Merchant Services and PCI Compliance Policy
http://www.dartmouth.edu/~control/policies/

Policy Owner: Controller’s Office
Administering Departments serving on the Merchant Services Committee: Controller’s Office, Information Security, Institutional Accounting, Risk Management, and Treasury
Last Revision: June 6, 2018
Policy Sections:
1. Overview
2. Dartmouth College Merchant Services Policy
3. Dartmouth College Procedures
4. Payment Card Industry Data Security Standard (PCI DSS)
5. Dartmouth College PCI DSS Confidentiality / Non-Disclosure Statement

1. Overview

Dartmouth College Merchant Services Mission

Dartmouth College has established a Charter to monitor regulatory statutes and contractual obligations specific to the Payment Card Industry Data Security Standard, (PCI DSS), merchant services, and electronic commerce (e-Commerce). The purpose of the Dartmouth College Merchant Services Policy is to maximize security of our customers’ card data, Dartmouth’s reputation, and avoid any financial costs associated with a breach of card information as well as outline Best Practices in all aspects surrounding handling of cardholder data.

Dartmouth Compliance and Ethics Hotline

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

Risk and Internal Controls Services provides independent risk-based audit, consulting, and operational services to protect and enhance organizational value in support of the mission of Dartmouth College.

Entities Affected By This Policy – Who Should Read This Policy?

Anyone that conducts Dartmouth College business and is affiliated with the acceptance of payment cards as a form of payment.
2. Dartmouth College Merchant Services Policy

Dartmouth College signed into a contractual agreement with Chase Paymentech as their primary credit card processor. By doing so, Dartmouth has an obligation to this Merchant Service Provider, therefore, individuals seeking any other alternative resources for payment card acceptance and processing is not permissible under our contractual agreement with Chase.

Any department that chooses to accept payment cards as a form of payment, must first seek the approval from the Controller’s Office. The Controller’s Office will review all Merchant Account Requests for acceptance of cards and will make determination of approval based on provided information from the Merchant Account Request Form.

PCI Training is mandated for any individual that is conducting Dartmouth College business and is affiliated in any aspect of processing credit cards. This includes but not limited to, acceptance of credit/debit/stored value cards, reconciliation of card revenue and expense, and the use of reporting tools reflecting credit card data.

For on-line credit card acceptance, Dartmouth College has approved the following PCI compliant Payment Application Gateways; JPMorgan Chase, Authorize.Net, and PayPal. If you choose any other option other than what is listed above, you must have the approval from the Controller’s Office.

For terminal credit card acceptance, Dartmouth College has approved the following equipment; Verifones VX520, VX680, MagTek eDynamo, EMV Mobile Reader (Chase Mobile Checkout), Ingenoco, Micros 9700 and iTerminal IPP320x3.

Members of the staff at Dartmouth College that have any association with the acceptance of payment cards must sign the PCI DSS Confidentiality/Non-Disclosure Statement. Signed statements should remain with the office in which the individual is conducting Dartmouth business. The PCI DSS Confidentiality/Non-Disclosure Statement is located on Page 10.

A Self-Assessment Questionnaire (SAQ) is a validation tool that must be completed by each merchant account holder before a merchant account will be set up, and annually thereafter in order to demonstrate compliance with the PCI DSS. If you have an existing merchant account, and your business operations will be changing significantly, you would need to complete a new SAQ. Every business area needs to reflect an accurate SAQ on file with the Controller’s Office at all times.
Department members serving on the Merchant Services Committee may conduct an internal audit of a merchant holder’s business operation, to ensure compliance and regulatory policies and procedures are in accordance with policies. Any business operation found not in compliance, risk losing their privilege for acceptance of credit card payments.

