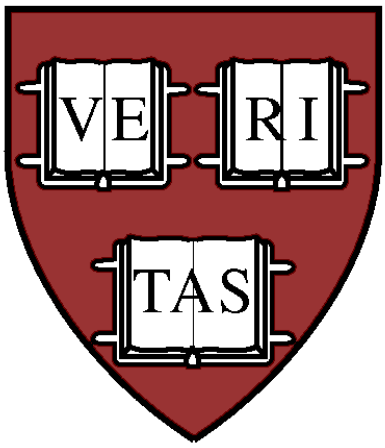


Harvard University

Credit Card Merchant Handbook

Revised May 2015

TABLE OF CONTENTS

Credit Card Merchant Handbook

Customers are required to contact Cash Management to obtain any of the following:

- Merchant account with Bank of America Merchant Services (BAMS)
- Login to ClientLine (BAMS Online Reporting System)
- Login to TrustKeeper
- CyberSource gateway account.

Check Cash Management's website at http://otm.finance.harvard.edu/ for current contact telephone numbers and email addresses.

Credit card processing is a complex process that requires careful attention to ensure that local processes are compliant with Harvard policy and Payment Card Industry (PCI) standards. Each credit card transaction involves many different third parties (See Appendix I). Please note that all acronyms and abbreviations used in this document are defined in the glossary. References to the Payment Card Industry Data Security Standard (PCI DSS) refer to version 3.1 of the standard. The Handbook will be updated as new versions are released.

Merchants must review the Payment Card Industry (PCI) standards and the Harvard Policies and understand the commitment of resources they require before requesting a credit card Merchant account.

PCI Executive Committee and Working Group

A PCI Working Group has been formed to oversee the PCI Compliance program of Harvard University. This committee has representatives from Office of Treasury Management and Harvard University Information Technology Security. There are three executive sponsors for the working group which comprise the PCI Executive Committee:

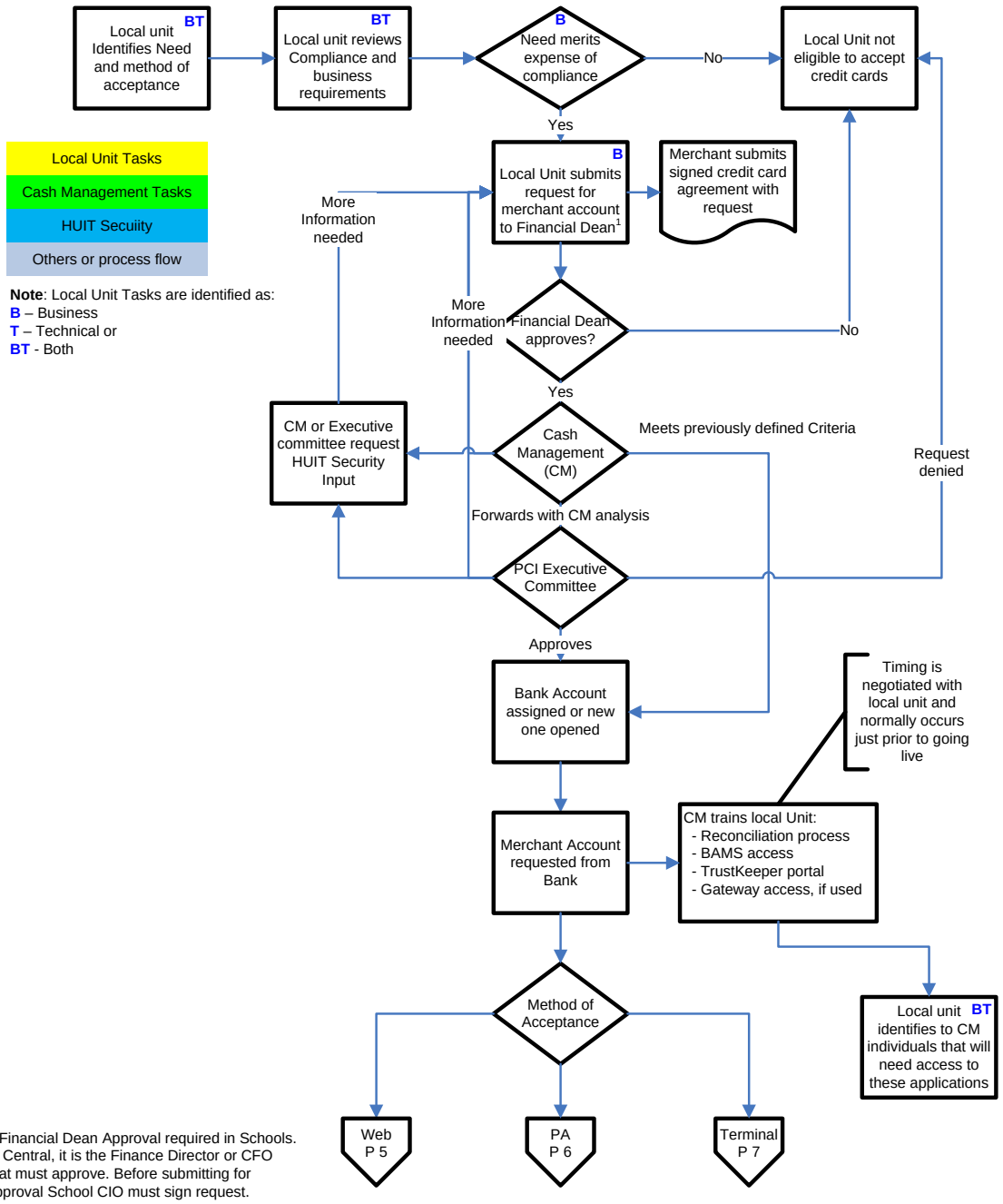
- Director of Treasury Management
- Director of Risk Management and Audit Services
- Vice President, University Chief Information Officer.

The Executive Committee is responsible for setting policy and providing high level direction to the PCI Compliance program. The Working Group provides assistance to the Office of Treasury Management in the development of standardized processes and procedures and makes recommendations to the PCI Executive committee regarding policy and approval of new merchants.

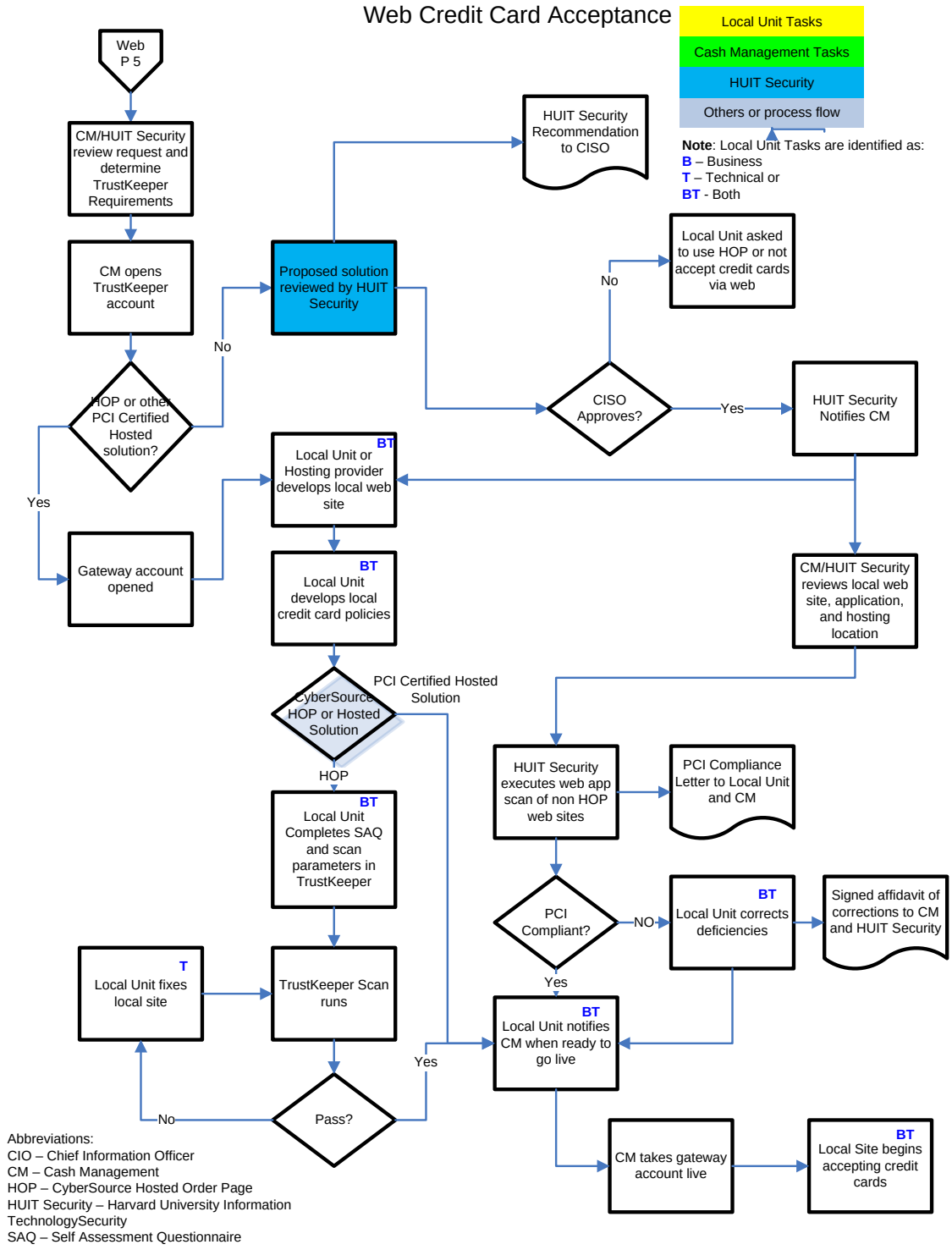
New Merchant Requests

The diagram on the following pages provides an overview of the request process.

