

**UNIVERSITY OF ALABAMA  
AT BIRMINGHAM (UAB)**

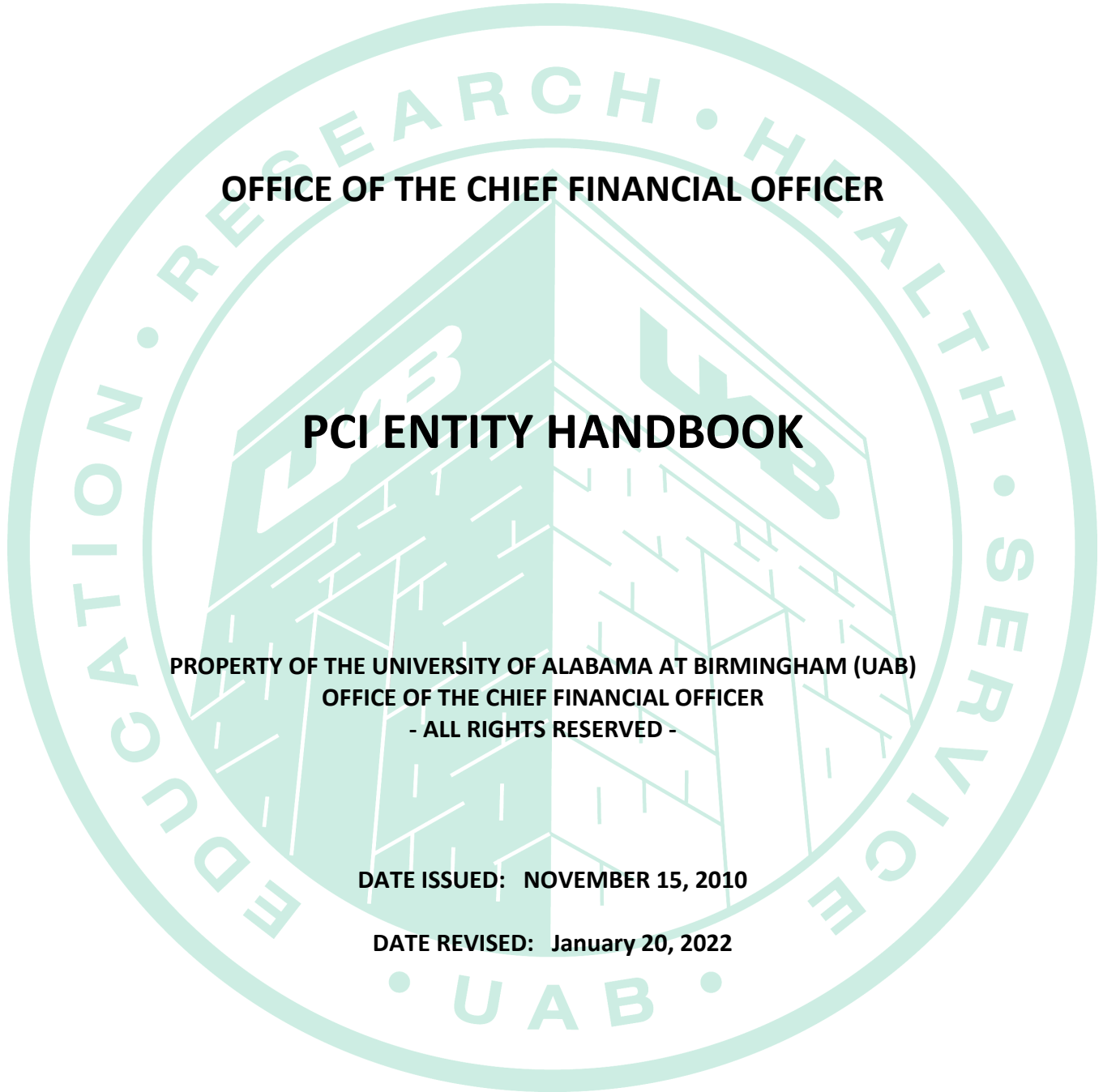
**OFFICE OF THE CHIEF FINANCIAL OFFICER**

**PCI ENTITY HANDBOOK**

**PROPERTY OF THE UNIVERSITY OF ALABAMA AT BIRMINGHAM (UAB)  
OFFICE OF THE CHIEF FINANCIAL OFFICER  
- ALL RIGHTS RESERVED -**

**DATE ISSUED: NOVEMBER 15, 2010**

**DATE REVISED: January 20, 2022**



**Contents**

PCI ENTITY HANDBOOK..... 1

1. Introduction ..... 1

    1.1. Background..... 1

    1.2. Scope / Applicability..... 2

    1.3. Implementation..... 2

    1.4. PCI Executive Committee ..... 2

    1.5. Handbook Overview..... 3

    1.6. Primary UAB PCI Contacts ..... 4

    1.7. Related Policies/Documents ..... 4

    1.8. Sanctions ..... 4

    1.9. Payment Card Privacy Statement ..... 5

    1.10. References ..... 6

2. PCI Entity Approval and Registration Procedures ..... 8

    2.1. Pre-requisites to Requesting a UAB Payment Card Account ..... 8

    2.2. Requesting a UAB Payment Card Account..... 9

    2.3. Certification of Compliance Requirements..... 11

    2.4. Security Awareness Training ..... 12

    2.5. UAB PCI Entity Account Agreement..... 12

    2.6. Background Checks ..... 13

    2.7. Required Entity Documentation ..... 13

    2.8. New Account Setup Summary..... 13

3. PCI Entity Payment Card Processing Environments..... 17

    3.1. Payment Card Processing Types ..... 17

        3.1.1. Terminals..... 17

        3.1.2. PIN Entry Devices (PED) ..... 17

        3.1.3. Point to Point Encryption (P2PE) ..... 18

        3.1.4. Payment Applications ..... 18

        3.1.5. Web Hosting..... 19

        3.1.6. Virtual Terminals..... 20

        3.1.7. Service Providers..... 20

    3.2. TouchNet Marketplace (UAB Provided Service) ..... 21

- 3.3 Fraud Prevention..... 21
- 4. PCI Entity Compliance..... 24
  - 4.1 Trustwave and the SecureTrust Portal..... 24
  - 4.2 Monthly Scans ..... 25
  - 4.3 Network Penetration Tests ..... 27
  - 4.4 Change Control (Technical) ..... 28
  - 4.5 Security Awareness Training ..... 29
  - 4.6 Annual Re-Certification Summary..... 30
  - 4.7 Compliance Certification Exception Process..... 31
- 5. PCI Entity Responsibilities..... 33
  - 5.1 Business Process and Procedures ..... 33
  - 5.2 Protecting Cardholder Data ..... 34
    - 5.2.1 Cardholder Data Access ..... 35
    - 5.2.2 Separation and Transfers..... 35
    - 5.2.3 Record Retention and Disposition ..... 36
    - 5.2.4 Restricting Physical Access to Cardholder Data..... 37
  - 5.3 Reconciliations ..... 38
  - 5.4 Recurring Charges ..... 38
  - 5.5 Charge Backs ..... 39
  - 5.6 Monitoring and Security Incident Handling..... 39
- 6. UAB PCI Information Security Standards..... 43
  - 6.1 Build and Maintain a Secure Network ..... 44
  - 6.2 Protect Cardholder Data ..... 47
  - 6.3 Maintain a Vulnerability Management Program ..... 48
  - 6.4 Implement Strong Access Controls ..... 50
  - 6.5 Regularly Monitor and Test Networks ..... 53
  - 6.6 Maintain an Information Security Policy..... 55
- 7. Definitions..... 57
- 8. Acronyms ..... 61
- APPENDIX A - PCI Entity Payment Card Account Request Form..... 63
- APPENDIX B – PCI Entity Payment Card Account Request Workflow ..... 65
- APPENDIX C – PCI Entity Account Agreement ..... 66
- APPENDIX D – Self Assessment Questionnaire Selection..... 67

APPENDIX E – Software Requirements ..... 75

APPENDIX F – Web Hosting Requirements ..... 77

APPENDIX G – PCI Entity Payment Card Process and Procedure Guidelines ..... 79

APPENDIX H – MasterCard Incident Response Requirements ..... 82

APPENDIX I – VISA USA Incident Response Requirements ..... 83

APPENDIX J – Discover Incident Response Requirements ..... 86

APPENDIX K – American Express Incident Response Requirements ..... 87

APPENDIX L – UAB Payment Card Capture Security Procedures ..... 88

*PCI ENTITY HANDBOOK***1. Introduction****1.1. Background**

The Payment Card Industry (PCI) Security Standards Council (SSC) is an open global forum, launched in 2006, that is made up of the major payment card associations (MC, Visa, Amex, Discover, and JCB) and is responsible for the development, management, education, and awareness of the PCI security standards, including: the Data Security Standard (DSS), the Payment Application Data Security Standard (PA-DSS), the Point to Point Encryption (P2PE) Requirements, and the Point of Interaction (POI) Requirements.

