

INFORMATION SECURITY POLICY

including

Policy for Credit Card Acceptance to Conduct College Business

SECURITY INFORMATION POLICY FOR ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

CONTENTS

- I. Overview
- II. Definitions
- III. Responsibilities
- IV. Procedures
- V. Related Documents and Forms

SECURITY INFORMATION POLICY FOR ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

I. OVERVIEW

Policy Statement: The Delaware College of Art and Design expects all departments that accept credit cards do so in compliance with credit card industry standards, and in accordance with the procedures put forth in this document. Credit card payments may only be accepted for goods, services, degree program tuition and fees, continuing education tuition and fees, school store purchases, exhibition sales, gifts to the college and library fees. Online credit card payments are accepted only for continuing education and specified gifts and events at the college.

Note: The College is not required to collect sales tax under Delaware law.

Reason for Policy: The College supports the acceptance of credit cards as payment for goods and services and to make cash collection more efficient. In addition, the College must support department compliance with industry standards governing credit card transaction processing, specifically with Payment Card Industry Data Security Standards (PCI DSS).

The security policy creates a roadmap for implementing security measures to protect cardholder data and sets the security tone for the whole college and lets employees know what is expected of them. All employees will be made aware of the sensitivity of the data and their responsibilities and the policy is posted on the website. (12.1)

The Security Policy will be reviewed annually to identify threats and vulnerabilities and results in a formal risk assessment will be updated when the environment changes.

Who Should Read this Policy: Any department that conducts college business using credit cards
Department Directors and Area Coordinators

Acceptable Credit Cards The College currently accepts Visa, MasterCard, Discover and American Express.

SECURITY INFORMATION POLICY FOR ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

Information Policy : Financial Management
Responsible Executive: Chief
Administrative Officer
Responsible Office: Business Office
Originally Issued: June 30, 2010

II. DEFINITIONS

These definitions apply to terms as they are used in this policy.

Cardholder Data	The primary account number and other data obtained as part of a payment transaction, including the credit card account number, cardholder's name, expiration date, service code and/or sensitive authentication data.
Bank	A financial institution that provides merchant accounts to enable the college to accept credit card payments. Funds are deposited into an account established at this institution.
Card Verification Code Value	A data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as the following depending on the payment card brand (e.g. CAV – card authentication value, CVC – card validation code for MasterCard, CVV – card verification value for Visa and Discover, CSC – card security code for American Express).
Chargeback	The deduction of a disputed sale previously credited to the College when the College fails to prove that the customer authorized the credit card transaction.
Customer	An individual or other entity that makes a payment to the College for goods or services.
Magnetic Stripe Information (also known as full track, track 1, or track 2)	The information contained in a credit card's magnetic stripe, including, the PAN, expiration date, customer's name, service code, and other discretionary data, such as PIN, CVV, etc.
Merchant Discount	A percent or per-transaction fee that is deducted from the college's gross credit card receipts and paid to the bank.
MID	Merchant ID. An account established for the College by the bank to credit sale amounts and debit processing fees.
PAN	Primary account number. The 16-digit account number on the front of the credit card.
PCI DSS	"Payment Card Industry Data Security Standard" – 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 security measures on a global basis.

SECURITY INFORMATION POLICY FOR ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

Information Policy : Financial Management
Responsible Executive: Chief
Administrative Officer
Responsible Office: Business Office
Originally Issued: June 30, 2010

II. DEFINITIONS, continued

PCI DSS Workshop	An annual program conducted by the Business Office that includes training and compliant processes and changes in industry standards.
PCI Security Standards Council	An organization for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection in the payment card industry, through education and awareness. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.
PIN	Personal identification number. A numeric password known only to the user and a system to authenticate the user to the system.
ROC	Report on compliance. An annual certification report issued by the PCI Security Standards Council to a third-party provider that has been validated as PCI compliant.
Self-Assessment Questionnaire	One of several forms used as a self-validation tool to assist merchants and service providers in evaluating their compliance with PCI DSS. For more information, contact the Business Office.
Terminal and Printer Processing	A method of processing credit cards at the college.

SECURITY INFORMATION POLICY FOR ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

III. RESPONSIBILITIES

The following are the major responsibilities each department has in connection with this policy.

Business Office

Negotiate all contracts with credit card companies. When evaluating contracts, verify that it will become null and void if the vendor does not maintain PCI DSS compliance.