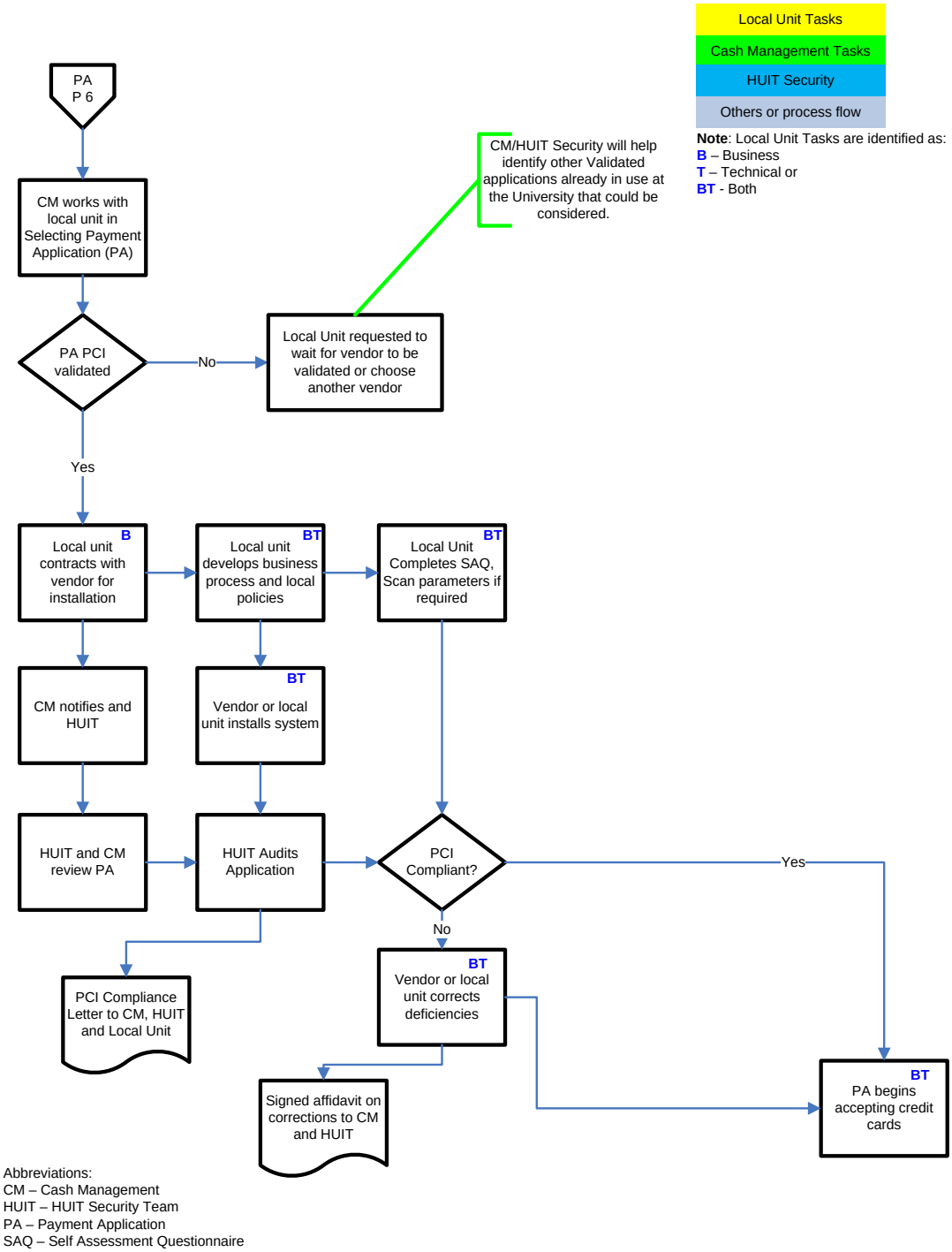
Requesting Credit Card Merchant Account



1 Financial Dean Approval required in Schools. In Central, it is the Finance Director or CFO that must approve. Before submitting for approval School CIO must sign request.

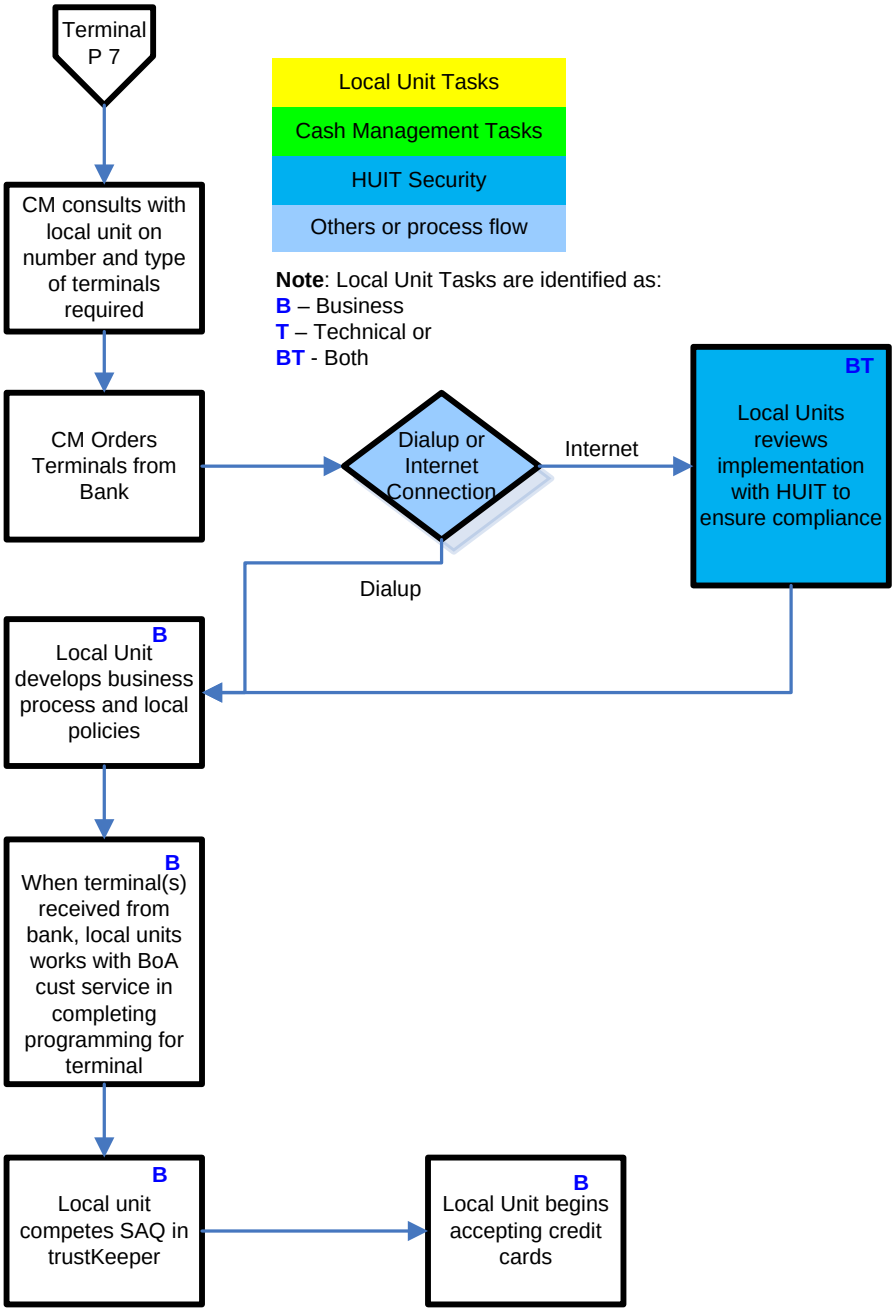

Web Credit Card Acceptance
Local Unit Tasks
Cash Management Tasks
HUIT Security
Others or process flow
Note: Local Unit Tasks are identified as:
B – Business
T – Technical or
BT - Both
Web P 5
CM/HUIT Security review request and determine TrustKeeper Requirements
CM opens TrustKeeper account
HOP or other PCI Certified Hosted solution?
No
Yes
Gateway account opened
Proposed solution reviewed by HUIT Security
HUIT Security Recommendation to CISO
No
Local Unit asked to use HOP or not accept credit cards via web
CISO Approves?
Yes
HUIT Security Notifies CM
BT
Local Unit or Hosting provider develops local web site
BT
Local Unit develops local credit card policies
CM/HUIT Security reviews local web site, application, and hosting location
CyberSource HOP or Hosted Solution
PCI Certified Hosted Solution
HOP
BT
Local Unit Completes SAQ and scan parameters in TrustKeeper
HUIT Security executes web app scan of non HOP web sites
PCI Compliance Letter to Local Unit and CM
PCI Compliant?
NO
BT
Local Unit corrects deficiencies
Signed affidavit of corrections to CM and HUIT Security
Yes
T
Local Unit fixes local site
TrustKeeper Scan runs
BT
Local Unit notifies CM when ready to go live
Yes
Pass?
No
CM takes gateway account live
BT
Local Site begins accepting credit cards
Abbreviations:
CIO – Chief Information Officer
CM – Cash Management
HOP – CyberSource Hosted Order Page
HUIT Security – Harvard University Information TechnologySecurity
SAQ – Self Assessment Questionnaire

Payment Application Credit Card Acceptance



Abbreviations:
CM – Cash Management
HUIT – HUIT Security Team
PA – Payment Application
SAQ – Self Assessment Questionnaire

Terminal Credit Card Acceptance



Abbreviations:
CM – Cash Management
HUIT – HUIT Security Team
RMAS – Risk Management & Audit Services
SAQ – Self Assessment Questionnaire

Before you request a merchant account

Because of Credit Card association rules for security and the risks associated with accepting credit cards, requesting a new credit card merchant account should not be requested without a full understanding of the responsibilities and alternatives.

- Contact Financial Dean or Financial Director for approval
- Determine if the anticipated annual credit card sales volume will approximate $100,000
- Review information in handbook and Self-Assessment questionnaire to evaluate whether the business need warrants the effort and cost required to obtain and maintain a credit card merchant account.
- Review alternatives to a merchant account, such as the online registration vendor for conferences and events
  (See http://www.events.harvard.edu/profile/web/index.cfm?PKwebID=0x2862d09&varPage=home.Discuss objectives with Cash Management to determine if other alternatives might be superior.