The PCI Security Standards Council members have agreed to incorporate the PCI DSS as the mandated set of security standards and technical requirements of each of their data security compliance programs. The PCI DSS were created to offer merchants and service providers a complete, unified approach to safeguarding cardholder data for all payment card brands. The PCI DSS apply to all payment card network members, merchants, and service providers that process, store, or transmit cardholder data, as well as to all methods of payment card processing, whether manual or computerized. Each founding member also recognizes the Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV) certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

The UAB PCI Entity Handbook (Handbook) provides a summary of the University of Alabama at Birmingham requirements for meeting PCI compliance in all activities related to the processing, storing, transmitting, or handling of payment card information. UAB is subject to examination of security measures employed to ensure cardholder data is securely maintained. As such, UAB is committed to adhering to the PCI DSS in order to ensure the protection of cardholder data, limit its liability, and maintain the ability to provide payment card transaction services.

All UAB payment card processing activities and related technologies must comply with this Handbook, the UAB Payment Card Processing and Security Policy, and the PCI DSS in its

entirety. Compliance with card processing activities must be maintained as described herein and in accordance with the policies listed in Section 1.7 Related Policies/Documents of this Handbook. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of this Handbook, the Payment Card Processing and Security Policy, or the PCI DSS. All references to PCI DSS refer to version 3.2.1 of the standard. This Handbook will be updated as new versions of the PCI DSS are released.

## 1.2. Scope / Applicability

This Handbook, in conjunction with the UAB Payment Card Processing and Security Policy, applies to all UAB employees, contractors, consultants, temporaries, vendors, other third party workers, and any unit that processes, stores, maintains, transmits, or handles payment card information in a physical or electronic format on behalf of the UAB enterprise, or in use of the UAB brand name. This includes any entity that utilizes any part of the UAB network infrastructure for payment card transaction services. Hereafter, these groups shall be referred to as “PCI Entities.”

## 1.3 Implementation

The Office of the Chief Financial Officer (CFO) is responsible for governing and enforcing the UAB PCI Compliance Program and approving any changes to the UAB Payment Card Processing and Security Policy or this Handbook. This Handbook and the UAB Payment Card Processing and Security Policy shall be reviewed at least annually and updated as needed to reflect changes to the PCI DSS or the UAB environment. The CFO or their designee shall maintain a register of all approved UAB PCI Entities and shall communicate to those Entities any updates or changes to the PCI standards, this Handbook, or any related UAB policies.

## 1.4 PCI Executive Committee

A PCI Executive Committee has been formed to oversee the formation of a UAB PCI Compliance Program. This committee has representatives from the Office of Financial Affairs & Administration, the Office of Information Technology, and the Hospital Information Security Office. The PCI Executive Committee is responsible for setting policy and providing

high level direction to the PCI Compliance Program. In addition, the Committee provides assistance to UAB PCI Entities in meeting and maintaining compliance requirements directed by the PCI Security Standards Council. The five executive sponsors for this Committee are:

- Mr. Brian D. Burnett, PhD. – Senior Vice President for Finance & Administration
- Ms. Stephanie Mullins – Chief Financial Officer
- Dr. Curt A, Carver, Jr - Vice President Chief Information Officer / CIO
- Mr. Brian Rivers – Associate Vice President Chief Technology Officer (University)
- Mr. Robert Ferrill – Assistant Vice President Chief Information Security Officer (University)

**Note: There is currently no representative on the committee from the Hospital. Robert Ferrill moved from the Hospital to the University and remained on the committee; a Hospital representative has not been named.**

The PCI Executive Committee will be provided with a quarterly progress report and bi-annual oversight meetings will be held.

### 1.5 Handbook Overview

This Handbook is intended to provide UAB PCI Entities, departments, units, and employees with a standard approach to reaching and maintaining compliance with the PCI security standards. This Handbook shall be reviewed and implemented in conjunction with those PCI standards, and is not intended to replace them. This Handbook establishes the standards and procedures for both new and existing UAB PCI Entities, and should assist Entities in establishing and maintaining a secure payment card processing environment.

In addition, UAB has established the [PCI Compliance - Financial Affairs](#) as a central support resource for all PCI Entities. The website contains background information on PCI compliance and instructions for all Entities on completing compliance requirements and submitting required documentation for Entity approval and registration.

## 1.6 Primary UAB PCI Contacts

For questions regarding the requirements for implementing the standards and procedures contained in this Handbook, please visit the [PCI Compliance web site](#), or contact the appropriate UAB PCI primary contacts outlined below.

- Office of Information Technology (IT) and the AskIT Help Desk at 996-5555.
- Enterprise Information Security Office at 975-0842.
- Health System Information Security Help Desk at 934-8888.
- Office of the Chief Financial Officer 934-5121.

## 1.7 Related Policies/Documents

[UAB Acceptable Use of Computer and Network Resources Policy](#)

[UAB Cash Receipts Policy](#)

[UAB Data Protection and Security Policy](#)

[UAB Information Disclosure and Confidentiality Policy](#)

[UAB Payment Card Processing and Security Policy](#)

## 1.8 Sanctions

Employees who do not follow the requirements as outlined in this Handbook, the UAB Payment Card Processing and Security Policy, and all requirements contained within the appropriate unit procedures may be subject to disciplinary action up to and including termination of employment.

UAB PCI Entities who do not follow this Handbook, the UAB Payment Card Processing and Security Policy, and all requirements contained within the appropriate unit procedures may be subject to suspension or loss of payment card processing capability and monetary fines.

Vendors or contractors who do not follow this Handbook, the UAB Payment Card Processing and Security Policy, and any PCI established compliance requirements may be subject to breach of contract penalties.



## 1.9 Payment Card Privacy Statement

Cardholder privacy is important to the University of Alabama at Birmingham (UAB). To better protect the privacy of cardholder data, UAB provides this privacy statement explaining the security and handling practices of cardholder data in the processing of payment card transactions. This privacy statement shall be made available at any point where personally identifiable cardholder data may be requested by a UAB PCI Entity (merchant).

This privacy statement applies to all cardholder data collected by or submitted to a UAB PCI Entity, or on a UAB-maintained website. UAB PCI Entities and UAB websites will only collect personally identifiable information and cardholder data voluntarily provided by cardholders and customers, and will only use that information for the specific purposes for which it was provided. UAB will keep this information strictly confidential, and will not disclose, sell, or lease the information to third parties unless required by law, or with the written permission of the cardholder.

As with most websites used for payment card transaction services, UAB web servers collect web session data used to analyze site trends and gather broad demographic data. UAB reserves the right to collect certain technical information of customers such as operating system, IP address, web browser software, and URL data through the use of cookies or other technology not linked to personally identifiable information or cardholder data.

UAB-maintained websites may have links to other third party sites used for payment card transactions. These third party sites may collect cardholder data and personally identifiable information through the use of forms, cookies, or from the customer's web browser. Cardholders and customers are strongly encouraged to review the privacy policies of all third party websites outside the control of UAB for their procedures for collecting, utilizing, and disclosing cardholder data.

UAB has made significant investment in security measures employed to protect cardholder data under its control. Access to acquired cardholder data and personally identifiable information is limited to only those personnel for whom there is an established business need to access that data.

For questions, comments, or concerns regarding this privacy statement, or UAB procedures for securely processing, storing, or transmitting cardholder data, please contact the AskIT Help Desk at (205) 996-5555. UAB reserves the right to amend this privacy statement at any time, and will post this privacy statement and any updates on the [PCI Compliance web site](#).

#### 1.10 References

Payment Card Industry Security Standards Council web site:

<https://www.pcisecuritystandards.org>.