Oversee the College's merchant accounts, merchant discounts and all other aspects of this policy.

Keep current with PCI DSS regulations and make changes to processes, as appropriate.

Coordinate and account for annual PCI DSS requirements

- Conduct the annual mandatory training sessions
- Collect, review, and remit to the PCI Security Standards Council annual self-assessment questionnaires for processing credit cards
- Confirm that third-party providers have submitted proper documentation.

Provide proper controls regarding who may process credit card transactions (e.g. the Credit Card Refund Authorization form)

Maintain a segregation of duties between employees who process credit card transactions and those who reconcile monthly credit card statements.

Balance the monthly credit card statement with the general ledger within 30 calendar days of the receipt of the bank statement.

Maintain a current list of those individuals with access to credit card data.

Bursar

Point of Sale

Get an authorization from the bank for every transaction.

Validate the signature on the card reasonably matches the signature of the purchaser.

Balance and transmit transactions to the bank daily through the terminals automatic daily batch.

Keep copies of credit card receipts stores securely until they are archived for the period stated in the College's Retention Policy.

Respond promptly to all disputed charges.

Process refunds according to this policy.

Card not Present (e.g. telephone payment or order form)

Obtain the expiration date for use in the authorization process.

Obtain an authorization from the bank for every transaction.

Retain a copy of the confirmation.

Destroy card number after process completion.

SECURITY INFORMATION POLICY FOR ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

III. RESPONSIBILITIES, continued

School Store

Point of Sale

Get an authorization from the bank for every transaction.

Validate the signature on the card reasonably matches the signature of the purchaser.

Turn in credit card transactions receipts to the Business Office daily.

Admissions, Continuing Education, Development and the Library (authorized departments)

Card not Present (e.g. telephone payment, enrollment or registration form)

Obtain the expiration date for use in the authorization process.

Turn in Credit Card Authorization Forms and all supporting documents to the Business Office daily. Do not retain the primary account number.

General Administration

Maintain security standards and employ procedures as required by this policy.

Individual

Report any breaches to Security and the Business Office.

ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

IV. PROCEDURES

A. Standards for Business Processes, Paper and Electronic Processing - Protection of Cardholder data (Requirement 3 and 4)

The standards that follow are adapted from the credit card industry's "Payment Card Industry Data Security Standards (PCI DSS). All departments within the College must comply with these standards.

1. Storage of cardholder data should be kept to a minimum. Bank Statement reconciliations with appropriate receipts will be kept for a time period of six years as required for business, legal and regulatory purposes which is laid out in the College's Retention Policy (**Section 3.1**).
2. The storage of Authentication is not permitted under this policy and will not be permitted in the future. Only the storage of the cardholder's name, primary account number (PAN) and expiration date is permitted and limited to authorized individuals.(**3.2.1**)

Never store the following credit card data: (3.2.2 & 3.2.3)

- Full contents of any track from a magnetic strip
 - CAV2/CVC2, CVV2, CID. These are the three digit numbers from backs of the cards (see "Card Verification Code or Value" in definitions).
 - Personal identification number (PIN) / PIN Block
3. Forms used for credit card sales should locate sensitive cardholder data together on the form, so that it can be easily destroyed and be marked "Confidential".
 4. The Disposal Policy is laid out in the Records Retention Policy and must be adhered to. Annual verification is performed to ensure that this policy is functioning correctly.

Destroy media properly:

- Shred materials so that cardholder data cannot be reconstructed.
 - Render cardholder data received on electronic media unrecoverable so that it cannot be restored.
5. Access to cardholder data is limited to those individuals with a business need as outlined in the Cardholder Data Policy.
 6. Additional Security Requirements.
 - Access privileges are assigned based on position responsibilities. (Section 7)
 - All data controls are reviewed annually confirming that there is a business need to have access to cardholder data.
 - The primary account number (PAN) should be masked showing only the last four digits, anywhere it is stored.
 - Credit card processing areas are restricted to those individuals who have authority to be there.
 - Cardholder information should never be stored electronically. (Section 4.1)
 - Non-electronic records containing cardholder data must be kept in secure locked cabinets.
 - Do not use unsecured e-mail (such as DCAD's Exchange Server) to transmit cardholder data. CAUTION: Instruct customers of this prohibition. If a department receives credit card information via email, the email must be deleted and the customer notified.
 - The Inventory of Devices includes one terminal and printer in the Bursar's Office and one in the School Store (1.4)

SECURITY INFORMATION POLICY FOR

ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

IV. PROCEDURES, continued

B. Prohibited Credit Card Activities

Certain credit card activities are prohibited by credit card companies and DCAD policies.