Requesting a Credit Card Merchant Account

Merchant accounts must be requested by your Financial Dean for local units or by your Financial Director for Central Administration Departments. A template for making the request is included in Appendix C and is available on Cash Management's website Merchant Account Request Form. The following data is required:

- Purpose for requesting credit card account
- Estimated annual activity volume, both numbers of transactions and total dollar value.
- A business case for why you need to accept credit cards. Please include who your customers are and the impact to your organization if you can't accept credit cards. Also describe any challenges you have with your current method of accepting payments.
- The target date for setup
- The name of the new account
- The Tub and Org where credit card transactions should be posted in the general ledger
- Clientele, who will be the customers
- What type of credit cards you wish to process (e.g. MC/Visa, Amex, and Discover)
- How will credit cards be accepted (Card Present, over the phone, via fax or via web) Please indicate all methods of acceptance
- If web based,
  - What software will be used to accept the credit cards
  - Locally developed applications will use CyberSource Secure Acceptance Secure Acceptances (HOP)
  - If purchasing off the shelf software that cannot use HOP, an exception must be approved by University CIO. (see Appendix A)
  - If using a hosted solution by a service provider, please see section on service providers below. **Use of service providers must receive prior approval from Cash Management.**
- If terminals will be used,
  - Type and quantity of terminals, printers and pin-pads
  - Whether you wish to purchase, lease or rent
  - Whether authorizations will be done via dial-up or Internet
  - Address of where the equipment will be shipped
- If a Point of Sale (POS) application will be used,
  - Name of POS application
  - Name and version of POS Software to be used

- Where the POS application will be hosted
- Whether wireless technology will be used

A POS application must not be purchased unless it has been approved by Cash Management.

- Contact Information (name, address, phone and email) for:
  1. Business owner
  2. Primary Business contact (may be same as business owner)
  3. Backup Business Contact
  4. Technical Contact (Required for all merchants except dial-up terminals only)
  5. Person responsible for posting the credit card activities and resolving reconciliation issues

Merchant Account Agreement

Merchants must sign a Harvard Merchant Credit Card Agreement as part of requesting a credit card merchant account. A copy of the most recent agreement can be found on the Cash Management's web site. A copy is included in Appendix D. This agreement is to be renewed annually.

New Account Setup Responsibilities for Merchants

Depending on the complexity, the set up process can take 3 - 6 weeks. This time may be required because of the number of 3rd parties involved in the process, particularly for web based merchants, which Cash Management cannot completely control. Request should be made early enough to allow for sufficient time (at least one month, more if possible). Once you receive the merchant account number you will be responsible to do the following:

- Log onto the TrustKeeper portal and complete the registration process within 3 business days of receiving TrustKeeper account information via email. Identify, notify and share information with all contacts that will need access to the portal (e.g. business owner and technical contact).
- Complete the on-line self assessment questionnaire (SAQ) for certification. If applicable, identify systems that need to be included in monthly scans and successfully pass the first scan before going live. Follow the instructions for scanning merchants: Trustkeeper Guide for Scanning Merchants
- Create business practices (see Appendix E) for the security and integrity of credit card transactions. They include but are not limited to: reconciliations, data access, retention, charge backs, background checks and physical security.
- Provide Cash Management a list of all individuals needing access to ClientLine and CyberSource. Please note that individuals in positions that require access to these accounts are required by PCI data security standard to have background checks performed. Therefore individuals should not be added casually, however all individuals must be identified because PCI also requires that accounts not be shared.
- Cash Management will provide training during the setup process on use of ClientLine and CyberSource access as well as reconciliation and PCI compliance. The Merchant must ensure that everyone requiring this training is present. If additional individuals require training later it is the merchant's responsibility to provide the training to these individuals.

Terminals

- Terminals are shipped directly to the address specified in the merchant account request.
- Terminals come with set-up instructions and a customer service number to call if there are questions.
- Merchants must follow the set-up instructions that come with the terminals to properly link them to their merchant account.

If the credit card terminals will be used to process authorizations and/or settlements via the internet instead of via dial up phone lines, they complete a different SAQ and will require CM's and HUIT's approval before going live.

Point of Sale (POS) Systems

Cash Management (CM) must approve the use of a POS application before purchase. Cash Management's approval will follow a review by HUIT IT Security of the proposed implementation. If the POS application's workstations will be used for standard office applications (email, web browsing, etc.) as well, these workstations must comply with the rules outlined in Appendix F. Please note that all workstations attached to a POS system, whether they process credit cards or not, are in scope for PCI and must meet applicable PCI requirements. Workstations that are not used for processing credit cards would meet PCI requirements if they conform to Harvard's Enterprise Security Policy.

CM will verify that the POS application is validated to be compliant with Payment Application Data Security Standard (PA DSS). Non-validated applications cannot be used. See https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html.

CM will engage HUIT IT Security to review the implementation of the system to be sure that it meets all University security requirements

Local Unit will need to supply CM with information regarding the manufacturer, product name and version number of the software as well a full implementation network diagram. (See section on "Requesting a Credit Card Merchant Account" for complete information needed)

Service Providers

A service provider is any third party that stores, transmits or processes credit card numbers on behalf of a merchant. If you plan on using a service provider you must have approval from Cash Management before you sign a contract with them. A list of certified compliant service providers is maintained by both MasterCard and Visa. See:
http://www.mastercard.com/us/company/en/docs/SP_Post_List_2012.pdf
http://www.visa.com/splisting/

Service providers must be contractually obligated to keep their systems and process in compliance with PCI requirements at all times. For current language of the credit card contract rider please go to Harvard's Security Site. See: http://www.security.harvard.edu/protected_files/cc_rider.php

Internet Gateways

Internet gateways are service providers that connect the internet to the proprietary payment card processing network of banks and processors. Web based merchants will need to use a gateway to accomplish on-line authorization and/or settlement of credit card purchases. Some POS applications and credit card terminals also require a gateway because they use the Internet instead of a dial-up connection for authorization and settlement.

For our preferred gateway, CyberSource, Cash Management (CM) will open the gateway account; CM will provide you with unique user names for everyone in your organization that needs access for reporting. Local unit must notify CM when authorized users leave your organization or no longer require access. Notifications should be sent to Cash_Management@harvard.edu.

For other gateways that may be required for your POS system, Cash Management and HUIT IT Security must approve the gateway and your implementation. Contracts for gateways other than CyberSource

must be reviewed by Cash Management and the Office of the General Counsel. Cash Management will contact the bank to obtain any processor information required by the gateway.

Virtual Terminals

Internet gateways provide ways for you to enter transactions directly through your web browser. This feature allows you to process manual transactions without having a physical credit card terminal. This would also apply if you are using a Certified PCI Compliant Service Provider whose solution includes a web interface where you can enter transactions. If you have workstations that are dedicated to one of these purposes, they must meet all the requirements in SAQ C-VT. If you use one of these features and the workstations are also used for other purposes, those workstations must meet all applicable requirements in the PCI Data Security Standard as outlined in SAQ D. Some Guidance is provided in Appendix F about which requirements are likely to be applicable, but the merchant is responsible for ensuring that their implementation is compliant.

Software & Website Hosting

New merchants accepting credit cards over the Internet must use CyberSource's Secure Acceptance Secure AcceptanceSecure Accesptance Secure Acceptance previously called (HOP) or another approved PCI Compliant external service provider. Cash Management can provide additional information on how to set this up. Exemptions to this requirement are outlined in Appendix A.

If the merchant changes their application and is not using SECURE ACCEPTANCE, then the merchant needs to follow the exemption process outlined in Appendix A. Changes do not include upgrading to a new release of software already exempted.

Websites, whether internal or externally hosted, that store, transmit or process credit card account numbers must comply with PCI Data Security Standards and Harvard University requirements. Websites that control any aspect of the payment page must be hosted by a Level 1 PCI Compliant service provider. (See Appendix B) Our acquiring bank, Bank of America Merchant Services, additionally requires that we provide the URL of the site to them in advance of going live. They will verify that the site uses encryption (i.e., SSL) to protect the credit card number and that a refund policy is clearly posted on the web-site. They will not issue the required processor information used to connect to a gateway until this accomplished.

Merchants that have these sites must work with Cash Management and HUIT IT Security to have a network penetration tests conducted at least annually. Please note that if you are using SECURE ACCEPTANCE you do not require a network penetration test. (See Section on Penetration Tests)

Web sites, whether internal or externally hosted, that accept or store credit card account numbers must have their hosting location evaluated by HUIT IT Security before being placed in production. (See Appendix B) For a list of hosting locations at Harvard that have already been qualified please email cash_management@harvard.edu. Web sites involved in order processing that redirect to another site to accept credit cards must meet PCI and Harvard requirements. (Also Appendix B)

Fraud Services

Merchants that accept web transactions must use Address Verification (AVS) and Card Number Verification (CVV/CVC) fraud prevention services. More details on AVS are available in Appendix H.

Compliance:

The credit card associations (MasterCard, Visa, American Express, Discover and JCB) have created a Payment Card Industry Data Security Standard (PCI DSS) with which all merchants must comply. In addition they have created and jointly share the governance of the PCI Security Standards Council. The PCI Security Standards Council (PCI SSC) is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), Pin Transaction Security(PCI-PTS) Requirements, and Point-to-point Encryption (PCI-P2PE).

All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PCI SSC as being qualified to validate compliance to the PCI DSS, PA-DSS, and PCI-P2PE. Devices that need to conform with PCI-PTS are evaluated by a SSC recognized Laboratory and approved by the PCI SSC.

Compliance with PCI data security standards is mandated for all merchants and any service provider that "transmits, stores, or processes" cardholder information. Each merchant must be certified annually to be in compliance with PCI data security standards in order to accept credit cards and will receive a compliance certificate once they have completed and passed the following requirements:

- The completion of an annual self assessment questionnaire.
- Quarterly network vulnerability scans performed remotely by an approved scanning vendor.

For more information on the PCI standards and these requirements please see:
https://www.pcisecuritystandards.org/.