Payment Card Industry Data Security Standards web site:

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

Navigating the Payment Card Industry Data Security Standards web site:

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_supporting\\_docs.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml)

Payment Card Industry Self-Assessment Questionnaire (SAQ) web site:

[https://www.pcisecuritystandards.org/document\\_library?category=sags#results](https://www.pcisecuritystandards.org/document_library?category=sags#results)

Payment Card Industry Self-Assessment Questionnaire (SAQ) Instructions and Guidelines

web site: [https://www.pcisecuritystandards.org/document\\_library?category=sags#results](https://www.pcisecuritystandards.org/document_library?category=sags#results)

Payment Application Data Security Standards (PA-DSS) web site:

[https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

PCI approved Personal Identification Number (PIN) Entry Device (PED) web site:

[https://www.pcisecuritystandards.org/security\\_standards/ped/pedapprovallist.html](https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html)

PCI approved Payment Applications web site:

[https://www.pcisecuritystandards.org/security\\_standards/vpa/vpa\\_approval\\_list.html](https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html).

MasterCard and Visa approved PCI compliant Service Providers web sites:

<http://www.visa.com/splisting/>

SecureTrust portal: <https://portal.securetrust.com>.

**This Page Intentionally Left Blank**

## 2. PCI Entity Approval and Registration Procedures

Each UAB PCI Entity must be approved by, and registered with, the Office of the Chief Financial Officer (CFO) to receive and operate a payment card account. The UAB CFO's office has been designated as the administrative focal point for handling the PCI Entity approval and registration process, which includes successful completion of the steps outlined in the procedures of this chapter.

In addition, the payment card associations (Visa, MasterCard, etc.) have mandated compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) for any UAB PCI Entity that transmits, stores, or processes cardholder information. This requires that each Entity be certified to be in compliance with the PCI DSS in order to be approved by the CFO's office to begin accepting payment cards.

The standards and procedures in this chapter are intended to assist new UAB PCI Entities in accomplishing the approval and registration process, and meeting the PCI compliance requirements for new Entities. Existing UAB PCI Entities granted payment card processing authorization should review the procedures in this chapter and complete all established requirements not previously required in order to meet newly issued PCI compliance standards.

### 2.1 Pre-requisites to Requesting a UAB Payment Card Account

With the PCI Security Standards Council rules for security and the risks associated with accepting payment cards, requesting a new UAB payment card account should not be done without a full understanding of the responsibilities and alternatives.

- Review information in this Handbook and the PCI Self-Assessment Questionnaires and evaluate whether your business need warrants the effort and cost required to obtain and maintain a payment card account.<sup>1</sup> See Appendix D – Self Assessment Questionnaire Selection for assistance in evaluating the requirements for each SAQ level.
- Discuss objectives with the CFO's office and Enterprise Information Security to review and determine other payment alternatives that might better suit your business need.

---

<sup>1</sup> PCI Self Assessment Questionnaires can be obtained at:

[https://www.pcisecuritystandards.org/document\\_library?category=sags#results](https://www.pcisecuritystandards.org/document_library?category=sags#results).

New PCI Entities must review the PCI standards, this Handbook, and the related UAB policies to understand the commitment of resources required before requesting a payment card account. Existing PCI Entities must be prepared to annually validate compliance with the PCI standards and UAB policies and procedures.

## 2.2 Requesting a UAB Payment Card Account

After reviewing the above pre-requisites, those Entities that wish to process payment cards as a requirement of their business process are required to contact the CFO's office to initiate the process to obtain a UAB PCI Entity payment card account. The CFO's office will provide requesting Entities with an Entity Payment Card Account Request Form. A template of the PCI Entity Payment Card Account Request Form is included as Appendix A and is available on the [PCI Compliance web site](#).

Entity Payment Card Account requests must be approved by the Entity Department Head and Dean/Associate Vice President, or their designee and should contain the following information in order to complete the request:

- Contact Information (name, address, phone and email) for:
  - Department or business owner.
  - Primary Department or business contact.
  - Backup Department or business contact.
  - Technical contact (Required for all Entities except dial-up only terminals).
  - Person responsible for posting payment card activities and resolving reconciliations.
- Purpose for requesting the payment card account.
- Your business case accepting payment cards. Please include who your customers will be and the impact to your organization if you can't accept payment cards.
- How payment cards will be accepted (card present, over the phone, via fax or web); please indicate all methods of acceptance.
- What type of payment cards you wish to process (e.g. MC/Visa/Discover/AMEX).

- What type of transactions you wish to process (e.g. services provided, admission fees, conference attendance, fines, etc.).
- The target date to be functionally operational.
- The DBA (doing business as) name of the new account.
- Oracle account number to charge the cost of necessary equipment.
- Oracle account number to charge monthly Entity fees (if different).

If payment card terminals will be used (See Chapter 3):

- Quantity of terminals.

If a payment application / Point of Sale (POS) system will be used (See Chapter 3):

- Manufacturer, product name, and version of the payment application or POS.
- Whether authorizations will be done via dial-up or over the Internet.
- Where the POS application will be hosted.
- Whether wireless technology will be used (Wireless technology use must be preapproved by Enterprise Information Security).
- Payment applications and POS systems must meet approved PCI PA-DSS requirements.

If a hosted service provider/web based (See Chapter 3):

- Provide the name of the service provider to be used.
- Locally developed applications are recommended to use TouchNet, and must meet the same criteria as PCI approved payment applications.
- If using a hosted service provider, see the section on service providers in Chapter 3. Use of service providers other than TouchNet must be approved by Enterprise Information Security and must meet the requirements of Appendix E – Software Requirements, and Appendix F – Web Hosting Requirements.

### 2.3 Certification of Compliance Requirements

In order to achieve certification of compliance and CFO office approval, all UAB PCI Entities are required to pass an evaluation of their internal systems and processes. New or existing PCI Entities that wish to start or maintain payment card processing services must be able to document compliance by completing a Self-Assessment Questionnaire (SAQ) that is appropriate for the manner in which they wish to acquire, process, transmit and store payment card data. The appropriate validation type for each Entity is determined according to the following guidelines:<sup>2</sup>

- **SAQ A** – Card-not-present merchants; all cardholder data functions are outsourced.
- **SAQ A-EP** – E-commerce merchants who outsource all payment processing to PCI DSS validated third parties. Websites do not directly receive cardholder data with no electronic storage, processing or transmission of any cardholder data.
- **SAQ B** – Imprint-only or stand-alone dial-up terminal merchants with no electronic cardholder data storage.
- **SAQ B-IP** - Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.
- **SAQ C-VT** - Web-Based Virtual Terminals, No Electronic Cardholder Data Storage.
- **SAQ C** – Merchants with payment application systems connected to the Internet with no electronic cardholder data storage.
- **SAQ P2PE-HW** - Hardware payment terminals included in a PCI SSC-listed, validated, P2PE solution with no electronic cardholder data storage.
- **SAQ D for Merchants** - All merchants not included in descriptions for the above SAQ types.
- **SAQ D for Service Providers** - All service providers defined by a payment brand as eligible to complete a SAQ.

Each PCI Entity will receive a compliance certificate once they have completed and passed the following requirements:<sup>3</sup>

---

<sup>2</sup> See Appendix D – Self Assessment Questionnaire Selection for assistance in evaluating the requirements for each SAQ level.

<sup>3</sup> See Section 2.7 and 4.1 for additional information on SecureTrust / TrustWave portal.

- The completion of an annual Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC) provided on-line by SecureTrust / TrustWave, a certified PCI vendor. This questionnaire provides a means for assessing an Entity's compliance to PCI standards.
- Successful completion of remote network vulnerability monthly scans of all outward facing IP addresses on the same subnet as computers dealing with payment cards (for SAQ-C and SAQ-D Entities Only) by SecureTrust / TrustWave, a PCI Approved Scanning Vendor (ASV).
- Submission of the SAQ, evidence of a passing scan (where applicable), and the Attestation of Compliance, along with any other requested documentation.

#### 2.4 Security Awareness Training

The Office of the Chief Financial Officer (CFO) is responsible for overseeing and enforcing a formal security awareness training program in order to educate PCI Entities of the importance of cardholder data security. PCI security awareness training shall be completed by all Entity members upon hire, or as part of PCI Entity approval and registration, and at least annually thereafter. This training is mandatory for all UAB PCI Entity members.

PCI security awareness training may be accessed on the UAB Campus Learning web site at [uab.edu/adminsys/](http://uab.edu/adminsys/). This training offers guidance on local and University-wide payment card policies and procedures regarding the proper handling of cardholder data, and on PCI compliance. Upon accessing the UAB Campus Learning System site, you will be required to log in using your Blazer ID and password. All PCI Entity members should be pre-registered to take the PCI security awareness training. If you are unable to access this training, please contact the CFO office to be registered.