**Merchant Account Holder’s Responsibilities**

**You should NOT do the following:**

1. Do not transmit cardholder’s credit card data by e-mail, fax or other electronic means
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 or the full credit card number
4. Do not electronically store any credit card data on any computer files, servers, laptops, PCs, mobile phones, tablets or any other electronic devices
5. Do not share user IDs and/or passwords for systems access
6. 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 without the full credit card number
2. Maintain strict control over the internal and external distribution that contains credit card data
3. Change vendor supplied or default passwords
4. Ensure that your department, computer systems and operations are in full compliance with the Dartmouth Information Security Committee (DISC) policy: [https://tech.dartmouth.edu/itc/services-support/help-yourself/knowledge-base/dartmouth-information-security-policy](https://tech.dartmouth.edu/itc/services-support/help-yourself/knowledge-base/dartmouth-information-security-policy)
5. Properly dispose of any media containing credit card data
6. If you receive an unencrypted email from a customer with credit card data notify the customer that they should no longer send this information via email and delete email immediately

**Responsibilities for Executive Officers, Fiscal Officers, and Management Officers**

1. Comply with Payment Card Industry Data Security Standard (PCI DSS) and Dartmouth Information Security Committee (DISC)
2. Obtain approval by Procurement Services prior to entering into any contract, purchase, or acquisition for software or system applications
3. Obtain approval from the Controller’s Office for new or replacement of equipment, wireless devices and Internet Gateway Providers
4. Establish procedures to restrict physical access to data or systems that house cardholder data
5. Communicate the Dartmouth College Merchant Services 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. Assign a unique ID and password to each person with computer access to credit card data
9. Do not allow credit card data to be sent by email, fax or other electronic means
10. Do not allow the storage of PIN or CVV2/CVC2/CID numbers on Laptops, PCs, mobile phones, tablets or other electronic devices
11. Do not allow outside consultants to store credit card data on their own PC equipment
12. Do not allow employees to share user IDs for systems access
13. Never allow the disclosure of cardholder’s data without the cardholder’s consent

3. Dartmouth College Procedures

**Dartmouth College Merchant Services Procedures**

The steps outlined below must be followed for a merchant account to be considered for credit card acceptance.

**1. Requesting a Merchant Account Request Form**

**Note** If your intentions for credit card acceptance is for both on-line and terminal acceptance, you will need to complete a separate Merchant Account Request Form for each processing type.

Departments interested in accepting payments for goods and services via a credit card must first obtain a Merchant Account Request Form located at the URL provided below [http://www.dartmouth.edu/~control/docs/accounting/dc_merchant_account_request_form.doc](http://www.dartmouth.edu/~control/docs/accounting/dc_merchant_account_request_form.doc) or by sending an e-mail request to Institutional.Accounting@Dartmouth.EDU.

This form must be completed thoroughly and accurately for determination in the approval process. Once the form has been completed, a scanned copy should be sent to
Institutional.Accounting@Dartmouth.EDU or mailed to Institutional Accounting, Hinman 6015. The requestor will be notified of the status of their request after the review process. Please allow 3-5 business days for the approval application process.

2. **Self-Assessment Questionnaire (SAQ)**
The SAQ is a validation tool that must be completed by each merchant account holder before a merchant account will be set up, and annually thereafter in order to demonstrate compliance with the PCI DSS. If you have an existing merchant account, and your business operations will be changing significantly, you would need to complete a new SAQ. Every business area needs to reflect an accurate SAQ on file with the Controller’s Office at all times.

The merchant account holder or supervisor/manager that is requesting the establishment of a new merchant account, will also need to complete an initial Self-Assessment Questionnaire (SAQ) based on the scope of their business operation. The appropriate SAQ for your business type will be sent to the requestor for completion upon receipt of the Merchant Account Request Form, and will be assisted in the completion and the submission of the SAQ.

3. **Purchasing new systems or software applications**
This policy pertains to existing merchant accounts where the business operation will be changing significantly, and for any new merchant account that may require a new system or software application for processing credit card data. You **must** submit vendor contracts to Procurement Services for their review/approval. Where applicable, some contracts may also require further review/approval from the offices of Risk and Internal Controls, and Information Security around compliance and security concerns. Once the contract has been approved, a signed copy of the document should be scanned to Institutional.Accounting@Dartmouth.Edu.

4. **Approved Merchant Account Request**
Once the merchant account request form has been approved, Institutional Accounting will complete a merchant account application with Chase Paymetech and one for American Express where applicable. Please allow 10 business days for this process to be completed. Once the merchant account(s) have been assigned by the banks, you will be notified by Institutional Accounting.