Merchants may also email pci compliance@harvard.edu with questions or concerns about the compliance of their implementation or the Harvard PCI compliance program

Harvard has contracted Trustwave to provide annual compliance certification and monthly vulnerability scans. Trustwave is an approved vendor of the PCI Security Council. Trustwave provides the TrustKeeper portal for merchants to achieve their compliance certification. Cash Management will set up all new merchants with a login to the TrustKeeper portal to complete the questionnaire and schedule a remote scan of their URL or IP address(es).

- Merchants are required to complete the self assessment questionnaire online in the TrustKeeper account provided by Cash Management.
- Merchants that accept or process credit cards online must also enter scan parameters (IP addresses or URLs for systems that fall in scope for PCI.
  - Merchants using SECURE ACCEPTANCE must have the web server that performs the redirect to the SECURE ACCEPTANCE site be scanned. Follow these instructions for scanning websites: Trustkeeper Guide for Scanning
  - Merchants that accept cards some other way must scan all outward facing IP addresses on the same subnet as the system(s) that stores processes or transmits credit card numbers.

New merchants must achieve certification before they can begin accepting credit cards. All merchants must maintain their compliance by fulfilling the annual and monthly requirements. Cash Management will deactivate any merchant account at BAMS if the local unit does not reach or maintain PCI certification. Any merchant who fails a monthly scan, PCI Audit or network penetration test will have 30 days to correct all high vulnerabilities identified. If not corrected in 30 day's Cash Management will deactivate the

merchant. Cash Management will notify the Financial Dean, RMAS and the PCI Committee of any failures and actions taken.

Merchant Responsibility for TrustKeeper Portal

Merchant must complete the TrustKeeper registration process within 3 business days of receiving a welcome email from TrustKeeper.

After completing the registration process and creating their login-ID, merchants can log into the portal at https://login.trustwave.com/portal-core/home

.

If applicable, enter IP addresses to be scanned. IP addresses to be scanned should be a Harvard address. If your web-site is hosted by a third party you should contractually obligate them to be compliant with PCI requirements and to have their systems scanned by an authorized assessor on a quarterly basis and those scan results should be made available if requested

Merchant must complete a self-assessment questionnaire.

If technical contacts will be required, ensure they have their own login ID to the portal account as well.

For help using the portal, see the online help, email support@trustkeeper.net or call 800-363-1621.

Merchant Responsibilities for Monthly Scans

Merchants will receive an email notification from Trustwave several days before the monthly scan is scheduled to run. This email should be forwarded to the local unit's IT staff to notify them that the scan will run within two business days. Trustwave will send a second email after the scan has run. The merchant must log into the TrustKeeper portal within 2 business days to review the results.

Reviewing the results of monthly scan reports:

- If the scan indicates that the Merchant has already been breached, immediately contact Cash Management to activate a PIRT in accordance with the PCI Security Breach Procedures. **Note: system must immediately be disconnected from the network.**
- If the scan indicates any PCI failure, vulnerabilities they must be immediately corrected. Consult with HUIT IT Securityon whether you have sufficient compensating controls to continue accepting credit cards while you correct the problem. If it is determined by HUIT IT Securitythat you don't have sufficient controls, you will be instructed to take system immediately off the Internet until fixed. If not corrected within 30 days Cash Management will deactivate the account.
- Merchant must review all medium and low findings. Merchant must confirm that these do not represent a risk to the system or schedules routine maintenance to address these issues. It is not uncommon for lower risk issues to rise to a higher risk as hackers discover further ways to exploit them. Therefore merchant must work remediation of medium and low vulnerabilities into their ongoing maintenance plans so that they can be fixed before they become high risks. Medium and low vulnerabilities must be corrected before the next quarterly scan.
- Merchant must evaluate all information warnings in the report to ensure their system is not at risk.

If the merchant believes any vulnerabilities identified are in error, the merchant may appeal the finding by logging into the TrustKeeper portal and in the reports section of the portal follow the appeal process. The merchant may also call the TrustKeeper Help Desk at 800.363.1621 for help in how to file the appeal. Local unit must notify Cash Management and HUIT IT Security if they file an appeal.

Trustwave will work with the local unit to confirm the validity of the vulnerability. If Trustwave agrees with the reason for the appeal, they will note it in future reports but won't flag it as vulnerability. They will also reissue a corrected vulnerability report. The appeal process may take up to 5 business days.

If vulnerabilities are identified the local unit must take the following steps:

Develop an action plan for correcting the vulnerabilities and email this to Cash Management within 7 days of the scan failure. Keep your financial dean informed of any warnings resulting from the scans and your progress towards fixing the cause.

If determined that vulnerabilities will not be remediated within 30 days of the scan contact Cash Management immediately and discuss the alternatives.

Merchants will not be allowed to continue processing credit cards in a non-compliant state past the 30 days. Merchants may be allowed a temporary suspension without deactivating your account in the following conditions:

- The merchant has deactivated/ taken their web site/page off line.
- The merchant submitted an action plan within 5 business days of the scan
- Merchant has diligently and continuously worked on the resolution(s)
- HUIT's Security Officer agrees that the tasks on your action plan will remediate the vulnerabilities and that they have reasonable time estimates
- The Financial Dean supports the request for the extension

Otherwise the out of compliance account will be deactivated by Cash Management at the end of 30 days or before if it is determined that you will not be able to meet the 30 day requirement.

If a merchant account is deactivated the local unit will need to re apply for a new merchant account after they become compliant and will incur any charges associated with the opening of the account. The opening of a new merchant number with the bank may take up to 10 business days. No request for acceleration of this process will be accepted for merchants in this category.

Merchant Responsibilities for Network Penetration Tests

According to Requirement 11 of PCI Data Security Standard, all merchants that accept credit card numbers directly on their web site, store credit card account numbers on a back-end server (Category 2 or 3 in Appendix B), or if some element of the payment page originates on the merchant's website (whether Harvard-hosted or externally hosted) must conduct penetration tests annually. Cash Management and HUIT must receive a copy of the report when the test has been completed.

If your site requires a Penetration test, the local unit is responsible for the cost of such a test. If you wish to have Trustwave conduct the test for you, Cash Management can make those arrangements.

Merchants are responsible for correcting any deficiencies identified during the test. High risk vulnerabilities must be corrected within 30 days and medium risk vulnerabilities must be corrected within 90 days. Merchants must submit a report to CM and HUIT when the deficiencies have been corrected. After the merchant has corrected deficiencies, CM will schedule a second test to be conducted by HUIT. HUIT will specifically test for the vulnerabilities previously identified. In addition, CM will schedule a full penetration test to be conducted by HUIT six months after the conclusion of the test conducted by the University's third party assessor.

Requirement 11 also requires penetration tests to be performed after major changes such as an operating system upgrade, new sub-nets installed or a new web-server in the payment environment. These additional tests are the responsibility of the merchant. They may contract for a third party assessor or use internal resources[1]. IT organizations supporting credit card merchants must have a process in place that business owners and CM are notified well in advance of these types of upgrades.

Merchant Responsibilities for Annual Re-Certification

All Merchants must re-certify annually. Harvard University must report to the bank as of June 30 therefore all merchants must complete the questionnaire by June 15th of each year.

- Merchant **must** log on to the TrustKeeper portal and complete the questionnaire **prior** to the deadline.
- Merchant must reviews scan parameters to ensure they are correct.
- Merchants must complete the Annual Compliance Attestation form and return the signed copies to Cash Management by June 30th.
- Merchants must complete PCI training each year.
    - At least one business contact and one technical contact must complete the web training on-line. (Merchants that only have dial-up terminals do not need technical contacts to complete the training.)
- Failure to complete the questionnaire successfully will result in the merchant account being deactivated.

Merchant Responsibilities for Changes

Cash Management should be notified of any significant change in the merchant's web environment (e.g., new systems component installations, changes in network topology, firewall rule modifications, product upgrades) and the following tasks must be performed:

- Re-evaluate self-assessment questionnaire to ensure answers would not change
- Perform functional tests on the environment
- Have a directed remote vulnerability scan performed
- Verify firewall rules are still effective
- Document and provide an updated network diagram to pci_compliance@harvard.edu

Service Providers

Local units must obtain prior approval from Cash Management if a service provider is being used to ensure they are compliant with PCI requirements. Cash Management maintains the official list of Service providers in use at the University. Merchants must keep Cash Management informed when service providers are added or dropped.

[1] HUIT IT Security Team offers this service on a per request basis. Merchants are free to use any internal resources consistent with their local policies.

Certification Exception Process

In cases where the merchant cannot meet the standard exactly as written, the following steps must be taken to apply for an exception to the PCI Standards:

- Document why the standard cannot be met as stated and what additional or alternative controls will be put in place to achieve the spirit of the requirement and send the document to Cash Management and HUIT IT Security.
- Cash Management will share this document with Trustwave. Trustwave will review the controls and may issue an opinion that the additional controls represent compliance. Trustwave may have additional questions for the merchant during this evaluation.
- Cash Management will report the issue to the bank along with the mitigating controls implemented and future steps we may be taking.
- The Bank will either accept our explanation, ask us to take additional steps or ask us to deactivate the account.

It should be noted that this does not reduce the University's exposure in the event of a breach. It only would exempt us from fines levied solely for being out of compliance. This process should only be pursued where achieving compliance is technically not feasible and the alternative of not accepting credit cards prevents the local unit from meeting its mission.

Ongoing Operations

Merchant Responsibilities for Monitoring and Security Incident Handling

In the event of breach or compromise of credit card data, The University must comply with Massachusetts and other state laws, credit card association rules and other requirements. Merchants must work with appropriate University and school offices to ensure these requirements are being met, This includes but not limited to, Office of General Counsel (OGC) and the Harvard Public Affairs and Communication Office (HPAC). This section deals with electronic as well as paper based records. For breaches of paper records, the steps that refer to electronic issues can be omitted.

1) The Technical Contact for the merchant account should be alert to potential breaches and regularly monitor system logs for:
   - Suspicious behavior
   - Unusual incidents in audit logs
   - User or anonymous report of problems
   - Unauthorized security configuration changes
   - Unusual traffic or activity
   - Lapsed physical security
   - Sensitive information in the wrong place or hands
   - User complaint which triggers an investigation
   - Loss or theft of a computer or backup media
2) Contain and limit the exposure *immediately*:
   - Log all actions taken
   - Do not access or alter compromised systems.
   - Do not turn the compromised machine off. Instead isolate compromised machines from the network (i.e., unplug network cable).
   - Preserve all available logs (firewall, IDS, web server, operating system, remote access, etc.) that could be used to help identify the source and extent of the attack.