#### 2.5 UAB PCI Entity Account Agreement

All new or existing PCI Entity members must sign or acknowledge the PCI Entity Account Agreement as part of requesting or maintaining a payment card account. Each Entity will be provided with a link to the UAB Cash Receipts Policy, the UAB Payment Card Processing and Security Policy, and the PCI Data Security Standards (See Section 1.7 and 1.10). Signing or acknowledgement of this agreement confirms that the Entity members have read and understand these policies and standards, and that they will maintain compliance with them. The PCI Entity Account Agreement shall be acknowledged and renewed annually by the members and management of each Entity by completing PCI Security



Awareness Training (See Section 2.4). A template of the agreement is included as Appendix C in this Handbook for reference.

## 2.6 Background Checks

The appropriate PCI Entity Human Resources (HR) department is responsible for ensuring applicable background checks are conducted prior to hire for all new Entity employees, transfers, and temporary workers for positions with an established business need to access cardholder data or payment card processing systems. Examples of applicable background checks include verification of previous employment history, criminal records checks, credit history, and reference checks.

PCI Entities must have local procedures that define which positions are subject to background checks. For 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, this requirement is a recommendation only. PCI Entities should inform their local HR department of which positions require background checks, and include in those positions' job descriptions the need for background checks.

## 2.7 Required Entity Documentation

It is the responsibility of PCI Entity management to maintain accurate records of all required Entity compliance documentation and to ensure the annual review of that documentation is completed. The CFO's office will provide PCI forms to the merchant contact during the PCI Entity's annual PCI compliance renewal month. The [PCI Compliance web site](#) also contains all of the necessary procedures for completing required Entity documentation that includes, but is not limited to, human resources documentation, technical documentation, network diagrams, Entity business process and procedures, SAQ type and completion status, and security awareness training completion status.

## 2.8 New Account Setup Summary

The following procedures provide a summary of the UAB PCI Entity approval and registration process, as well as the initial PCI compliance certification requirements for new Entities.<sup>4</sup> In order to receive a PCI Entity payment card account and be authorized to accept payment cards, requesting Entities will be responsible for completing all of the items in the following list. Depending on the complexity

---

<sup>4</sup> See Appendix B – PCI Entity Payment Card Account Request Workflow.

of each Entity card processing environment, the set up process can take a number of weeks. The time required may be based on the level of compliance required for the Entity card processing environment, the number of third parties involved, or other factors. Requests for new accounts should be made early enough to allow for sufficient time to achieve compliance.

1. Contact the CFO's office to request the PCI Entity Payment Card Account Request Form. Complete the form and have it reviewed and signed by the Entity Department Head and Dean/Associate Vice President. Additional instructions for completing the Account Request Form can be found on the [PCI Compliance web site](#). Submit completed and signed form to CFO's office for review and approval.
2. The CFO's office will submit request form to Fiserv (Formerly First Data) (the payment processor for Compass Bank, UAB's acquiring bank) and Compass Bank, and notify Entity when approval has been received. If the entity will use a swipe terminal, an order for a terminal is included in the account request.
3. When established, Fiserv (Formerly First Data) will notify the CFO's office of the new merchant account number, indicating the Entity can begin processing payments, and the CFO's office will notify the Entity.
4. If the new merchant is accepting payments on-line, the CFO's office will submit a Service Now Request ticket for UAB IT to assist the Entity with TouchNet set up. The CFO's office provide the Entity with the contact name in the Controller's office who will explain the depositing process, and assist the Entity with accessing TouchNet and completing and submitting deposit forms.
5. If the new merchant is using a swipe terminal, the CFO's office will notify the Entity when the terminal arrives and set up a time to deliver the terminal and explain how to operate the terminal and the depositing process.
6. Meet with CFO's office after verification that the account has been approved and set up by Fiserv (Formerly First Data) and the bank. The purpose of the meeting is to explain the requirements of PCI compliance, the Entity's responsibilities for PCI compliance, information concerning the online PCI training course, and gather information regarding the business process for the merchant account.

7. Complete the online PCI training course (See Sections 2.4 and 4.5). The Entity is responsible for listing all individuals who will need to complete the PCI training on the Cardholder Data Flow and Fact Sheet form; and for notifying the CFO's office when new individuals are hired and need to complete the training. The CFO's office is responsible for sending the assignment list to Financial Affairs Training; they in turn, will assign the course. The CFO's office will monitor the PCI training course and verifying completion of the course by each individual assigned.
8. The CFO's office will create a merchant account in the SecureTrust / TrustWave portal, using the Merchant ID information provided by First Data and the bank. The individual in the Entity who will be responsible for completing the SAQ and PCI documents will be designated on the account.
9. Log on to the SecureTrust portal (SecureTrust will send link when account is setup) and complete the account registration information within three (3) business days from the time the email and link are received from SecureTrust.
10. Log on to the SecureTrust portal and complete the on-line Self-Assessment Questionnaire (SAQ) within five (5) business days from time the email and link are received from SecureTrust. If applicable, identify systems that need to be included in monthly scans and successfully pass the first scan before accepting payment cards. For help in completing the SAQ contact the CFO's office at 975-5207.
11. Note: the registration and SAQ can be done at the same time.
12. The CFO's office will log on to the SecureTrust portal, access the merchant account, review the updated information provided by the merchant contact and the completed SAQ. The SAQ and PCI Certificate (which includes the completion date and name of the person completing the SAQ), along with the AOC Report for the account, will be saved and uploaded to the merchant account's folder in the PCI Compliance web site Merchant Library.
13. The CFO's office will send the required PCI documents for completion to the contact person for the merchant account. The completed forms are to be returned to the CFO's office via email within five (5) business days. The CFO's office will review the forms and upload them to the merchant account's folder in the PCI Compliance web site Merchant Library.
14. Based on information gathered during the initial meeting between the merchant account contact and the CFO's office, the CFO's office will prepare a draft of the business process for the account regarding processing payment card transactions.

15. The draft will be emailed to the merchant account contact for review, and revisions if necessary, then sent back to the CFO's office. Once the draft is final the CFO's office will send a final copy to be signed and dated by the merchant account contact and returned. The CFO's office will upload the final signed copy to the merchant's folder in the PCI Compliance web site Merchant Library.
16. Contact the CFO's office for any additional assistance on use of terminals, or the AskIT Help Desk for assistance on the setup and use of the TouchNet gateway. Training for payment applications should be requested through your application provider.

### 3. PCI Entity Payment Card Processing Environments

This chapter provides an overview of the various payment card processing environments and transactions types in scope of the Payment Card Industry (PCI) Data Security Standards (DSS) and available to UAB PCI Entities. The requirements and recommendations provided in this chapter should be considered when selecting, implementing, and maintaining Entity card processing environments. These requirements and recommendations are based on the PCI standards for securing cardholder data developed and maintained by the PCI Security Standards Council.

The following is a description of the three types of transactions in scope of the PCI DSS:

- *In-Person Transactions* are those transactions completed while the payer is present. This type of payment can be initiated through a card swipe or by a cashier that manually enters the payment card data.
- *Phoned-In Transactions* are those transactions completed when a payer phones in and provides payment card data.
- *Back Office Transactions* are those transactions initiated by a payer who mails a payment to the school / department.

#### 3.1 Payment Card Processing Types

##### 3.1.1 Terminals

Terminals are standalone card swipe machines that are issued by the bank and are traditionally used over analog dial-up telephone lines. Terminals come with set-up instructions and a customer service number, or you may contact the CFO's office with any questions.

If the payment card terminals will be used to process authorizations and/or settlements via the Internet instead of via dial-up phone lines, they will be treated as point of sale systems for compliance purposes. This will mean the Entity must complete the SAQ that is applicable to point of sale systems.

##### 3.1.2 PIN Entry Devices (PED)

Personal identification number (PIN) entry devices are those devices that allow a purchaser to enter a secret numeric password known only to the user for authentication. The PCI Security

Standards Council has assumed responsibility of PED security requirements with the overall objective of protecting the cardholder's PIN during financial transactions. Authorizations to use PEDs must be approved through the established UAB contract review process, and must be for PCI approved PIN Entry Devices.

For a listing of PCI approved PEDs, see:

[https://www.pcisecuritystandards.org/security\\_standards/ped/pedapprovallist.html](https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html)

### 3.1.3 Point to Point Encryption (P2PE)

A point-to-point encryption (P2PE) solution is provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment.

