Dartmouth College Merchant Credit Card Policy for Managers and Supervisors

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 the 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 was to review all credit card merchant accounts, identify all the systems, applications and devices that process, store or transmit cardholder data. CPAC has identified and assisted in the implementation of any business or technological changes required to comply with PCI DSS.

Entities Affected By This Policy

Any College department that accepts credit card payments and retains sensitive cardholder data in paper or electronic format must comply with the Policy.

Who Should Read This Policy

Any departmental staff that conducts college business through credit card transactions. There are two versions of the Merchant Credit Card 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.

- **Merchant Credit Card Policy – for Supervisors and Managers (detailed version)**

Any supervisors or managers with the responsibilities of processing, storing or transmitting credit card data. This includes Executive or Fiscal Officers who oversees the department.
## 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

<table>
<thead>
<tr>
<th>Requirement 1</th>
<th>Install and maintain a firewall configuration to protect cardholder data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 2</td>
<td>Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
</tbody>
</table>

### Protect Cardholder Data

<table>
<thead>
<tr>
<th>Requirement 3</th>
<th>Protect stored cardholder data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 4</td>
<td>Encrypt transmission of cardholder data across open, public networks</td>
</tr>
</tbody>
</table>

### Maintain a Vulnerability Management Program

<table>
<thead>
<tr>
<th>Requirement 5</th>
<th>Use and regularly update anti-virus software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 6</td>
<td>Develop and maintain secure systems and applications</td>
</tr>
</tbody>
</table>

### Implement Strong Access Control Measures

<table>
<thead>
<tr>
<th>Requirement 7</th>
<th>Restrict access to cardholder data by business need-to-know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 8</td>
<td>Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td>Requirement 9</td>
<td>Restrict physical access to cardholder data</td>
</tr>
</tbody>
</table>

### Regularly Monitor and Test Networks

<table>
<thead>
<tr>
<th>Requirement 10</th>
<th>Track and monitor all access to network resources and cardholder data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 11</td>
<td>Regularly test security systems and processes</td>
</tr>
</tbody>
</table>

### Maintain an Information Security Policy

| Requirement 12 | Maintain a policy that addresses information security |

---
Compliance Certification Process

I Purchasing a system or application

Departments that require a system or application to process credit card data must contact Procurement (Strategic Sourcing) and Computing Services (IT Security Engineer) before initiating the purchase.

Procurement and Computing Services must approve any contract with a third party vendor which must be PCI compliant.

II Opening a Merchant Account

The departments interested in accepting payments for goods and services via a credit card must obtain a Merchant Account Request Form from Institutional Accounting and send it back for approval at least three weeks prior to accepting credit card transactions. Upon approval, Institutional Accounting will establish a new merchant account.

Merchants with Phone, Mail, Fax or Counter Sales Credit Card Processing

Departments using terminal (VeriFone) via phone line must meet following business requirements:

1. Cardholder and merchant receipts must print only last four digits of the credit card number. Expiration dates must be excluded
2. Any terminal that does not meet the above requirement must be reprogrammed or a new terminal must be purchased or leased by Department
3. Merchant Account Request Form has been submitted and approved by Institutional Accounting Office
4. Complete initial Self-Assessment Questionnaire (SAQ) according to instructions from the Institutional Accounting Office
5. Reconciliation between the Software or Payment Application and General Ledger is completed at least once a month
6. Background checks per HR policy may be required per PCI Requirement 12

Paper documents containing credit card data should be secured in a locked office and stored in a cabinet. In an open office environment paper documents should be stored in locked cabinets. Paper documents should not be left in an unsecured office after work hours. Please refer to Retention section for instructions.

Merchants with Internet Related Software, Point-of-Sale or Wireless Processing
Departments are not permitted to process, store or transmit credit card data on College’s computer systems or Internet without approval from Institutional Accounting, Computing Services and Dartmouth PCI Review Board. Any third party vendors must be PCI approved and compliant.

Merchants who use payment application systems (for example, point-of-sale) are connected to the Internet (via high speed connection, DSL, cable modem, etc), software applications installed on College computers or wireless device must meet the following requirements:

1. Passes architecture review by Computing Services (IT Security Engineer)
3. Complete initial Self-Assessment Questionnaire (SAQ) according to instructions from the Institutional Accounting Office
4. Contact Computing Services (IT Security Engineer) to set up a quarterly vulnerability scan
5. No access to 16 digit credit card numbers
6. Merchant Account Request Form has been submitted and approved by Institutional Accounting
7. Reconciliation between the software or Payment Application and General Ledger is completed at least once a month
8. Background checks per HR policy may be required per PCI Requirement 12

III Closing a Merchant Account

When a merchant account is no longer used, contact Institutional.Accounting@Dartmouth.edu and provide the merchant account number(s) that should be closed. Please contact Materials Management regarding the disposal of all college property and they will direct the disposal of the equipment.

