Dartmouth College Merchant Credit Card Policy for Processors

Mission Statement

Dartmouth College requires all departments that process, store or transmit credit card data remain in compliance with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the Merchant Credit Card Policy is to protect our customers’ credit card data, to uphold the College’s reputation, to reduce the financial costs associated with a breach of credit card information and to outline best practices for all aspect of credit card transactions.

Background

PCI DSS was established by credit card industry in response to an increase in identity theft and credit card fraud. Every merchant who handles credit card data is responsible for safeguarding that information and can be held liable for security compromises. This standard has 12 requirements, including controls for handling credit card data, computer and internet security and an annual self assessment questionnaire.

The College launched the Card Privacy and Control (CPAC) Project in 2008. The project objective is to review all credit card merchant accounts, identify all the systems, applications and devices that process, store or transmit cardholder data. CPAC will identify and implement any business or technological changes required to comply with PCI DSS.

Entities Affected By This Policy

Departments that accept credit card payments and retain sensitive cardholder data in paper or electronic format.

Who Should Read This Policy

- **Merchant Credit Card Policy – for Processors (how to handle credit card information)**

  Any persons including part-time students with the responsibilities of processing, storing or transmitting credit card data.

What is PCI Data Security Standard

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. The PCI standard is comprised of 12 requirements. They are summarized below but more detail can be found at: [https://www.pcisecuritystandards.org/security_standards/documents.php?category=standards]
Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Compliance Certification Process

Confidentiality Form

All individuals involved in processing, storing or transmitting credit card data must sign a PCI confidentiality statement.

See Exhibit 1

Self-Assessment Questionnaire (SAQ) The SAQ is a validation tool that must be completed by merchant account holders before an account will be set up and annually thereafter be able to demonstrate compliance with the PCI DSS. If there is a significant change to business process or system application then a new SAQ must be submitted.
Reconciliation

The department, owning of the merchant account, will receive a weekly/monthly statement of activity from the credit card processor. This statement must be reconciled to the settlement reports from your machine/software/web site and to monthly GL Oracle reports.

Compliance Issues

Faculty, staff, or students may report PCI compliance problems through standard management channels, beginning with the immediate supervisor. Alternatively, inquiries or reports may be addressed to the Ethics Point: [http://www.dartmouth.edu/~rmi](http://www.dartmouth.edu/~rmi)

Local Policies

Retention

PCI DSS recommends keeping to a minimum the credit card information that is retained. Local policy should make it a practice not to retain sensitive cardholder data. Limit your storage amount and retention time to that which is required for legal or regulatory purposes.

- **Electronic** - The College policy is no credit card data will be stored on laptops and/or PC’s. Computing Services must approve any systems or applications that process, store or transmit credit card data.
- **Paper** – Files with credit card information should be stored in a secure area on site for 18 months to 2 years and then placed in Records Management for the remainder of the retention period. The College recommends only keeping the information for 3 years. The files should be securely disposed directly from Records Management. Any paper containing credit card data must be shredded before disposal.

Chargeback

The payment processor will notify a merchant of a disputed charge. The merchant is responsible to provide the bank with written proof that the transaction was authorized by the customer.

If you are experiencing frequent charge back complaints or suspect fraud contact the Office of Risk and Internal Controls Services @ 6-3039.

Refunds

When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited only to the same account from which the purchase was made. In addition, under no circumstances is it permissible to issue cash refund.
Responsibilities

1) General Responsibilities for Processors:

You should NOT do the following:

1. Do not transmit cardholder’s credit card data by e-mail or fax
2. Do not store credit card data for repeat customers on paper in an unsecured area
3. Do not store PIN or CVV2/CVC2/CID number
4. Do not electronically store on the College computer file or server any unencrypted credit card data
5. Do not electronically store any credit card data on laptop or PC’s
6. Do not share user IDs for systems access
7. Never acquire or disclose any cardholder’s data without the cardholder’s consent

You should DO the following:

1. Store all physical documents containing credit card data in a locked drawer, locked file cabinet, or locked office
2. Maintain strict control over the internal and external distribution that contains credit card data
3. Change vendor supplied or default passwords
5. Properly dispose of any media containing credit card data
6. If you receive an unencrypted email from customer with credit card data notify the customer that they should no longer send this information via email and delete email immediately

Glossary:

More definitions can be found at PCI DSS site

Application    Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications
Backup         Duplicate copy of data made for archiving purposes or for protecting against damage or loss
Cardholder     Customer to whom a card is issued or individual authorized to use the card
Cardholder data Full magnetic stripe or the PAN plus any of the following: * Cardholder name
* Expiration date
* Service Code

Chargeback  A process that initiated by the cardholder who may contact credit card issuing bank regarding an inconsistency in the statement. Issuing bank will credit back to the cardholder then charge a fee to the merchant

Data Entry Processor  An individual who is responsible for credit card data entry for day-to-day operations

Encryption  Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure

Merchant  A unit that accepts credit cards as a method of payment for goods, services, information, or gifts

Merchant Account  An account established for a unit by a bank to credit sale amounts and debit processing fees

SAQ  Self-Assessment Questionnaire is a validation tool for merchants and service providers not required to undergo an on-site data security assessment per the PCI DSS Security assessment Procedures, and may be required by your acquirer or payment brand.

Sensitive Data  Sensitive Data include, the account number, magnetic stripe data, CVV2/CVC2 and expiration date.

Service Code  Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction
Exhibit 1

Dartmouth College

Payment Card Industry Data Security

Confidentiality / Non-Disclosure Statement - Processors

As a member of the staff of Dartmouth College, I acknowledge that in the course of my employment I may have access to personal, proprietary, transaction-specific, and/or otherwise confidential data concerning faculty, staff, students, alumni and/or other persons through the processing of credit card transactions.

As an individual with responsibilities for processing, storing and/or transmitting credit card data, I may have direct access to sensitive and confidential information in paper or electronic format. To protect the integrity and the security of the systems and processes as well as the personal and proprietary data of those to whom the College provides service, and to preserve and maximize the effectiveness of College’s resources, I agree to the following:

- I will maintain the confidentiality of my password and will not disclose it to anyone.
- I will utilize credit card data for College business purposes only.
- I will uphold Dartmouth College’s Code of Ethical Business Conduct, available at Ethics Point: http://www.dartmouth.edu/~rmi and I agree to abide by it.
- I have been provided a written copy of the College’s Merchant Credit Card Policy regarding the proper storing, protection, and disposal of such confidential data and I will ensure that any such data is shredded or otherwise disposed of as per approved office policy when no longer needed.
- I have read, understand, and agree to abide by Dartmouth College Merchant Credit Card Policy.

The use of sensitive credit card data for personal purposes is illegal and is grounds for termination. The abuse of systems access or unauthorized disclosure or distribution of any customer’s credit card data may result in prosecution.

Name (Print) ____________________________
Signature/Date__________________________________
Department_________________________________ Phone #___________________________________
Manager/Supervisor__________________________ Fiscal Officer _______________________________

January 2013