- If using wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.
- Be on high alert and monitor other systems that accept, store or process credit card account numbers as well as any other computers that users on the breached computer have accounts (too often the same password is used).

3) Contact Cash Management immediately of discovery that a breach or suspected breach has occurred or is in progress. (See PCI Security Breach procedures)

4) Work with PCI Incident Response Team (PIRT) to investigate the breach and repair the systems.

5) Identify what account numbers or other personal information (PI) may have been compromised.

6) Work with CISO, RMAS and OGC to determine if notification should be sent to individuals affected by the incident. (See Notifications)

7) Compromised systems must not be put back into production or connected to the Internet until the PIRT gives its consent.

8) If notifications are to be sent, work with OGC, HUIT, HPAC and Cash Management on content of notification. Cost of sending notifications is responsibility of Merchant.

9) All requests from the media must be directed to the OGC and HPAC or school Communications Officer.

10) Assume any extra costs associated with the incident:

- Any external resources contracted to participate in the investigation
- HUIT resources used to supplement local IT support resources
- It is up to the individual school to determine if IT resources expended on PIRT are billed to the local unit or absorbed as overhead
- Cost of level 1 PCI Security Standard Assessment performed by external third party. (See Security Breach Business Process Document for Scope of this external assessment)
- Any fines or penalties assessed by the Bank, credit card associations and/or State
- Any legal fees or penalties incurred as a result of the incident
- Any costs associated with producing and sending notifications
- Any external costs associated with a follow-up audit by RMAS

Reconciliation Procedures

The merchant is responsible for posting all credit cards transactions and associated fees via journal voucher on a monthly basis. Copies of all journal vouchers and supporting documentation must be sent to Cash Management, 1033 Massachusetts Avenue Room #411. Cash Management will provide training to the local unit on the process.

- Cash Management will provide merchant with instructions on what coding to use in debiting the cash account.
- Cash Management will be responsible for performing monthly reconciliation's of the bank account and email a copy of the reconciliation listing all un-reconciled transactions to the responsible person at the local unit.
- Merchant is responsible for researching and resolving all un-reconciled items within three months from transaction date. Cash Management will work with the local unit to resolve any outstanding items that are a direct result of a bank processing or posting error.

- On a monthly basis all transactions 90 days or older which have not been posted to the general ledger by local units, will be posted by Cash Management to each local units default coding. An email will be sent prior to posting to the default account to allow the local units a final opportunity to post the activity to the appropriate GL account.

Electronic Data Access

- Electronic access to cardholder account numbers should be restricted to only those with a business need to access that data. This includes all systems that contain the account numbers, e.g., local POS, Local applications, CyberSource Business Center, & BAMS.
- When employees leave or no longer need access Merchants must disable the access in any local systems and notify Cash Management so that access to CyberSource and BAMS can be disabled.
- Customer credit card numbers must not be stored on any user computer. Please see www.security.harvard.edu to review policy.

Paper records containing cardholder data

Paper records that have cardholder account numbers (e.g., credit card slips, order forms, hardcopy reports) must be kept locked up when not in use. Access to these records must be restricted with those who need it to perform job functions.

Retention: You should have a local data retention policy that determines how long you retain credit card information. Keep cardholder information storage to a minimum. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in your data retention policy.

- **Electronic** - Credit card numbers must never be stored locally in electronic form. If your business requires that you temporarily store credit card account numbers on a centrally located server, then the credit card data must be encrypted and securely disposed when no longer needed. It is permissible to retain the last four digits of the credit card number.
- **Paper** - Federal and credit card association require merchants to retain the original signed credit card merchant slip for 2 years. These should be kept locked on site for 2-3 months and then placed in Harvard University Records Center for the remainder of the 2 years. They should be securely destroyed directly from the records center. The reason for keeping these records is to dispute a chargeback (see below), if your ticket value is low or you experience very few charge backs, you may want to destroy these records after 2-3 months and accept any chargebacks that occur after that period. The risk of undisputed charge backs needs to be weighed against the exposure in the event these records become compromised. Please note: if receipts do not include the full credit card number they should be retained for the full two-year period required by the card associations. No additional security is required to retain these receipts.

Destruction of records: when no longer needed, paper records containing credit card numbers must be shredded with a cross cut shredder or incinerated.

Chargebacks

Chargebacks occur when a cardholder disputes a charge on their statement. Customers may dispute because they believe that they did not receive the goods or services for which they were charged or if they did not authorize the charge. Merchants are notified by the acquiring bank of the disputed charge. Merchants must follow the instructions on the form they receive from the bank and reply by the date specified. Merchants must have a local process for handling chargebacks. If a tub is experiencing

frequent charge back complaints or fraud is suspected, then Cash Management, Risk Management & Audit Services and tub Financial Dean or Financial Director should be contacted.

Merchants must have a local process for handling charge backs which should include:

- **How complaints will be handled**
- **What investigation, if any, will be done**
- **Who should be notified**

If you are experiencing frequent charge back complaints or suspect fraud, you need to contact Cash Management @ 5-4397 and/or cash_management@harvard.edu

Background Checks

Background checks must be performed on employees who have access to aggregate credit card account numbers. Merchants must have local policies that define which positions are subject to background checks. Background checks are for new hires, transfers into a covered position and temporary workers. Employees who only have access to one card number at a time while they are processing a transaction and then no longer have access to the card number are exempted from this requirement. Merchants should inform their local HR department of which positions require background checks, and include in those positions' job descriptions the need for background checks. Background checks should be carried out by local HR departments and evaluated in conjunction with OGC.

Local Policies and Procedures

Merchants must develop and maintain local policies and procedures for handling credit cards. Local policies and procedures should supplement this policy, the University Credit Card Merchant Handbook and University security policies that are found on www.security.harvard.edu. At a minimum, local policy should address the following areas:

1) authorization of transactions,
2) segregation of duties,
3) reconciliations,
4) chargebacks,
5) record retention,
6) data access
7) training,
8) background checks
9) physical security.

In addition, there may be local processes involved with the credit card processing that are not included in these general procedures (e.g., managing your point of sale system). These policies must be documented locally, and a copy of the documentation must be sent to Cash Management and the tub finance office. A guideline of what needs to be included in local policies is included in Appendix E.

Employees who are involved in credit card processing must receive copies of local policies and be made aware of the Cash Management web-site containing University policies. Employees should annually sign an acknowledgement that they have read and understand the policies and that they will comply with them. A sample acknowledgement form is included as Appendix G.

Credit Card Expenses[1]

Each credit card has its own monthly fees and rates (subject to change):

- Amex – 2.05% – 2.60% (Lowest rates are for tuition and related goods and services)
- Discover/MC/Visa – rates range from .05% + $.22 to 3.26% + $.10 depending on the credit card used, method of acceptance and use of fraud prevention services. Rates for online acceptance run higher. (See Appendix J for details)

  In addition Visa and MasterCard have added an Acquirer Network fee that is based on the number of merchant locations, sales volume, and Merchant Category Code. Please refer to the Visa and MasterCard websites for specific fee information.

Equipment: (subject to change)

- Terminals- Effective October 2015, all merchants are required to use EMV terminals that have the ability process chip-enabled credit cards. If you need a new or replacement terminal, contact your Cash Management accountant to receive a price quote and to place your order.

Monthly Merchant Statement:	Waived
Chargeback Fee	$ 15.00

CyberSource Program Pricing:

• Set Up Fee	$ 100.00
• Per transaction fee	$.10 per transaction (Note this is in addition to discount and transaction fees assessed by card type outlined above. Also note that this rate can fluctuate based on the overall University Volume)

Financial Administration Costs - $2,400 per merchant. These fees are not billed but represent the cost to central to support reconciliations and compliance. Compliance covers the cost of certification, ongoing monitoring and periodic audits.

Internal Costs - To operate the terminal you will need to have an "Analog Line" set up. Please contact your telecommunications support.

Resources for information on Credit Card Acceptance

Cash Management web site.

http://otm.finance.harvard.edu/credit-card-merchant-accounts

Information on Payment Card Industry Data Security Standards

http://www.usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

[1] All Cost subject to change

http://www.mastercard.com/us/merchant/security/what_can_do/SDP/merchant/index.html

Harvard Information Security Policiy web site.

http://security.harvard.edu/book/information-security-policy

- See #4 Credit Cards – Accepting Payment Cards on left hand navigation bar.

Glossary

DEFINITIONS

Acquiring Bank – The bank which provides the University's merchant services and issues the local units a merchant number.

Assessor – a company authorized by the card associations to certify merchants as compliant with PCI requirements.

Card association – Each brand of credit cards, (Visa, MasterCard, etc.) has a governing body that sets rules for its acceptance and processing. These governing bodies are known as card associations, Visa MasterCard, American Express, and Discover card associations have jointly agreed on the Payment Card Industry Data Security Standards.

Cash Management Credit Card Merchant Database – This is an Access Database that contains all relevant data about all Credit card merchants at Harvard.

Compliance Portal – The online access to compliance certification status. The portal has two aspects. First, each merchant has access to change and review their own self assessment questionnaire, scan parameters and profile as well as view only for their compliance and vulnerability scan reports. Second, Cash Management has access to a sponsor account that allows them to review status of all merchants as well as view individual compliance reports and scan parameters. The portal is provided by our assessor.

CyberSource Secure Acceptance Secure Acceptances (previously Hosted Order Page (HOP)) – A web page hosted by CyberSource, the University's designated gateway vendor, that accepts credit card information and then returns success or failure responses back to your local web-site. Secure Acceptance was previously Hosted Order Page (HOP).

EMV (Europay, MasterCard, and Visa) - a global standard for inter-operation of integrated circuit cards "chip cards" and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions. Also known as chip or smart cards.

