NICHOLS COLLEGE

PCI Compliance Policy

Name: PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

Purpose: The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for **security management, policies, procedures, network architecture, software design and other critical protective measures** to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

Reason for the Policy: The standards are designed to protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the College. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

Entities Affected by this Policy: All departments that collect, maintain or have access to credit card information must comply with PCI policy. These currently include:

- Student Accounts – accept and process credit cards for payment of student accounts
- Financial Operations - accept and process credit cards for miscellaneous transactions
- Advancement/Alumni - accept and process credit card transactions for various purposes
- Mailroom – accept credit cards for mail transactions (send to Financial Operations for processing)
- Student Records - accept credit cards for transcript costs (send to Financial Operations for processing)
- Admissions – accept credit cards for deposits (send to Financial Operations for processing)

Third Party vendors that process and store credit card information for Nichols using Nichols' merchant accounts include:

- Capital Bankcard – Student Accounts and Financial Operations
- Blackbaud NetCommunity (thru IATS) – Advancement
- Sodexo Dining Services
- Barnes & Noble Book Store
- Square – for Alumni events

Who Should Read this Policy: All persons who have access to credit card information, including:

- Every employee that accesses handles or maintains credit card information. Nichols College employees include full-time, part-time and hourly staff members as well as student workers who access, handle or maintain records
- Employees who contract with service providers (third party vendors) who process credit card payments on behalf of Nichols College
- IT staff responsible for scanning the College systems to insure no credit card numbers are stored electronically.

Definitions:

Merchant Account - A relationship set up by the Controller's office between the college and a bank in order to accept credit card transactions. The merchant account is tied to a general ledger account to distribute funds appropriately to the organization (owner) for which the account was set up.

Coordinator – The college official who has oversight responsibility for the regulation/standard. Regulation monitors stay abreast of updates to their respective regulations, ensure policies are up to date and notify the Information Security Officer and Data Managers about changes.

Credit Card Data - Full magnetic strip or the PAN (Primary Account Number) plus any of the following:

- Cardholder name
- Expiration date
- Service Code

PCI-DSS - Payment Card Industry Data Security Standard

PCI Security Standards Council - The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Self-Assessment - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

Overview: College policy prohibits the storing of any credit card information in an electronic format on any computer, server or database including Excel spreadsheets. It further prohibits the emailing of credit card information. Based on this policy, compliance with a number of the PCI Compliance requirements do not apply. The following list communicates the full scope of the compliance requirements but based on the College policy that prohibits storing of credit card information electronically and utilizing third-party vendors for web based credit card processing, some may not be relevant.

Requirements:

- Build and Maintain a Secure Network
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy
- Insure Third Party Compliance
- Training

Recommendations:

- Complete an annual self-assessment
- Perform a quarterly Network scan

Without adherence to the PCI-DSS standards, the College would be in a position of unnecessary reputational risk and financial liability. Merchant account holders who fail to comply are subject to:

- Any fines imposed by the payment card industry
- Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees
- Suspension of the merchant account.

Procedures:

Nichols requires compliance with PCI standards. To achieve compliance, the following requirements must be met by departments accepting credit cards to process payments on behalf of the College.

General Requirements

- Credit card merchant accounts must be approved by the Controller
- Management and employees must be familiar with and adhere to the PCI-DSS requirements of the PCI Security Standards Council.
- Management in departments accepting credit cards must conduct an annual self-assessment against the requirements and report results to the Coordinator. All employees involved in processing credit card payments sign a statement that they have read, understood, and agree to adhere to Information Security policies of Nichols College and this policy
- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by the Controller.

Online Processing of Credit Card Transactions

- Online credit card transactions can only be processed on desktop computers that have been specifically configured to securely enter these transactions. These desktop computers are setup so that only credit card transactions on the designated credit card processor's secure web site can be processed.
- As of September 12, 2016, only two computers are configured to process online transactions. These computers are located in the Payroll Specialist's office and in the Cashier's office. Use of any other computer to process online credit card transactions is a violation of this policy.

Storage and Disposal

- Credit card information must not be entered/stored on College network servers, workstations, or laptops
- Credit card information must not be transmitted via email
- Web payments must be processed using a PCI-compliant service provider approved by the Controller. Credit card numbers must NOT be entered into a web page of a server hosted on the Nichols College network
- Any paper documents containing credit card information should be limited to only information required to transaction business, only those individuals who have a business need to have access, should be in a secure location, and must be destroyed via approved methods once business needs no longer require retention.
- All credit card processing machines must be programmed to print-out only the last four or first six characters of a credit card number.
- Securely dispose of sensitive cardholder data when no longer needed for reconciliation, business or legal purposes. In no instance shall this exceed 45 days and should be limited whenever possible to only 3 business days. Secured destruction must be via shredding either in house or with a third-party provider with certificate of disposal
- Neither the full contents of any track for the magnetic strip nor the three-digit card validation code may be stored in a database, log file, or point of sale product.

Third Party Vendors (Processors, Software Providers, Payment Gateways, or Other Service Providers)

- The Controller must approve each merchant bank or processing contact of any third-party vendor that is engaged in, or propose to engage in, the processing or storage of transaction data on behalf of Nichols—regardless of the manner or duration of such activities.
- Insure that all third-party vendors adhere to all rules and regulations governing cardholder information security.
- Contractually require that all third parties involved in credit card transactions meet all PCI security standards, and that they provide proof of compliance and efforts at maintaining ongoing compliance.

Self-Assessment

- The Coordinator will notify each department head of the time-line to complete and submit the annual assessment.
- The PCI-DSS Self-Assessment Questionnaire must be completed by the merchant account owner annually and anytime a credit card related system or process changes. This assessment is the responsibility of the head of the department approved to accept credit cards.

Training

- Ongoing training programs must be offered to train employees on PCI DSS and importance of compliance

Responsible Organization/Party: The Controller shall serve as the **Coordinator** of the policy which includes responsibility for notifying the Information Security Officer, applicable Department Heads and Data Managers about changes to the policy. S/he will be assisted by the CIO, the Director of Student Accounts and other College Officers as needed.

Enforcement: The Information Security Officer will oversee enforcement of the policy. Additionally this individual will investigate any reported violations of this policy, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the policy. S/he will be assisted by the CIO, Controller, and the Director of Student Accounts as well as other College Officers as needed.

Additional Resources

- PCI Compliance Guide
- Nichols College Acceptable Use Policy

I have read the PCI Compliance Policy and related documents referenced in the Policy, including the Nichols College Acceptable Use Policy. I understand what the requirements are, and agree to adhere to the requirements of these policies and recommendations.

Name (print): _____

Signature: _____

Date: _____