IV Confidentiality Form

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

See Exhibit 1

V 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.
VI Changes to Merchant Accounts

Changes to an existing merchant account must be approved by Institutional Accounting and/or Computing Services. Examples of changes are: purchasing or discarding a terminal, purchasing software, selecting a new service provider, etc. A new SAQ must be completed whenever there is a major change to system, application or process involving credit card information.

VII Checklist for Merchant Account Owners

See Exhibit 2

Reconciliation

The department, owning 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 as well as to your account in the College’s General Ledger using the applicable and appropriate 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

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 of directly from Records Management. Any paper containing credit card data must be shredded before disposal.
Changes

Before making any changes to your technical architecture or business practices regarding credit cards you should insure that you remain in compliance with PCI data security requirements. You should contact Computing Services (IT Security Engineer) to conduct a Quality Scan Assessment prior to placing any systems or application changes into production.

Chargeback

The bank 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 chargeback complaints or suspect fraud contact the Office of Risk and Internal Controls Services at 646-3039.

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 credit card account from which the purchase was made. In addition, under no circumstances is it permissible to issue cash refund.
**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 credit 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**
Process when the cardholder contacts the credit card company or the issuing bank regarding an inconsistency in their credit card statement. The issuing bank will credit back to the cardholder for the disputed transaction 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 that are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures, which may be required by your acquirer (bank) 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

**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’s computer file or server any unencrypted credit card data
5. Do not electronically store any credit card data on laptop or PCs
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.

2) **General Responsibilities for Executive Officers, Fiscal Officers, Management Officers and Systems Managers:**

1. Comply with Payment Card Industry Data Security Standard (PCI DSS)
2. Obtain approval by Institutional Accounting, Procurement Services and Computing Services prior to entering into any contract, purchase, acquisitions, or replacement equipment, software, Internet provider, or wireless device
3. Submit for approval any new merchant accounts to Institutional Accounting
4. Establish procedures to restrict physical access to data or systems that house cardholder data
5. Communicate the Dartmouth College Merchant Credit Card Policy to all employees
6. Restrict access to credit card data by business need-to-know basis
7. Establish appropriate segregation of duties between personnel handling credit card processing, refunds and reconciliations

8. Perform background checks on employees who have access to systems, networks and multiple credit card information. This does not include personnel who have access to one card number at a time
9. Assign a unique ID to each person with computer access to credit card data
10. Do not allow credit card data to be sent by email or fax
11. Do not allow the storage of PIN or CVV2/CVC2/CID numbers
12. Do not allow electronic storage of any credit card data on the College’s computer files or servers except for systems and applications that have been approved by Computing Services
13. Do not allow electronic storage of any credit card data on laptop or PCs
14. Do not allow outside consultants to store credit card data on their own PC equipment
15. Do not allow employees to share user IDs for systems access
16. Do not allow the use of imprint machines to process credit card payments except in an emergency situation (e.g. power outage)
17. Never allow the disclosure of cardholder’s data without the cardholder’s consent
Exhibit 1

Dartmouth College

Payment Card Industry Data Security

Confidentiality / Non-Disclosure Statement - Managers and Supervisors

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_____________________________

January 2015

Page 10 of 13
### Exhibit 2

**Payment Card Industry Data Security Standard (PCI DSS) – Checklist for Merchant Account Owner**

**Department ___________________________ Merchant Account Owner ___________________________**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Contacts</th>
<th>Completion Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Get an approval from Procurement and Computing Services before purchase or lease a system or application to process credit card transactions.</td>
<td>Procurement - Strategic Sourcing Computing Services – IT Security Engineer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Complete PCI Online Training via Canvas</td>
<td>Institutional Accounting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Complete a Self-Assessment Questionnaire (SAQ)</td>
<td></td>
<td></td>
<td>The SAQ must be completed before a Merchant Account will be set up.</td>
</tr>
<tr>
<td>4</td>
<td>Open a Merchant Account</td>
<td>Institutional Accounting</td>
<td></td>
<td>It takes 3 weeks to process a merchant account request.</td>
</tr>
<tr>
<td>5</td>
<td>Background Checks for new and transfer employees per HR policy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Have all staff and students who process, store and transmit credit card data sign the Confidentiality Statement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Changes to the existing Merchant Account must be communicated to the Institutional Accounting Computing SERV</td>
<td></td>
<td></td>
<td>Changes to a system such as an upgrade, new terminal or selecting a new service provider.</td>
</tr>
</tbody>
</table>
|   | Close a Merchant Account | Institutional Accounting  
Material’s MGT  
Computing SERV | For purchased terminal disposal please contact Material MGT |