Local Unit - A Harvard department or school that has obtained a credit card merchant number assigned from Cash Management

Merchant – A local unit that is processing credit card transactions. Please note that a local unit may obtain more than one merchant number.

Merchant File – A file maintained by Cash Management that is organized by individual Merchant.

Merchant ID (MID) - MID stands for the unique number assigned to a merchant and identifies the merchant to an ISO (independent sales organization or reseller), acquiring bank or third party processor. This not the same as the merchant account number.

PCI Compliance file – A file maintained by Cash Management that is organized by Merchant. It contains reports and logs of communications regarding compliance of the merchant.

Service Provider – Service providers are organizations that process, store, or transmit cardholder data on behalf of merchants. Service providers must be certified to be PCI Compliant as indicated on the MasterCard or Visa websites..

Terminal ID (TID) - This is the number assigned to a credit card transaction device (i.e. POS terminal or Virtual Terminal). It identifies the merchant's physical equipment, gateway or software to the processor and bankcard data transport networks. A merchant account may have multiple TIDs.

TrustKeeper – Harvard's compliance portal provided by Trustwave.

Trustwave – Trustwave is the University's PCI assessor for PCI Compliance Certification.

ABBREVIATIONS

AVS – Address Verification Service

BAMS – Bank of America Merchant Services

BoA – Bank of America

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CM – Cash Management

CVC/CVV – Card verification services provided by MasterCard and Visa for card not present transactions

DSS -- Data Security Standard

PCI DSS – Payment Card Industry Data Security Standard

PA DSS – Payment Application Data Security Standard

HCCMA – Harvard Credit Card Merchant Agreement

HPAC – Harvard Public Affairs and Communications

HUIT – Harvard University Information Technology

HUIT IT Security – Harvard University Information Technology IT Security team

IT – Information Technology

MC – MasterCard

OGC – Office of General Counsel

OTM – Office of Treasury Management

PA – Payment Application

PCI – Payment Card Industry

PI – Personal Information

PIRT – PCI Incident Response Team

POS – Point of Sale System

RMAS – Risk Management and Audit Services

TID – Terminal ID

VPF – Vice President for Finance

Appendix A - Software Exemptions

Overview

Harvard University Policy requires merchants accepting credit cards over the Internet use CyberSource Secure Acceptance (previously called Hosted Order Page or HOP), which is the approved method to perform this function. It is recognized that some software purchased to perform a specific function may have credit cards acceptance built into the functionality. If this software is being purchased off the shelf, and modifying it to use Secure Acceptance is either not feasible or not practical (e.g., cost to modify to use Secure Acceptance is greater than the cost of the software) then exemptions may be requested from the CIO. The local unit purchasing the software is responsible for ensuring that the software, the systems on which its runs, including the implementation, are complaint with all regulations regarding credit card acceptance. Software can only be considered for exemption if it meets the criteria below.

Criteria

Merchant must provide a written document from the vendor stating that the software is compliant with all PCI Data Security Standards and they will provide support for resolving any compliance issues discovered by Harvard or our scanning vendor and that there will not be a charge beyond the normal maintenance contract for resolving any compliance issues. The document must include the following:

- Vendor must guarantee that the software will be made compliant within the PCI mandated timeframe if the PCI Data Security Standard is changed and that there will not be a fee to upgrade to the compliant version.
- Vendor must agree that its software is currently certified to run on the latest release of the operating system it is designed to run on.
- Vendor agrees to support its product and rectify any problems quickly if the local unit installs security patches supplied by the operating system vendor when such patches are released.
- Vendor provides support for PCI compliance issues either through its standard helpdesk or through a different contact that they are contractually obligated to maintain.

Local Unit must demonstrate that using Secure Acceptance is not practical and that they have reviewed previously approved exemptions of similar software. Local Unit must cooperate with HUIT in their review of the software's compliance with the above criteria.

Process

- Local Unit requests an exemption from Cash Management
    - The request for an exemption must be in writing and must include detailed business justification as to why existing authorized software solutions do not meet their business needs.
- Cash Management reviews expected use and compares it to software previously exempted. If software appears similar, CM will provide the information to local unit to review. Local unit may continue their request for an exemption but existing software that meets their need will be considered in the review by HUIT IT Security.
- Cash Management provides local unit information to HUIT IT Security for evaluation.
- HUIT IT Security meets with Local Unit and compares software against criteria.

- HUIT IT Security forwards request with their report, including their recommendation, to the CIO with copy to Cash Management.
- CIO approves or rejects exemption request.

Appendix B - Web Hosting Requirements

Overview

Harvard Websites that accept credit cards must always comply fully with PCI Data Security Standard requirements. Full requirements for the PCI standard can be found at:
https://www.pcisecuritystandards.org/

In addition Harvard has established additional requirements depending on the category of web site maintained by a merchant. In some cases noted below the data center housing the web site must be qualified. A description of the qualification procedures are listed after the requirements section.

Categories of web sites

1.  Stand alone web site for ordering – link to Secure Acceptance to accept credit cards
   a. Some sites may also be linking directly to another certified service provider hosted site to accept cards
2.  Stand alone web site accepting credit cards directly not storing credit card account numbers
3.  Web site for orders paired with a data base server that stores credit card account numbers
4.  Stand alone web site accepting credit cards directly and storing credit card account numbers

Requirements by category

Stand alone web site for ordering – link to Secure Acceptance to accept credit cards

1. Local systems and processes must be fully compliant with Harvard Enterprise Security Policy.
2. Web server must be isolated from the network with all outside access restricted to hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN). Any other protocols or ports required for a specific business purposes must be documented (See PCI Requirement 1.1.6 & 1.1.7).
3. Local system must be scanned for vulnerabilities prior to being placed in production.
4. Local system must be scanned monthly for vulnerabilities by Harvard's chosen vendor.
5. System must be in a secure physical environment.
6. Periodic audits

Stand alone web site accepting credit cards directly – not storing credit card account numbers

1. Systems and Processes must be fully PCI compliant
2. Web server must be housed at UIS or in another qualified site
3. Web server must be isolated from the network by a firewall with all outside access restricted to hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN). Any other protocols or ports required for a specific business purposes must be documented (See PCI Requirement 1.1.6 & 1.1.7).
4. System must be scanned for vulnerabilities prior to being placed in production
5. System must be isolated from non credit card applications on the network
6. Local unit must have sufficient resources devoted to monitoring the systems and maintaining the security environment as required in PCI DSS.
7. Local unit must have resources available 24/7 to respond to breaches or other emergencies. (These can be local resources or contracted.)

8. Local unit must undergo periodic audits no less frequently than once every three years.

Web site accepting orders paired with a data base server that stores credit card account numbers

1. Systems and Processes must be fully PCI compliant.
2. Must supply a compelling business requirement to store credit card numbers. (Business case must be extremely compelling. If breached, the initial cost could easily be measured in seven figures with additional operating costs for all of Harvard in terms of increased transaction fees and more stringent compliance certification costs.)
    a. A special exemption must be granted to keep credit card account numbers. The merchant must request an exemption from Cash Management (CM). The merchant will be able to present their business case to CM and HUIT IT SECURITY IT Security. CM and HUIT IT SECURITY will write up their evaluation and it will be forwarded on for approval by the school financial dean, the CIO, and VPF.
    b. CyberSource offers a service named Recurring Billing, which allows them to keep the cardholder data and supply you with a profile reference number to retain for your records. This is the preferred method to meet the business need for recurring charges.

2) Web server and database servers must be housed at HUIT IT SECURITY or in another qualified site
3) The credit card account numbers are stored on a separate data base server that is not Internet accessible. This separate system must also be protected by a firewall.
4) The data base server(s) must be isolated from non credit card applications on the network.
5) Web server must be isolated from the network by a firewall with all outside access restricted to hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN). Any other protocols or ports required for a specific business purposes must be documented (See PCI Requirement 1.1.6 & 1.1.7).
6) System must be scanned for vulnerabilities prior to being placed in production
7) System must be isolated from non credit card applications on the network
8) Local unit must have sufficient resources devoted to monitoring the systems and maintaining the security environment.
9) Local unit must have resources available 24/7 to respond to breaches or other emergencies. (These can be local resources or contracted.)
10) Local unit must undergo annual audits. Local unit must bear the cost of this audit if it cannot be provided by RMAS.

Stand alone web site accepting credit cards directly and storing credit card account numbers

Not permitted by PCI data security standard.

Qualified Sites

Schools wishing to have a site qualified must request RMAS to evaluate their site. RMAS will review sites for the following compliance to PCI requirements:

- Physical Security of the data center
- Local policies supporting the credit card IT architecture in compliance with PCI requirements
- Ability to support 24/7 response to breaches
- Appropriate logging at the Operating System level with ongoing review of logs

Appendix C - Template for New Merchant Request

New Merchant Request Form

Appendix D –

Harvard Credit Card Merchant Agreement (HCCMA)

I. Introduction

The Harvard credit card merchant agreement represents the terms and conditions for Harvard University departments obtaining a credit card merchant account.

1. Purpose of this document

This agreement provides the basis for a partnership between Cash Management (CM), HUIT IT SECURITY and _____ (merchant/local unit). It details the services provided by CM and HUIT IT SECURITY and outlines the basic responsibilities of each party involved. Throughout this document the term ***Merchant*** refers to the local unit named above.

2. Dispute resolution

The primary point of contact is the CM credit card accountants at 617-495-4397 or 496-0853. If a satisfactory resolution has not, or cannot be reached, the problem will be brought to the attention of the Manager of Cash Management. For current contacts, please refer to the list of contacts provided on Cash Management's web site. CM and HUIT IT SECURITY play a primary role in interpreting the policies and procedures outlined in this document and other University communications pertaining to credit card processing. CM is the only area with employees authorized to contact our credit card processor. Bank of America Merchant Services (BAMS), Harvard's preferred merchant services provider, provides equipment and other operational assistance to our merchants.

II. General Responsibilities

CM agrees to:

- Set up and maintain merchant account(s) with the credit card processor.
- Notify merchants on a regular and timely basis about service availability, product features and upgrades and changes to University and credit card association policies.
- Provide customer support via telephone and e-mail during normal business hours (Monday thru Friday, 9 AM – 5 PM).