All individuals listed on the Merchant Account Request form that require Payment Card Industry (PCI) training, will be set up by Institutional Accounting and notified by e-mail of their training. If those individuals do not take the required training, they should not handle credit card functions. One reminder will be sent to the individual after the initial e-mail notification has been sent. If training hasn’t occurred within ten business days of the final reminder, the
recommendation would be suspension of tasks affiliated with any credit card functions until further compliant.

5. Reconciliation of Merchant Accounts

Reconciliation – It is highly recommended that a reconciliation between the Software and/or Payment Application Gateway and Dartmouth’s General Ledger be completed at least once a month for credit card settlement accountability. Any discrepancies should be followed up in a reasonable timeframe.

Chargeback - The bank will notify a merchant holder of a disputed charge. The merchant holder is responsible to provide the bank with proof that the transaction was authorized by the customer. Case information is available for two years and document information is available for six months from the last case status change date. If you need assistance with the chargeback process, the Chase Paymentech Chargeback Management Guide is available, please contact Institutional.Accounting@Dartmouth.Edu.

Refund - 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 originally made. In addition, under no circumstances is it permissible to issue a cash refund.

Online Reporting - If you encounter any reporting issues or need assistance with the Chase Paymentech Resource Online module, please contact Institutional.Accounting@Dartmouth.Edu for assistance.

6. Closing a Merchant Account

When a merchant account is no longer needed, the merchant holder will need to contact Institutional.Accounting@Dartmouth.Edu and provide the merchant account(s) that need to be closed. Prior to requesting a closure, you should always allow ample time for any refunds, chargebacks or fees that may need to process against the merchant account. If you were using a payment gateway provider, and/or software application it’s the responsibility of the merchant account holder to cancel the account that was established for use with the merchant account(s). This should occur when the merchant account has been requested to be closed, otherwise, you may potentially be subject to monthly fees.
7. Return of credit card equipment
It is the responsibility of the merchant account holder to ensure that all leased or rented equipment from Chase Paymentech, or any other provider, be returned when the merchant account has been requested to be closed. If the equipment is owned by Chase Paymentech, contact Institutional.Accounting@Dartmouth.Edu and you will be provided with a contact in working out the return details. If the equipment is Dartmouth College property and requires disposal, please contact Materials.Management@Dartmouth.EDU for assistance with this removal.

8. Retention Period of credit card information
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/Paper - Dartmouth’s policy is no credit card data should be stored on laptops, I-pads PC’s or any other technical device. 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 and not be left in an unsecured office at any time. Dartmouth’s policy is keeping transactional reconciliations for seven years, whether stored electronically or on paper for internal/external audit purposes. You should never store a card holder’s entire account number. In the event the card holder’s number needs to be written down for keying in later, the document needs to be shredded immediately afterwards.

4. Payment Card Industry Data Security Standard

<table>
<thead>
<tr>
<th>Payment Card Industry Data Security Standard (PCI DSS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Official PCI DSS URL - <a href="http://www.pcisecuritystandards.org">http://www.pcisecuritystandards.org</a></td>
</tr>
<tr>
<td>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 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 and are summarized below.</td>
</tr>
</tbody>
</table>
**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 for all personnel

---

**PCI DSS Glossary – most commonly used**

<table>
<thead>
<tr>
<th>Application</th>
<th>Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>Duplicate copy of data made for archiving purposes or for protecting against damage or loss</td>
</tr>
<tr>
<td><strong>Cardholder</strong></td>
<td>Customer to whom a credit is issued or individual authorized to use the card</td>
</tr>
</tbody>
</table>
| **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 |
5. Dartmouth College PCI DSS Confidentiality / Non-Disclosure Statement

Dartmouth College
Payment Card Industry Data Security Standard
Confidentiality / Non-Disclosure Statement

**NOTE** All completed forms remain on file with member’s manager

As a member of the Dartmouth College Community, 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 Dartmouth provides service, and to preserve and maximize the effectiveness of Dartmouth 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 Dartmouth College business purposes only.
- I will uphold Dartmouth College’s Code of Ethical Business Conduct, available at Ethics Point: [http://www.dartmouth.edu/~rmi](http://www.dartmouth.edu/~rmi) and I agree to abide by it.
- I have been provided access to Dartmouth College’s Merchant Services 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 Services 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 # _________________________________