A PCI P2PE solution must include all of the following:

- Secure encryption of payment card data at the point-of-interaction (POI)
- P2PE - validated application(s) at the point-of-interaction
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

Any PCI Entity that plans to use a P2PE solution for payment card related services must use a vendor or third party provider that is a PCI Validated P2PE Solution and PCI Validated P2PE Application to be eligible to complete the SAQ P2PE-HW.

### 3.1.4 Payment Applications

Payment applications include all purchased and custom software programs or groups of programs, including internal and external applications, such as web applications that are used at the point of sale (POS). In most cases, software vendors develop payment applications that

store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (Entities).

Any PCI Entity that plans to use a payment application for payment card related services must use a vendor or third party application that is a PCI Validated Payment Application that meets the Payment Application Data Security Standard (PA-DSS) requirements. Authorizations to use payment applications must be approved through the established UAB contract review process. Enterprise Information Security will verify that the payment application being requested for use is validated to be compliant with the PCI PA-DSS. Payment applications that do not meet PA-DSS requirements cannot be used. Any use of payment applications that have not been validated by PCI must be approved through the exception process outlined in Appendix E – Software Requirements.

For a listing of PCI approved payment applications, see:

[https://www.pcisecuritystandards.org/security\\_standards/vpa/vpa\\_approval\\_list.html](https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html).

Enterprise Information Security will also review the implementation of the application to ensure that it meets all UAB information security requirements. PCI Entity management is responsible for providing all information regarding the manufacturer, product name, and version number of the software, as well as validation of PCI PA-DSS compliance in any contracts for review.

Mixed Use Workstations are only allowed within the UAB cardholder data environment when certified point-to-point encryption (P2PE) hardware is used. A mixed use workstation is where a payment application would be used on workstations that would also be used for standard office applications (email, web browsing, etc.).

If a PCI Entity decides to change to a different application, the same requirements described above will apply to the new application. Changes do not include upgrading to a new release of software already exempted, which are covered in Section 4.4 – Change Control.

### 3.1.5 Web Hosting

Web site hosting service providers offer various services to PCI Entities that range from shared server space to various “shopping cart” options, and may include payment applications and/or

connections to payment gateways and processors. Websites that are used to store, transmit or process payment card account numbers must comply with the PCI DSS and UAB requirements in Appendix F – Web Hosting Requirements.

- PCI Entities that utilize UAB hosted sites must have their hosting location evaluated by Enterprise Information Security before being placed in production and must have network penetration tests conducted at least annually.<sup>5</sup> Any costs associated with network penetration tests are the responsibility of the Entity.
- PCI Entities that utilize third party service provider hosted sites, or sites that redirect payment card acceptance or storage, must contractually obligate those service providers to maintain compliance with the PCI DSS and UAB requirements at all times, and have their systems scanned by an authorized assessor at least quarterly.

### 3.1.6 Virtual Terminals

Internet gateways provide ways for you to enter transactions directly through your web browser, which allows you to process manual transactions without having a physical payment card terminal. This is considered a virtual terminal. If your business process includes the use of this feature, the workstations are within PCI scope, must be single use and must comply with all applicable PCI DSS requirements.

### 3.1.7 Service Providers

A service provider is any third party that stores, transmits or processes payment card numbers on behalf of a PCI Entity. Service providers may offer payment card transaction services through various means, such as PEDs, payment applications, web applications and site hosting, and virtual terminals. Service providers must be contractually obligated to keep their systems and process in compliance with PCI requirements at all times. UAB offers payment card transaction services through the PCI approved TouchNet service provider.

Authorizations to use a service provider other than TouchNet shall be approved through the established UAB contract review process. Enterprise Information Security will verify that the service provider being requested for use is validated to be a PCI compliant service provider.

---

<sup>5</sup> See Section 4.3. - Network Penetration Tests



Approvals for the use of service providers will only be granted for PCI approved service providers.

A list of compliant service providers is maintained by both MasterCard and Visa at: <http://www.visa.com/splisting/>

### 3.2 TouchNet Marketplace (UAB Provided Service)

UAB PCI Entities that wish to process or accept payment card transactions over the Internet are encouraged to use the UAB service provider, TouchNet Marketplace. TouchNet Marketplace is a comprehensive framework for enterprise-wide eCommerce used by campus departments and organizations to create, manage, and operate online storefronts and compliant payment systems for campus-developed web applications and other third party business software. Marketplace helps centralize control of eCommerce finances and technology while distributing management and operations of those sites to authorized campus Entities. TouchNet Marketplace offers two modules:

- **uStore** – Provides Entities with the infrastructure for online malls, storefronts, registration sites, and shopping cart applications.
- **uPay** – Provides Entities with the ability to remove payment processing from existing campus web-based business applications and move them to a central, secure payment application for greater transaction security and easier compliance reporting.

For additional information on TouchNet Marketplace and the set up requirements for the service, contact the AskIT Help Desk at [askit@uab.edu](mailto:askit@uab.edu) or call 966-5555. Exceptions to this recommendation are outlined in Appendix E – Software Requirements, and Appendix F – Web Hosting Requirements.

### 3.3 Fraud Prevention

Card-not-present transactions are those in which the card and cardholder are not present at the point of sale, which may include orders placed by Internet, phone, mail, or fax. PCI Entities that accept card-not-present transactions must take measures to verify the card's legitimacy.

- Ask the customer for the card expiration date, and include it in your authorization request. An invalid or missing expiration date might indicate that the customer does not have the actual card in hand.

- Use fraud prevention tools, such as Visa’s Address Verification Service (AVS), Card Verification Value (CVV/CVV2), and Verified by Visa (VbV) fraud prevention services.
  - **AVS** - Allows card-not-present Entities to check a Visa cardholder’s billing address with the card issuer. The Entity includes an AVS request as part of the authorization and receives a result code indicating whether the address given by the cardholder matches the address on file with the issuer.
  - **CVV/CVV2** - Is a three-digit number imprinted on the signature panel to help card-not-present Entities verify that the customer has a legitimate card in hand at the time of the order. The Entity processor asks the customer for the CVV/CVV2 code and then sends it to the card issuer as part of the authorization request. The card issuer checks the CVV/CVV2 code to determine its validity, then sends a CVV/CVV2 result back to the Entity along with the authorization. CVV/CVV2 is required on all Visa cards. To protect CVV/CVV2 data from being compromised, **PCI Entities are prohibited from keeping or storing CVV/CVV2 numbers in any form once a transaction has been completed.**
  - **VbV** – Enables e-commerce Entities to validate a cardholder's ownership of an account in real-time during an online Visa card transaction. When the cardholder clicks "buy" at the checkout of a participating Entity or service provider, the processing server recognizes the registered Visa card and the “Verified by Visa” screen automatically appears on the cardholder’s desktop. The cardholder enters a password to verify his or her identity and the Visa card. The issuer then confirms the cardholder’s identity.

**This Page Intentionally Left Blank**

## 4. PCI Entity Compliance

The procedures in this chapter are intended to assist existing UAB PCI Entities in maintaining annual Payment Card Industry (PCI) compliance requirements. See Chapter 2 for approval, registration, and compliance requirements for new PCI Entities. Existing UAB PCI Entities granted payment card processing authorization should review the procedures in this chapter and complete all established requirements not previously required in order to meet newly issued PCI compliance standards.

Compliance with the PCI Data Security Standards (DSS) is mandated for all UAB PCI Entities that transmit, store, or process cardholder information. Each Entity must be initially certified to be in compliance with the PCI DSS in order to start accepting payment cards, and must maintain their compliance by fulfilling monthly, quarterly and annual compliance requirements. The CFO's office is responsible for deactivating any Entity bank account if the Entity does not reach or maintain PCI compliance certification, and will notify the Department Head and Dean or Associate Vice President to initiate remediation of any non-compliant Entities and document corrective actions.

### 4.1 TrustWave and the SecureTrust Portal

UAB has contracted with TrustWave to provide annual compliance certification and monthly vulnerability scans. TrustWave is a PCI Approved Scanning Vendor (ASV) that provides the SecureTrust portal for PCI Entities to achieve their initial and annual compliance certification. The CFO's office will request the setup of a login to the SecureTrust portal for all new PCI Entities, as outlined in Chapter 2. Existing PCI Entities must access their established SecureTrust account in order to fulfill annual compliance certification requirements, which include completing the appropriate Self-Assessment Questionnaire (SAQ) and scheduling a remote scan of their URL or IP address(es), where applicable.

- Entities can log into their SecureTrust account in the SecureTrust portal at <https://portal.securetrust.com/#/>.
- PCI Entities are required to complete the appropriate SAQ online using the SecureTrust portal account. For Entities that have dedicated technical support staff, ensure they have their own login ID to the portal account as well.