Merchant agrees to:

- Read, understand and carryout all responsibilities outlined in the Harvard Credit Card Merchant Handbook.

- Attend annual campus credit card training meetings and implement any changes expected by the card processor. Information about these will be provided by CM.
- Meet connectivity and security requirements as provided herein.
- Follow University policies and procedures for ensuring data security and comply with guidelines for credit card acceptance.

III. Account Setup, Testing, & Maintenance

Account Setup

Upon receipt of signed, completed CCMA Merchant Request Form, CM will do the following:

- Present request to the PCI Executive Committee for approval.

If Approved:

- Create a merchant account with a credit card processor contracted by Cash Management.
- Create an account in the TrustKeeper portal used for compliance certification for the merchant account.
- When required, initiate requests for:
  1. CyberSource account (Our preferred Internet Gateway)
  2. BAMS – access to Bank of America Merchant Services web base platform

Before the user can create transactions, the merchant must be certified to be in compliance with Payment Card Industry (PCI) Standards. Compliance is certified through the completion of a self-assessment questionnaire in the TrustKeeper compliance portal and a successful scan of any Internet accessible computers that store, transmit or process credit card account numbers.

Depending on the complexity of the set-up process, establishment of a new account can take a number of weeks. This period of time may be necessary because of the number of third parties involved in the process, particularly for web based merchants, which Cash Management cannot completely control. Request should be made early enough to allow for sufficient time. (Our recommendation is 4-6 weeks.)

User Training

Cash Management will provide basic training and documentation outlining the transaction authorization and settlement process. Participation is required before the credit cards can be accepted and the account activated.

Account Maintenance

Cash Management will act as a liaison to the bank, gateway and processor.

Refunds/credits to an account must be processed by a different user authorized to access that account. The user who creates a transaction cannot process a refund/credit.

Requests to activate, deactivate, or suspend a merchant account must be received in writing from an authorized signer(s).

IV. Security

Security is a top priority for credit card transactions. In order to accept credit cards over the Internet, a merchant must have a secure web site. RMAS must qualify physical locations housing credit card servers. Individual credit card information is confidential; failure to maintain strict controls over this information could result in unauthorized use of a credit card number and serious problems for both the customer and the merchant. The risks of non-compliance by the University include substantial fines and penalties imposed by the card associations, as well as reputational risk and liability for all losses incurred as a result of a security failure. In the event of a security breach, all penalties, fines, and costs imposed by the credit card associations and the banks are the responsibility of the local units.

Merchant-level Security

It is the merchant's responsibility to maintain a secure environment for credit card processing. Merchant agrees to take sufficient measures to ensure security of a cardholder's information. These include, but are not limited to:

State and federal data privacy and security laws, including:

- SB1386 (CA Civil Code 1798.29 & 1798.82-1798.84),
- Gramm-Leach-Bliley Act of 1999,
- Massachusetts Notification of Data Breaches, and
- Other state legislation regarding privacy and security

Restrict access to authorized administrative users.

Merchant must *never*:

- Transmit credit card information via unencrypted e-mail.
- Store card information in an unsecured database or other digital medium.

CM reserves the right to suspend or terminate service at any time if sufficient security measures are not employed by the merchant.

V. Third Party Vendors

Merchants are responsible for third party processors that they grant access to cardholder data. Merchants must only use certified service providers to handle or process cardholder account numbers.

All vendors with access to cardholder account numbers must be contractually obligated to comply with the PCI requirements. Merchants must notify Cash Management of service providers being used and obtain approval.

VI. Support

Technical

- CyberSource provides support to Merchants using SECURE ACCEPTANCE or Virtual terminal.
- Merchant is responsible for establishing and maintaining local web-site.
- CM does not provide any technical assistance to the Merchant.
- Technical Support beyond HUIT IT SECURITY IT Security's guidance must be separately contracted with HUIT IT SECURITY

Administrative

- Cash Management
    - Manage bank relationship
    - Be primary liaison between bank and local unit on issues related to the bank
    - Reconcile bank account to the general ledger
    - Notify the Merchant about any reconciliation or deposit problems
    - Post any unreconciled items over 90 days old to default coding provided by merchant
- Merchant
    - Ensure that a mandatory reviewer is set up for each account used
    - Post revenue (credit card deposits) and expenses (credit card fees) in a timely manner to the General Ledger
    - Research and resolve any un-reconciled items in a timely manner
    - Ensure that any refunds/credits are processed by a user other than the one who created the original transaction.
- The CM Support Team is the Merchant's first line of contact for support. Support Team members can answer questions about:
    - Merchant setup and maintenance
    - Billing questions
    - General processing questions

VII. Reporting

Bank of America Merchant Services (BAMS) provides online access to your credit card transactions. Cash Management will set up merchant user responsibilities in the system as well as merchant user access to CyberSource. If a local unit uses CyberSource, then Cash Management will provide authorized users with access to review reports from the gateway. Merchants must notify Cash Management if the authorized users need to change.

VIII. Cost and Billing

Bank Fees

All bank fees (access, interchange, processor, etc.) are negotiated by CM and are subject to change without notice.

- Bank fees are billed directly to the merchant in the form of assessment fees. It is the responsibility of the merchant to post these fees to the general ledger. The actual payment is deducted directly out of the bank account.
- Please see current rate sheet for the most current rates charged by the processor.

IX. Signatures

The parties listed below agree to the terms and conditions listed in the HCCMA. Any updates to the original agreement shall be considered part of the original agreement entered into unless written notification within 30 days is provided by party, thereby nullifying said agreement.

Department Name: _____
Department Default Coding: _____
Merchant Name: _____

_____ _____
Department Representative/Business Owner Date

School CIO's are responsible for security of electronic storage and processing of credit card data.

_____ _____
School or Unit CIO

Not Required by Merchants only using Dial-up terminals

_____ _____
Financial Dean/Financial Director Date

Appendix E

Merchant's Local Credit Card Policy Guidelines

This document represents an outline of items that should be covered in a local policy regarding credit cards. It should be viewed as a starting place for developing your own policy and not a finished product. Due to the significant differences in each individual merchant's processes this outline may include items that are not relevant to your situation. It also may not include items that should be included in your policy. If you wish to get feedback on your individual policy please send it to cash_management@harvard.edu.

All Merchants

Authorization of Transactions

Include positions that can approve refunds. If you are authorizing and settling at different times you should identify positions that can authorize settlements as well.

Segregation of Duties

Discuss how tasks are split within the local unit for control purposes. For example, the person reconciling the account should not be the one creating transactions.

Reconciliations

Identify who is responsible to reconcile the account. Also identify what local systems or local data needs to be reconciled to the credit card transactions. Depending on the complexity of the process, spell out the steps to take.

Charge backs

Identify the process you would go through when notified by the bank that a charge has been disputed by the cardholder. Identify the following:

- What research would be performed
- Who or what positions can approve refunds

Spell out the steps to take in responding to the bank's inquiry. If you are not challenging the cardholder's dispute, you should issue a refund and notify the bank of what you have done. Failure to notify the bank can result in the refund being issued twice (once by you, once by the bank).

Record Retention

Identify how long you will keep any records (electronic and paper) that contain credit card numbers. You should start from a position of not storing full card numbers. Add specific storage exceptions only where required for business reasons. Card associations have different requirements (6 months to 2 years) for storing card numbers to dispute charge back requests. You may retain the last 4 digits of the card number longer than two years.

For paper records, specify how and where they will be locked when not in use. Specify which positions should have access to the files.

Please note: if receipts do not include the full credit card number they should be retained for the full two-year period required by the card associations. No additional security is required to retain these receipts.

Data Access

Identify positions which will have access to systems or files containing credit card numbers.

Training

Specify who is responsible for conducting local security training. Training should be held at least annually. Local training needs to include all aspects of local policies. It may additionally cover University Policy and PCI requirements. University Policy and PCI requirements will be covered by training provided by Cash Management on an annual basis.

Background Checks

Need to identify which positions have access to aggregate credit card data. These positions will be subject to background checks as specified by your local HR office. The job descriptions for these positions should include an indication that individuals need background checks before assuming the responsibilities of the position. Local HR needs to be aware of which positions require background checks.

Physical Security

Describe physical security of systems and files which contain credit card numbers.

Annual Certification

Identify who is responsible for completing the annual self assessment questionnaire.

Incident Response

Identify which positions need to be involved when responding to a breach or suspected breach of cardholder data. Identify which local staff will carry out the responsibilities indicated in the PCI Data Security Breach Procedures issued by Cash Management. Also identify reports or other circumstances that may indicate a breach has occurred.

Web & POS Merchants

Security Policies

Identify specific security policies which deal with the technical infrastructure supporting your payment acceptance. Your local policies should be consistent with the security policies found on www.security.harvard.edu.

Change Control

Describe the process on how changes to your payment application are managed. Include who can make changes, who approves them and what testing takes place. Changes should be tested in a test environment prior to being placed in production. This section should also deal with new releases and patches supplied by vendors.

Business Continuity

Describe how your response to a disaster or other incident will maintain the security of cardholder data.

Monthly Scans

Identify who is responsible for reviewing TrustKeeper Portal after a scan has been run. Also identify the process for correcting vulnerabilities discovered.

Penetration Tests

Identify what types of changes in your local environment would necessitate a separate penetration test from your annual one. Identify who will work with Cash Management in scheduling your annual penetration test. Identify resources that will correct deficiencies identified during the test.

System Monitoring

Identify what positions are responsible for monitoring systems involved in credit card acceptance or storage of cards. Identify logging and other monitoring currently taking place.

