PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS PROCEDURE

Policy Number: 3.7001
Subject Area: Business Services and Finances
Adopted: 12/18/2017
Revised: 02/14/2024

Oversight

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

Definitions

Merchant Account is a relationship set up by Business Office personnel between Kaskaskia College and a bank in order to accept credit and debit card transactions.

Cardholder Data indicates the full magnetic stripe or the PAN plus any of the following:

- Cardholder name
- Expiration date
- Card Verification Value (CVV) also known as CVM

PAN is the 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**.

Responsibility

The Payment Card Industry Compliance Officer is responsible for the coordination of and oversight for this policy, as well as maintaining documentation to support compliance. Responsibilities also include identification of risks, approval of changes in service providers and payment processing equipment/software, and approval/training of groups with access to cardholder data.

The Information Technology Department is responsible for developing and implementing processes and procedures to support network architecture, software design, and identifying risks and vulnerabilities. Information Technology is also responsible for regularly monitoring the effectiveness of those processes and procedures.

All departments that collect, maintain, or have access to credit and debit card information must comply with this Payment Card Industry policy. These currently include:

- The Business Office accepts mail that may contain credit and debit card information and processes refunds.
- The Accounts Receivable/Cashiers who accept and process credit and debit cards for payment of student accounts and for other customers.
- The Cafeteria accepts and processes credit and debit cards as payment for food items.
- The Executive Director of Development and the Finance & Advancement Services Administrative Assistant who accept or coordinate information on behalf of the College Foundation.
- The Cosmetology Salon accepts and processes credit and debit cards for payments of services offered in the Salon.
- Other groups utilizing the mobile point of sale system kept by the Information Technology Department for the acceptance of credit and debit cards at fundraising or other special events. Use of this mobile system must be approved (in writing) by the Payment Card Industry Compliance Officer or their designee, and the machine must be operated by an employee who has received Payment Card Industry Compliance training from one of the above-listed groups.

No employee, or any other person outside of the groups listed above, may accept, store, or use cardholder data on behalf of the College or under the guise of College business without prior approval by the Payment Card Industry Compliance Officer or their designee.

If a student or customer attempts to provide credit or debit card information to an employee not authorized in the above categories, the employee should direct them to a Cashier for immediate assistance. This rule applies, but is not limited to, education centers, community education, and club transactions. Under **no circumstances** should the employee accept the credit or debit card information for any type of transaction.

No forms developed or used by the College shall provide the opportunity to supply credit or debit card information. Instead, they

should direct customers to a Cashier or online payment. Any links placed on the College website that involve the acceptance of credit and debit cards by the College or any other business must be approved by the Payment Card Industry Compliance Officer or their designee.

Goals:

The College 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. The following list communicates the full scope of the compliance requirements, but based on the College policy that prohibits storing of credit and debit card information electronically and utilizing third party vendors for web-based credit and debit card processing, some listed requirements may not be relevant.

Goals and PCI DSS Requirements

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access• Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for employees and contractors

Procedures

The College requires compliance with Payment Card Industry standards. To achieve compliance, departments accepting credit and debit cards to process payments on behalf of the College must meet the following requirements.

General Requirements

Management and employees must be familiar with and adhere to the Payment Card Industry Data Security Standards requirements of the Payment Card Industry Security Standards Council.

All employees involved in processing credit and debit card payments must sign a statement that they have read, understood, and agree to adhere to the Information Security policies of the College and this policy.

Credit card merchant accounts must be approved by the Business Office.

Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of cardholder data must be brought to the attention of and be approved by the Payment Card Industry Compliance Officer or their designee.

All departments must establish a refund policy addressing credit or debit card transactions. The refund policy must be disclosed to customers, via signs in the physical location or in a relevant place on the website.

The Vice President of Instructional Support & Technology/CIO and the Vice President of Administrative Services must approve all equipment and technologies used to process or access credit and debit card information including remote access technologies, removable media, wireless technologies, laptops, software and other system requirements. Relocation of this equipment and these technologies must also be approved by the Vice President of Instructional Support & Technology/CIO.

Job descriptions for employees with access to cardholder data must be reflective of this access and must include data security requirements associated with access.

All new employees who will have duties handling cardholder data must undergo a background check prior to being hired.

New employees handling cardholder data must undergo Payment Card Industry training upon hire through Safe Colleges.

Existing employees handling cardholder data must undergo Payment Card Industry training annually through Safe Colleges.

Access to the cardholder data environment must be restricted to only those employees with a need to access, and physical controls must be in place to protect the cardholder data environment. Employees may not share cardholder data with other employees unless deemed necessary by a supervisor.

Storage and Disposal

Cardholder data must not be entered or stored on College network servers, workstations, laptops, spreadsheets, or removable

storage devices.

Cardholder data must not be transmitted via email.

The College discourages sending or receiving cardholder data through the mail.

Web payments must be processed using a Payment Card Industry compliant service provider approved by the Vice President of Administrative Services. Credit and debit card numbers must not be entered into a web page of a server hosted on the College network.

Although electronic storage of credit and debit card data is prohibited by this policy, the College will perform a periodic scan to ensure that the policy has not been violated.

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.

If cardholder data must be written down in the event of power failure or other equipment failure, this information should be securely disposed of when no longer needed for reconciliation, business, or legal purposes. In no instance shall this exceed seven days, and should be limited whenever possible to three business days. Secured destruction must occur via shredding, either in house using a crosscut shredder, or with a third-party provider with certificate of disposal.

Any cardholder data kept in a physical format, under circumstances referenced above, must be physically secured at all times. All credit and debit card processing equipment must be physically secured as well.

All credit and debit card processing machines must be programmed to print out only the last four digits of a credit or credit card number and should be regularly inspected for skimming devices or other unusual alterations.

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

The Vice President of Administrative Services must approve each merchant bank or processing contract of any third-party vendor that is engaged in, or propose to engage in, the processing or storage of transaction data on behalf of the College regardless of the manner or duration of such activities.

Third-party vendors must adhere to all rules and regulations governing cardholder information security.

The College must contractually require that all third parties involved in credit and debit card transactions meet all Payment Card Industry security standards, and that they provide proof of compliance and efforts at maintaining ongoing compliance.

Self-Assessment

The Payment Card Industry Self-Assessment Questionnaire must be completed by the merchant account owner annually and anytime a credit or debit card related system or process changes. This assessment is the responsibility of the Information Technology staff in coordination with the relevant department.

Training

Annual training programs must be offered to train employees on Payment Card Industry Data Security Standards and the importance of compliance. This training will be offered through Safe Colleges Training.

Reporting a Suspected Breach

In the event of a suspected breach of security, including the suspicion that credit or debit card information has been exposed, stolen, or misused, immediately notify the Information Technology staff (618-545-3098) and the Payment Card Industry Compliance Officer or their designee.

Payment Card Industry Compliance Officer: Assistant Controller (618) 545-3021.

Approval History: Approved 12/18/17; Revised 02/14/24