- PCI Entities that accept or process payment cards online must also enter scan parameters (IP addresses or URLs) for systems that fall in scope for PCI compliance. IP addresses to be scanned should be a UAB address. If your web-site is hosted by a third party, you should contractually obligate the third party to be PCI compliant and to have their systems scanned by an authorized assessor at least quarterly.
  - PCI Entities using TouchNet’s payment application must have the web server scanned that performs the redirect to the TouchNet site.
  - PCI Entities that accept cards in some other way must scan all outward facing IP addresses on the same subnet as the system(s) that stores, processes, or transmits payment card data.

For help using the SecureTrust portal, contact the CFO’s office.

#### 4.2 Monthly Scans

The PCI DSS require that internal or external network vulnerability scans for UAB PCI Entities be conducted on at least a quarterly basis and after any significant change in the Entity card processing environment, such as new system component installations, changes in network topology, firewall rule modifications, or product upgrades. UAB will employ monthly scanning procedures to ensure passing results are obtained in a timely manner. After monthly scans have been completed, Enterprise Information Security will notify Entity management of any scan failures and their associated vulnerabilities. Entity management must acknowledge receipt of monthly scan results from Enterprise Information Security within 2 business days. If acknowledgement is not received within 7 business days, Enterprise Information Security will escalate the issue with the Department Head and Dean or Associate Vice President and contact the CFO’s office.

Addressing the results of monthly scan reports:

- Entity management is responsible for evaluating and mitigating all information warnings in the monthly scan report to ensure their system(s) is not at risk.
- If the scan indicates any high risk vulnerabilities, those vulnerabilities must be immediately corrected. Contact Enterprise Information Security to determine if you have sufficient compensating controls to continue accepting payment cards while you correct the problem.

If it is determined by Enterprise Information Security that the vulnerabilities represent an unacceptable risk, the system must be immediately removed from the network and any access to the Internet will be disabled until the issue is resolved. If the issue or vulnerability is not corrected within 30 days, the CFO's office will be notified and the account will be deactivated.

- PCI Entities must review all medium and low risk findings and correct those vulnerabilities within 90 days. Entity management and/or their technical support staff must confirm that these medium/low risk findings do not represent a risk to the system or the UAB network. Entities must work with their IT or administrative staff, Enterprise Information Security, or other necessary departments on remediation of medium and low risk vulnerabilities as part of their ongoing maintenance plans so that these issues can be fixed before they become high risks.
- Develop and document planned steps for correcting within 30 days any identified high risk vulnerabilities, or 90 days for any identified medium and low risk vulnerabilities. The planned steps for remediation should include a list of the vulnerabilities to be corrected, how they will be corrected, who is responsible for implementing the corrections, and the proposed timeline for completing those corrections. The plan for remediation must be sent to the Enterprise Information Security within 7 business days of the scan failure.
- If it is determined that high risk vulnerabilities will not be remediated within 30 days of the scan, the CFO's office should be contacted immediately to discuss possible alternatives.

PCI Entities will not be allowed to continue processing payment cards in a non-compliant high risk state past the 30 days. Entities may be allowed a temporary suspension without deactivating their account in the following conditions:

- The Entity has deactivated or taken their web site/page off line
- The Entity has submitted planned steps for remediation within 7 business days of the scan or penetration test
- The Entity has diligently and continuously worked on resolution(s) to the vulnerabilities

- Enterprise Information Security agrees that the tasks on the proposed plan will remediate the vulnerabilities and that the Entity has proposed reasonable time estimates for remediation, and
- The Department Head and Dean/Associate Vice President for the Entity supports the request for the extension.

In any other circumstance, the out-of-compliance account will be deactivated by the CFO's office at the end of 30 days, or before if it is determined that the Entity will not be able to meet compliance within the 30 day requirement.

If a PCI Entity account is deactivated, Entity management will need to re-apply for a new Entity account after the Entity has taken steps to become compliant. No request for acceleration of this process will be accepted for Entities in this category.

If PCI Entity management believes any vulnerabilities identified in monthly scans are in error, Entity management may discuss the findings with Enterprise Information Security. Enterprise Information Security will work with UAB's external assessor, TrustWave, to confirm the validity of the vulnerability. If TrustWave agrees with the justification for the appeal, they will not flag it as a vulnerability in future scan results and will reissue a corrected vulnerability report.

### 4.3 Network Penetration Tests

The PCI DSS require that network penetration tests be performed at least annually for all applicable UAB PCI Entities, which includes those Entities that accept payment card numbers directly on their web site or that store payment card account numbers on a back-end server.<sup>6</sup> If an Entity requires a penetration test, as outlined within Section 11 of the DSS, the Entity is responsible for the cost of such a test. Enterprise Information Security will arrange for TrustWave or an approved third party penetration tester to conduct tests for UAB PCI Entities annually. The Entity may also contract with an approved third party assessor to have the test completed. If contracting with a third party assessor, all test results must be submitted to Enterprise Information Security within 2 business days of the completion of the test.

---

<sup>6</sup> See also Chapter 6 – PCI Entity Information Security Standards

Addressing the results of annual penetration test reports:

- Enterprise Information Security will receive a copy of the penetration test report when the test has been completed and will contact the Entity management to discuss any test failures or vulnerabilities
- Entity management must acknowledge receipt of annual penetration test results with Enterprise Information Security within 2 business days. If acknowledgement is not received within 7 business days, Enterprise Information Security will escalate the issue with the Department Head and Dean or Associate Vice President and contact the CFO's office.
- Entity management is responsible for correcting any deficiencies identified during annual penetration tests.

High risk vulnerabilities must be corrected within 30 days and medium and low risk vulnerabilities must be corrected within 90 days. Entities must submit a report of the planned steps for remediation of high risk vulnerabilities to Enterprise Information Security within 7 business days and must notify Enterprise Information Security when the deficiencies have been corrected. After the Entity has corrected the noted deficiencies, Enterprise Information Security will schedule a second test to be conducted to specifically test for the vulnerabilities previously identified. The cost of follow up testing is the responsibility of the Entity.

PCI Entities are also required to have penetration tests performed after any significant changes are made to the Entity card processing environment, such as operating system upgrades, new sub-net installations, or new web-server implementations. The costs for these additional tests are the responsibility of the Entity. The Entity may contract with a third party assessor to conduct the test, or may contact Enterprise Information Security to arrange for the test. Significant changes to the Entity card processing environment also require Enterprise Information Security review and approval prior to implementation.

#### 4.4 Change Control (Technical)

Applicable PCI Entities are responsible for documenting and maintaining change control procedures that describe the process of how technical changes to your payment card processing environment are managed. Include in the procedures those individuals authorized to make changes, who can



approve them, what functionality testing will take place, back-out procedures and what the customer impact is for the change. Changes should be tested in a test environment prior to being placed in production. Change control procedures should also outline steps for implementing new releases and patches supplied by vendors, back out procedures for changes, and notifications to the CFO's office and Enterprise Information Security for changes in roles, vendors, and IT equipment in scope for PCI compliance.

Planned implementations of any significant change in the PCI Entity's information technology or web environment (e.g., new systems component installations, changes in network topology, firewall rule modifications, product upgrades) shall warrant performing the following tasks:

- Request approval of the planned changes from the CFO's office and Enterprise Information Security
- Re-evaluate the appropriate Self-Assessment Questionnaire
- Perform functional tests on the card processing environment before placing systems in production
- Verify firewall rules are still effective, and
- Have a directed remote vulnerability scan performed.

Requests for significant changes to the PCI Entity card processing environment should be signed by the Department Head and submitted by the Entity management or technical contacts to the CFO's office and Enterprise Information Security for approval. Upon completion of a significant change, all relevant PCI DSS requirements must be implemented, documented and tested.

#### 4.5 Security Awareness Training

The Office of the Chief Financial Officer is responsible for overseeing and enforcing a formal security awareness training program in order to educate PCI Entities of the importance of cardholder data security. PCI security awareness training shall be completed by all Entity members upon hire or transfer, or as part of PCI Entity approval and registration, and at least annually thereafter. This training is mandatory for all UAB PCI Entity members.

PCI security awareness training may be accessed on the UAB Campus Learning web site at [uab.edu/adminsys/](http://uab.edu/adminsys/). Upon accessing the UAB Campus Learning System site, you will be required to log in using your Blazer ID and password. All PCI Entity members should be pre-registered to take the PCI Security Awareness Training. If you are unable to access this training, please contact the CFO's office to be registered.