Appendix F

Single Use Workstations (Virtual Terminals)

Workstations (desktop or laptops) that are used to enter credit card numbers should only be used for that function. These workstations must comply with all relevant PCI data Security Standards. ***Outlined below are the minimum requirements that would be relevant.***

- These workstations must be protected by a firewall that isolates them from the internet and other Harvard networks. This can be accomplished through a personal firewall on the machine or a direct connection to a stateful inspection firewall.
    - Firewall rules should be implemented with the default of deny and specifically allow only those connections required.
- They cannot be installed using vendor supplied default passwords and other security parameters
- The connection to remote site must be encrypted e.g., by using SSL (//https :)
- Anti-virus software must be installed, actively enabled and up-to-date
    - The AV software must address all types of malware.
- Must have latest security patches installed
- Presence of wireless access points must be tested for by installing a wireless IDS/IPS or by using a wireless analyzer or by other methods specified in requirement 11.1 of PCI DSS at least quarterly

In addition the following Harvard requirements must be met:

- Contact HUIT for assistance with imaging the system to comply with Harvard requirements.
- All firewall rules that specifically allow a connection need to be documented with the business requirement and any additional security in place for that connection.
- All software and operating system patches must be up-to-date
- Anti-virus/anti-malware must be installed, configured for real-time detection, and up-to-date
- The system must be separated from the Internet using a network firewall configured to block all unwanted inbound traffic
- A host-based firewall must be installed, running, and configured to block all unsolicited traffic
- Laptops and other portable systems must be encrypted
- Accounts with administrative privileges must use strong passwords
- Web browsers must be configured to not store passwords

- All users of the system must have individual accounts configured with non-administrative access. Harvard users must configure their accounts with a strong password.

Appendix G – Employee Acknowledgement

Employee Acknowledgement Form

Example 1:

I have read and understand this policy; and I acknowledge receipt of a copy of this policy and agree to follow it.

Employee Signature_____ Date: _____

Example 2

Another alternative is to have a separate form for the employee to sign.
Employees are required to acknowledge each year that they have read, understand and will comply with security policies. This can be done by having them sign a copy of the merchant's local credit card policies. A sample statement is below.

Name: _____
HUI: _____

AS an employee of the <<Department Name>> I acknowledge the following statements:

- I am aware that University security policies regarding credit cards can be found at http://vpf-web.harvard.edu/otm/cm/index.shtml
- I have received a copy of my department's policies regarding credit card security.
- I understand how these policies relate to my job duties and will comply with these policies.

Signed: _____ Date:_____

Appendix H – AVS Codes

AVS is a fraud prevention service that Harvard web merchant must use in accepting credit card transactions online. The below table reflects that standard codes that the bank processing network will return on any transaction using AVS. If using CyberSource SECURE ACCEPTANCE, CyberSource's standard AVS processing will apply. If using an API, merchants must follow the recommended action unless they have approval from Cash Management for an optional action.

AVS Code	Result	Detail Description	Recommended Action	Merchant Option
A	Partial match	Street address matches, but both 3-digit and 9-digit postal code do not match.	Customer can have up to three chances to get information correct. Display a standard message (see below).	Merchant, in consultation with Cash Management may decide to accept this code.
B	Partial match	Street address matches, but postal code not verified. Returned only for non-U.S.-issued Visa cards.	Customer can have up to three chances to get information correct. Display a standard message (see below).	Merchant, in consultation with Cash Management may decide to accept this code.
C	Not verified	Street address and postal code not verified. Returned only for non-U.S.-issued Visa cards.	Accept	Merchant may choose to not accept this type of transaction. If Merchant chooses this option, display a message that you do accept cards that were issued outside of the United States.
D	Match	Duplicate of M. Street address and postal code both match. Returned only for non-U.S.-issued Visa cards. Although D and M are duplicates, it is possible that you will receive both.	Accept	
E	Invalid	AVS data is invalid.	Accept	
G	Not supported	Non-U.S. issuing bank does not support AVS.	Accept	Merchant may choose to not accept this type of transaction. If Merchant chooses this option, display a message that you do accept cards that were issued outside of the United States.
I	Not verified	Address not verified. Returned only for non-U.S.-issued Visa cards.	Accept	Merchant may choose to not accept this type of transaction. If Merchant chooses this option, display a message that you do accept cards that were issued outside of the United States.

AVS Code	Result	Detail Description	Recommended Action	Merchant Option
J	Match	This code is returned only if you are signed up to use AAV+ with the American Express Phoenix processor. Card member's name, billing address, and postal code all match. Shipping information verified and chargeback protection guaranteed through the Fraud Protection Program.	Accept	
K	Partial match	This code is returned only if you are signed up to use Enhanced AVS or AAV+ with the American Express Phoenix processor. Card member's name matches. Both billing address and billing postal code do not match.	Customer can have up to three chances to get information correct. Display a standard message (see below).	Merchant, in consultation with Cash Management may decide to accept this code.
L	Partial match	This code is returned only if you are signed up to use Enhanced AVS or AAV+ with the American Express Phoenix processor. Card member's name matches. Billing postal code matches, but billing address does not match.	Customer can have up to three chances to get information correct. Display a standard message (see below).	Merchant, in consultation with Cash Management may decide to accept this code.
M	Match	Duplicate of D. Street address and postal code both match. Returned only for non-U.S.-issued Visa cards. Although D and M are duplicates, it is possible that you will receive both.	Accept	Merchant may choose to not accept this type of transaction. If Merchant chooses this option, display a message that you do accept cards that were issued outside of the United States.
N	No match	Street address, 3-digit postal code, and 9-digit postal code all do not match.	Customer can have up to three chances to get information correct. Display a standard message (see below).	These codes cannot be overridden
O	Partial match	This code is returned only if you are signed up to use Enhanced AVS or AAV+ with the American Express Phoenix processor. Card member's name matches. Billing address matches, but billing postal code does not match.	Customer can have up to three chances to get information correct. Display a standard message (see below).	Merchant, in consultation with Cash Management may decide to accept this code.

AVS Code	Result	Detail Description	Recommended Action	Merchant Option
P	Partial match	Postal code matches, but street address not verified. Returned only for non-U.S.-issued Visa cards.	Accept	Merchant may choose to not accept this type of transaction. If Merchant chooses this option, display a message that you do accept cards that were issued outside of the United States.
Q	Match	This code is returned only if you are signed up to use AAV+ with the American Express Phoenix processor. Card member's name, billing address, and postal code all match. Shipping information verified but chargeback protection not guaranteed (Standard program).	Accept	
R	System unavailable	System unavailable.	Accept	
S	Not supported	U.S. issuing bank does not support AVS.	Accept	
U	System unavailable	Address information unavailable. Returned if the U.S. bank does not support non-U.S. AVS or if the AVS in a U.S. bank is not functioning properly.	Accept	
V	Match	This code is returned only if you are signed up to use Enhanced AVS or AAV+ with the American Express Phoenix processor. Card member name matches. Both billing address and billing postal code match.	Accept	
W	Partial match	Street address does not match, but 9-digit postal code matches.	Customer can have up to three chances to get information correct. Display a standard message (see below).	Merchant, in consultation with Cash Management may decide to accept this code.
X	Match	Exact match. Street address and 9-digit postal code both match.	Accept	
Y	Match	Exact match. Street address and 3-digit postal code both match.	Accept	
Z	Partial match	Street address does not match, but 3-digit postal code matches.	Customer can have up to three chances to get information correct. Display a standard message (see below).	
1	Not supported	CyberSource AVS code. AVS is not supported for this processor or card type.	Accept	

AVS Code	Result	Detail Description	Recommended Action	Merchant Option
2	Invalid	CyberSource AVS code. The processor returned an unrecognized value for the AVS response.	Accept	

Note:

The three attempts at getting it right should be a limit regardless of whether it was caused by incorrect entry to fields, CVV error or AVS error. After the three attempts the transaction should be rejected.

When displaying error messages it is important to not give too much information as to what was wrong. If someone is using a card fraudulently you do not want to let them know which peach of information caused a problem. The response to the browser should be identical regardless of error. Display a message similar to: "Some of the information that you have supplied does not match the data from the bank that issued the credit card. Please verify and then submit again. Common problems are the CVN number was incorrectly entered or the address does not match the billing address for the credit card supplied."

Appendix I Credit Card Transaction Data Flow

Appendix J– Visa and MasterCard Rate Structure

Qualifying for the Best Rate

Card Present
In order to qualify for the best rates, locations should if possible, swipe the card to read and capture the card information via the magnetic stripe. If the magnetic stripe is damaged, manually key the card number and expiration date to the terminal. If the the terminal is down, the location should contact Terminal Support for assistance and instructions to process the transaction. To prove that the card was present at the time of the transaction,the sales slip must have the card member's signature. Failure to follow these procedures could result in a chargeback. Batches must be settled within 24 hours of the transaction date.

Card Not Present
If a location is accepting mail/telephone/Internet orders, the merchant must collect the following information: the card member's account number; expiration date; CVV code, date of transaction; description of the goods and services; amount of the transaction (including shipping, handling, insurance, etc.); card member's name, billing address and ship to address; authorization code; and merchant's name and address (city and state required).

You may not submit a transaction for processing until after the merchandise has been shipped or the service has been provided to the customer.

It is recommended batches be settled daily.

Address Verification Service (AVS)
Address Verification Service (AVS) is a process that is required by Visa to minimize the risk involved in processing card-not-present and manually keyed transactions. The merchant is required to enter the cardholder's zip code and order number. This information is sent with the authorization request for verification. The AVS response code is sent to the merchant with the authorization number assigned by the authorization center. The merchant can use the response code to determine whether the merchandise should be shipped and the transaction completed. The AVS response codes range from address and 5-digit zip match to address and zip do not match.

Manually keyed transactions processed by Retail merchants require a full zip code match or retry response to qualify for the best rate.

Credit Card Verification Numbers
To help guard against fraud, the Visa and MasterCard have implemented a system to ensure the credit card used in a transaction is actually possessed by the user. This systems are called CVV2 (Visa) or CVC2 (MasterCard). (American Express has a similar system called CID). The verification number is a non-embossed number printed on the credit card. CVV2/CVC2 provides a cryptographic check of the information embossed on the card and helps validate that the customer has a genuine Visa or MasterCard and that the card account number is legitimate.

Visa/MasterCard/Discover Interchange Rates
Visa and MasterCard have a complex fee structure based on the type of card used and whether the transaction is "qualified". A detailed description can be found at these sites. A current summary is also posted on Cash Managements website (fad.harvard.edu/otm/cm)

- http://www.mastercard.com/us/merchant/how_works/interchange_rates.html

- http://usa.visa.com/merchants/operations/interchange_rates.html