College through the following reporting options:

- Senior Director of Financial Affairs (563) 884-5141
- Anonymous Reporting (844) 990-0002

RESPONDING TO A BREACH

The College takes reasonable steps to:

1. Review, assess and, if appropriate, investigate all reports or complaints of any potential or actual breaches that might involve the acquisition, access, use or disclosure of unsecured payment card information;
2. Determine if there is a breach;

3. Where breaches are found to have occurred, make appropriate notification to affected individuals; and

4. Where breaches are found to have occurred, take appropriate steps to prevent its recurrence and remedy its effects.

TRAINING

The College requires all employees who handle, process, support or manage payment-card transactions to successfully complete the College's specified PCI DSS and Red Flag compliance training annually. Training is accessed on the College's employee Portal.

STANDARD INSTITUTIONAL POLICY PROVISIONS

Institutional policies are supplemented by provisions that are applicable to all institutional policies. It is the responsibility of all employees and students to know and comply with these standards.

- Standard Provisions Applicable to All Institutional Policies
    - Disciplinary Action
    - Reporting Noncompliance
    - Confidentiality
    - Report Content and Anonymity
    - Retaliation
    - Reporting False Claims
    - Investigations
    - Violations of Law and College Policies
    - Amendment of Policy

Additional Information

ASSOCIATED POLICIES, PROCESSES AND/OR PROCEDURES

This Policy is supplemented below. It is the responsibility of all employees and students to know and comply with policies and procedures as supplemented.

POLICIES

- N/A

PROCESSES AND/OR PROCEDURES

Contact the Financial Affairs Department to obtain copies of the below referenced documents.

- The College's PCI Requirements
- The College's PCI Procedures

FORMS/INSTRUCTIONS

- N/A

OTHER RELATED INFORMATION

- PCI Security Standards Council
  https://www.pcisecuritystandards.org
- Third-Party Vendors
  https://www.visa.com/splisting/
- Glossary of PCI, DSS, PA-DSS Terms, Abbreviations and Acronyms
  https://www.pcisecuritystandards.org/document_library
- PCI Payment Application, PA-DSS Approved Software
  https://www.pcisecuritystandards.org

CONTACTS

Financial Affairs

- Senior Director for Financial Affairs
  1000 Brady Street
  Davenport, IA 52803
  (563) 884-5412

- Laura Regan
  Accountant
  1000 Brady Street
  Davenport, IA 52803
  (563) 884-5876
  laura.reagan@palmer.edu

Security Officer

- James Mountain
  Director of Information Security
  1000 Brady Street
  Davenport, IA 52803
  (563) 884-5728
  james.mountain@palmer.edu

HISTORY

Adopted: ..... Friday, April 6, 2018

Responsible Officer: ..... Jennifer Randazzo, M.A.S., C.P.A.
Vice Chancellor of Finance
Palmer College of Chiropractic
1000 Brady Street
Davenport, Iowa
Phone: (563) 884-5141
jennifer.randazzo@palmer.edu

Issuing Office: ..... Office of Compliance
Earlye Julien, PHR, M.S. Ed., CQIA
Senior Director for Compliance
Palmer College of Chiropractic
1000 Brady Street
Davenport, Iowa
Phone: (563) 884-5476
Fax: (563) 884-5883
earlye.julien@palmer.edu