This training offers guidance on local and University-wide data security policies and payment card procedures regarding the proper handling of cardholder data, and on PCI compliance. The program will utilize multiple methods of communicating awareness and educating personnel such as posters, memos, web-based trainings, meetings and promotions. All PCI Entity members must also acknowledge in writing or electronically that they have read and understand the information security policy.

As a part of the security awareness training program, UAB will provide appropriate role based security training for personnel that support the PCI Entities. Training will vary based on role and level of access within cardholder data environment.

- Training in secure coding techniques for developers (6.5)
- Security training specific to area of support- server, network, etc. (12.6.1)
- Security breach response responsibilities for response team members (12.10.4)

#### 4.6 Annual Re-Certification Summary

The following procedures provide a summary of the annual PCI compliance requirements. PCI Entity compliance with the PCI DSS must be validated annually and in the event of any significant change in the Entity card processing environment. UAB must report PCI compliance with its payment card processing activities; therefore, all PCI Entities must complete the requirements in the following list by the Entity approval and registration date of each year, and provide all necessary documentation to the CFO's office in a timely manner to receive certification of compliance:<sup>7</sup>

- The CFO's office will email the individual responsible for annual re-certification of the merchant account. Emails for each account will be sent during the first week of the month

---

<sup>7</sup> For more information, see the PCI standards: <https://www.pcisecuritystandards.org/>

that the account is scheduled for renewal. The email will contain instructions for accessing SecureTrust / TrustWave for the SAQ renewal, all of the required PCI forms to be completed, as well as information to complete the forms, and a draft of the business process for review, and updates by the Entity if needed.

- Log on to the SecureTrust portal annually and complete the appropriate SAQ and Attestation of Compliance prior to the annual deadline. Failure to complete the questionnaire successfully will result in the Entity account being deactivated.
- Complete the PCI documents, including review and updating the draft of the business process, and email back to CFO's office. The CFO's office will send a final copy of the business process to the Entity for signature; when returned it will be uploaded to the Entity's account in the Merchant Library along with the other PCI documents.
- For those Entities required to have monthly scans completed, review scan parameters to ensure they are correct.
- Successfully pass monthly network vulnerability scans performed remotely by a PCI Approved Scanning Vendor (TrustWave).
- Successfully pass an annual network penetration test performed internally or externally by an approved tester.
- PCI Entity management, members, and technical support staff must complete PCI security awareness training and acknowledge the PCI Entity Account Agreement upon hire or transfer, and annually thereafter. (Entities that only have dial-up terminals are not required to have technical contacts complete the training.).

#### 4.7 Compliance Certification Exception Process

Any exception to the standards and procedures outlined within this Handbook or the UAB Payment Card Processing and Security Policy must be requested in writing in advance and approved by the Office of the Chief Financial Officer (CFO) and the Office of the Vice President for Information Technology (OVPIT).

In cases where the PCI Entity cannot meet the institutional requirements exactly as written, complete an [Information Security Exception Request Form](#) on the IT Policies & Compliance webpage – which includes:

- Document which standard cannot be met as stated, why it cannot be met, and what additional or alternative controls will be put in place to achieve the spirit of the requirement and send the document to the CFO's office.
- The CFO's office and OVPIT office will review and approve the request.
- Enterprise Information Security will seek guidance and coordinate review of the exception request with UAB's PCI compliance assessors and will determine if the additional controls represent compliance.

Exceptions are valid for a one-year period. Annually, the Enterprise Information Security group will send a copy of approved exceptions back to the requestor and the PCI Entity point of contact, who must determine whether the conditions that justified the original exceptions are still in effect. If necessary a new request for exception must be submitted, reviewed and approved.

It should be noted that granting an exception does not reduce the University's exposure to a compromising event or breach. This process should only be pursued where achieving compliance is technically not feasible and the alternative of not accepting payment cards prevents the Entity from meeting its intended mission.

## 5. PCI Entity Responsibilities

### 5.1 Business Process and Procedures

Each UAB PCI Entity must develop, implement, and maintain local business process and procedures for conducting secure payment card transaction related activities in accordance with the Payment Card Industry (PCI) Data Security Standards (DSS) and other applicable UAB policies referenced in the Related Policies/Documents section of this Handbook. See Appendix G – PCI Entity Payment Card Process and Procedure Guidelines for guidance on Entity process and procedure development. At a minimum, PCI Entity procedures should address the following areas:

- Authorization of transactions
- Separation of duties
- Data access
- Record retention
- Physical security
- Reconciliations
- Recurring charges
- Charge backs
- Background checks
- Training

In addition, there may be local processes involved with Entity payment card processing that are not included in these general procedures. Entity procedures must be documented locally, and a copy of the documentation must be maintained in the Entity Merchant Library on the [PCI Compliance web site](#).

PCI Entity senior management shall review their procedures developed to meet PCI DSS requirements at least annually and update those as needed to reflect changes to PCI DSS or their

card processing environment. Entity senior management is responsible for ensuring all cardholder data is protected against unauthorized use, disclosure, fraud, or other compromising activity.

PCI Entity members must be familiar with local business process and procedures, and shall review them, as well as those outlined in the PCI Entity Account Agreement, at least annually. Entity members are required to sign/acknowledge the PCI Entity Account Agreement annually, confirming that they have read and understand those policies and that they will comply with them.

## 5.2 Protecting Cardholder Data

**Do not store cardholder data unless it is absolutely necessary.** If it is necessary to store cardholder data, PCI Entities must make every effort to keep cardholder data storage to a minimum, and only retain that data in accordance with Entity, department, school, or unit record retention standards or procedures. Entity data retention and disposal procedures should limit the storage of cardholder data to that which is required for business, legal, and/or regulatory purposes. **Entities must not store sensitive authentication data in any form** after authorization, even if the data is encrypted.

Sensitive authentication data includes:

- Full contents of the magnetic stripe
- Card Verification Code or Card Verification Value (CVC/CVC2/CVV/CVV2/CID)
- Personal Identification Number (PIN) or the encrypted PIN block

In the normal course of business, the following cardholder data elements from the magnetic stripe may need to be retained, but must be protected:

- The cardholder's name
- Primary Account Number (PAN)
- Expiration date
- Service code

To minimize risk, store only these data elements as needed for business purposes. The PAN must be masked to display only the last 4 digits or first 6 digits on any paper-based records or receipts (this requirement does not apply to employees and other parties with a legitimate business need to see

the full PAN). The PAN, at a minimum, must be rendered unreadable by using strong cryptography, one-way hashes, truncation, or index tokens any time it is stored electronically. If disk encryption is used, rather than file or column level database encryption, logical access must be managed independently of native operating system access control mechanisms and decryption keys must not be tied to user accounts. For additional assistance in determining if your systems or applications are currently storing the above named data elements, contact your service provider, Entity technical support or Enterprise Information Security.

Successfully processing a transaction returns an authorization number that is unique per transaction and has no intrinsic value. It is safe to store this value, write it to logs, present it to staff, and email it to the customer.

#### 5.2.1 Cardholder Data Access

Electronic access to cardholder data must be restricted to authorized personnel with an established business need to access that data. This includes access to all information systems used to process, store, or transmit payment card account numbers. Information systems must employ access control mechanisms to restrict access based on a user's need-to-know and least privilege. Access to UAB information technology resources requires supervisor approval that specifies required privileges for handling cardholder data.

Paper records that contain cardholder data (e.g., payment card slips, order forms, hardcopy reports) must be secured when not in use, and securely disposed of when no longer needed. Access to these records must be restricted to authorized personnel with an established business need to access that data. If paper records containing cardholder data are retained locally, they must be stored in a locked file cabinet and in a locked room within a secure UAB facility.

#### 5.2.2 Separation and Transfers

When Entity members or employees separate from UAB and no longer require access to cardholder data or card processing environments, PCI Entity management must immediately request access to any local systems and access privileges be disabled, and must notify the AskIT Help Desk so that access to TouchNet can be disabled, where applicable. For those Entity

members and employees that transfer to other positions within UAB, and those job responsibilities no longer require access to cardholder data, Entity management must immediately request access privileges be modified to reflect the appropriate access privileges for the new member or employee position.

### 5.2.3 Record Retention and Disposition

PCI Entities should have local data retention standards and procedures that define the payment card data retention requirements for that business unit. It is highly recommended that cardholder information storage be kept 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 procedures.