1. The disbursement of cash from the college for amounts over a sale item is prohibited.
2. Adjustment of the price of goods or services based upon the method of payment (e.g., giving a discount to a customer for paying with cash) is prohibited.

C. Methods of Processing Transactions

There are two acceptable methods for processing transactions: Terminal and printer and secure website (outside vendor verified as PCI compliant).

Method	Description	Sending Transactions to the Bank
Terminal and Printer	Credit card is swiped/entered to obtain authorization for the transaction. Merchant receipts must be secured in a locked, limited access place.	The day's transaction are batched and transmitted to the bank automatically on a daily basis. If the automatic transmittal fails, the prior day's transactions must be batched and transmitted manually before any new transactions can be processed.
Secure Web Site	This is the required method for credit card orders received through the internet. The College uses an outside service provider to process online credit cards. The College does not receive any credit card data electronically.	Transactions are sent automatically to the bank via the gateway service provider.

D. Third Party Outsourcing

Third-party data service providers of storage, processing, or transmission of cardholder data must provide a Report on Compliance (ROC) or be listed on the PCI DSS website as evidence of a successfully completed PSI DSS assessment. The college will not engage any third-party service providers that are not PCI compliant.

E. Transaction Reconciliation

The Business Office will post the sales transactions from the bank to the student records system (Gradpro).

F. Refunds

When an item or service is purchased using a credit card and a refund is necessary, the refund must be credited to the same account from which the purchase was made, unless the original credit card account has been cancelled, in which case the refund may be issued to a different credit card. In addition, documentation of the original charge must be included with any refund transaction processed along with the Credit Card Refund Authorization Form.

ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

IV. PROCEDURES, continued

G. Handling a Customer Disputed Charge

The bank is obligated to provide the College, in writing, of a disputed charge. The College is responsible to provide the bank with written proof that the transaction was authorized by the customer either by a signed transaction receipt, a signed Credit Card Authorization form, completed registration form or a online registration form . Failure to respond and provide a copy of one of these documents will result in a chargeback to the College.

H. Physical Access - Facilities Control (9.1 and 9.3)

Access to building controlled by security guard when the building is open and alarm system when building is closed. Cameras monitor hallways. All students, faculty and staff must carry their DCAD identification card and visitors are limited to the gallery unless they have an appointment. Visitors must sign in and out of the log and are issued a visitors pass and must be accompanied by a DCAD employee. The log is maintained for a minimum of three months.

I. Non-Compliance

Non-Compliance with PCI DSS regulations may have severe consequences to the College's finances and reputation. In the event of data compromise, the College may incur large industry fines and/or be subject to follow-up examination, resulting in significant costs. Further, in the event of a breach, the PCI DSS Council or credit card company has the right to suspend all credit card processing by the College until the required remediation(s) is met.

J. Reporting a Breach

Departments must adhere to the local incident response procedure approved by the Business Office and train/inform all employees on procedures that must adhered to when there is a suspected breach.

- Requirements of the individual: The most effective method to minimize the harm perpetrated in a breach situation is to take immediate action. If you suspect or have a confirmed breach of credit card information, please immediately contact the Business Office at 302-622-8867x121.
- Immediately contain and limit the exposure to prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information.
- The Business office will contact the merchant bank.
- Be prepared to provide all potentially compromised accounts and related information, as requested by the processing bank.
- Be prepared to provide an incident report to Security within three days of the reported compromise

ACCEPTING CREDIT CARDS FOR COLLEGE BUSINESS

V. SECURITY POLICY

DCAD has developed a Technology Policy (Appendix B) that sets operational security procedures including usage policies and wireless access. No contractors should be provided with cardholder data or remote access without prior authorization. (12.2 & 12.3)

VI. NOTICE TO USERS

This Policy may be revised from time to time as necessary to reflect changes in law or other requirements. It is the responsibility of the users to ensure that they have reference to the most current version as posted under policies on the colleges website www.dcad.edu

VII. RELATED DOCUMENTS

- a. Retention Policy
- b. Card Holder Data Policy (June 2010)
- c. Technology Policy (2003)
- d. Transfer of Funds Request Form