The Office of the Chief Financial Officer has advised UAB PCI Entities that electronic and paper records (e.g. logs, files, database entries, copies of payment card purchases, or daily payment card terminal summary tapes) that contain payment card or sales tax information must be retained for a minimum of 3 years as outlined by the Public Universities of Alabama Functional Analysis & Records Disposition Authority for the purposes of providing appropriate records in the event of an audit. Exceptions to this recommendation may be applied based on longer record retention requirements defined in grants and contracts.

At the end of each fiscal year, any payment card transaction data or documentation older than 3 years may be disposed of in a manner that renders the data unrecoverable. PCI Entity management is responsible for the proper sanitization and destruction of all payment card transactional data, either electronic or paper-based.<sup>8</sup>

For electronic cardholder data records:

- Destroy (shred, crush, overwrite, or degauss) any computer media (hard drives, portable storage) that contained cardholder data when those devices are retired or the data are no longer needed.

---

<sup>8</sup> See “Secure Media Destruction” at <https://www.uab.edu/it/home/it-reports-and-publications/item/211-what-is-the-process-for-uab-secure-media-destruction>; “Drive Wiping Procedures” at <https://www.uab.edu/it/home/it-reports-and-publications/item/233-how-do-i-securely-wipe-a-disk-drive?>; UAB HIPAA core standard Media Reallocation and Disposal at <http://www.uab.edu/policies/content/Pages/UAB-AD-POL-0000721.aspx>



For paper-based cardholder data records:

- Cross-cut shred, incinerate, or pulp paper documents containing cardholder data when no longer needed. Payment card transaction documentation is authorized for transfer and destruction to a UAB approved shredding company.

#### 5.2.4 Restricting Physical Access to Cardholder Data

Physical access to cardholder data and payment card transactional systems should be restricted to authorized personnel, and protected against the loss of confidentiality, integrity, and availability. The following requirements shall be incorporated in the development of PCI Entity business process and procedures for the physical security of cardholder data:

- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
  - Use video cameras to monitor sensitive areas.
  - Restrict physical access to publicly accessible network jacks.
  - Restrict physical access to wireless access points, gateways, and handheld devices.
- Develop procedures to distinguish employees and visitors in areas where cardholder data is accessible.
- Ensure all visitors who enter areas where cardholder data is processed or maintained are authorized before entering those areas, and are given a physical token (e.g., badge or access device) that identifies them as non-employees and is surrendered when leaving the facility or upon expiration of the device.
- Use a visitor log that contains name, department/company, and authorizing employee at all facilities used to process, store, or transmit cardholder data for auditing visitor activity.
- Properly inventory and physically secure all paper and electronic media that contain cardholder information. Store media back-ups (if any) in a secure off-site facility and review the offsite location's security at least annually.

- Maintain strict control over the storage, accessibility, and distribution of media containing cardholder data.
- Ensure Entity management approves the removal of any media containing cardholder data from a secure facility.

### 5.3 Reconciliations

PCI Entities are responsible for posting all payment card transactions via deposit forms within 48 hours. Copies of all deposit forms and supporting documentation must be sent to the Entity's depository (Financial Operations Center or Hospital Cashiering). The Controller's office will provide training to the Entity members on the process.

- The Controller's office in conjunction with the Budget Office will be responsible for performing monthly reconciliation's of the bank account and will email a copy of the reconciliation listing all un-reconciled transactions to be booked by the responsible person in the local Entity.
- PCI Entities are responsible for researching and resolving all un-reconciled items within 30 days from transaction date. The Controller's office will work with the local Entity to resolve any outstanding items that are a direct result of a bank processing or posting error.
- On a quarterly basis, all transactions 90 days or older which have not been posted to the general ledger by local Entities will be posted by the Controller's office to each local Entity's account. An email will be sent prior to posting to the default account to allow the Entity a final opportunity to post the activity to the appropriate account.

### 5.4 Recurring Charges

One of the few business reasons for storing payment card numbers is recurring charges or payments.

PCI Entities have several responsibilities if they support recurring charges:

- Maintain original signed authorizations from payment card transactions in accordance with your record retention procedures.
- If the full Primary Account Numbers (PAN) are stored electronically, PCI guidelines require the numbers to be encrypted. Work with your Entity technical contacts or Enterprise Information Security to employ approved encryption techniques.

- Limit the term of the recurring payment to no more than one year, particularly if you have card- not-present (CNP) transactions.
- Expunge the payment card details as soon as the agreement is completed.
- **Sensitive authentication data for card-not-present transactions such as CVV/CVV2, CVC/CVC2 and PIN numbers cannot be stored for recurring payments.**

### 5.5 Charge Backs

Charge backs occur when a cardholder disputes a charge on their statement. Customers may dispute charges 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. The Controller's office will notify PCI Entity management of disputed charges presented by the acquiring bank. PCI Entities must follow the instructions on the form they receive from the bank and reply by the date specified. If an Entity is experiencing frequent charge back complaints or fraud is suspected, then the CFO's office should be contacted. PCI Entities 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

### 5.6 Monitoring and Security Incident Handling

Any known or suspected breach, compromise, or unauthorized access of cardholder data shall be reported immediately to the PCI Entity Senior Management and the Enterprise Information Security office. Enterprise Information Security is responsible for notifying the Office of the Chief Financial Officer (CFO). The CFO's office shall coordinate incident handling procedures with Enterprise Information Security in accordance with UAB Data Protection and Security Policy and UAB IT Incident Handling Procedures.

A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations, including:

- Regulatory notification requirements

- Loss of reputation
- Loss of customers
- Potential financial liability (for example, regulatory and other fees or fines)
- Litigation

PCI Entities must be prepared to respond to a security incident involving the breach or compromise of cardholder data on a 24/7 basis. Entity incident handling procedures shall include procedures for continuity planning and business recovery, data back up, and appropriate training for Entity members designated with security incident handling responsibilities. Entity incident handling procedures should include alerts from all appropriate sources (intrusion detection, intrusion prevention, file integrity monitoring) and reviews of payment brand and regulatory incident handling requirements, and shall be tested at least annually. Entity procedures for incident handling should be periodically modified to reflect industry developments and lessons learned.

The following section outlines incident handling procedures that deal with electronic as well as paper based records.

Be alert to potential compromises of cardholder data and regularly monitor system logs, and card processing or storage locations 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

If a suspected or actual breach has occurred or is in progress, contact the Enterprise Information Security office immediately (Phone 975-0842) and follow the below procedures:

- Submit a ticket at: <http://www.uab.edu/it/home/information-security>
- Contact your Supervisor
- Contain and limit the exposure *immediately*, and 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).
- If applicable, preserve all available logs (firewall, Intrusion Detection System, web server, operating system, remote access, etc.) that could be used to help identify the source and extent of the attack.
- If using a wireless network, change the SSID on the wireless access point 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 payment card account numbers as well as any other computers that users on the breached computer have accounts (too often the same password is used).
- Work with Enterprise Information Security to investigate the breach and repair the systems.
- Identify any account numbers or other personal information that may have been compromised.

Compromised systems must not be put back into production or connected to the UAB network until Enterprise Information Security has given its approval.

Work with the CFO's office and appropriate UAB Office of Counsel personnel to determine if notifications should be sent to the payment brands or individuals affected by the incident. If notifications are to be sent, work with the Office of Counsel and the Entity Human Resources department on the content of the notification.

The PCI Entity is responsible for assuming any costs associated with the incident that may include but not limited to:

- Any internal or external resources contracted to participate in the investigation
- UAB IT resources used to supplement local IT support resources
- It is up to the individual department, unit, or school to determine if IT resources expended on IT Incident Response are billed to the local unit or absorbed as overhead
- Any fines or penalties assessed by the Bank or payment card associations
- Any legal fees or penalties incurred as a result of the incident
- Any costs associated with producing and sending notifications, and
- Any external costs associated with a follow-up audit.

The credit card companies have individually specific requirements the PCI Entity must address in reporting suspected or confirmed breaches of cardholder data.

MasterCard	Appendix H
VISA	Appendix I
Discover	Appendix J
American Express	Appendix K

## **6. UAB PCI Information Security Standards**

The Payment Card Industry (PCI) Data Security Standards (DSS) were developed to enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS uses at its foundation the following 12 high level requirements:

### **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/passphrases 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: Protect all systems against malware and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications.

### **Implement Strong Access Controls**

- Requirement 7: Restrict access to cardholder data by business need-to-know.
- Requirement 8: Identify and authenticate access to system components.
- Requirement 9: Restrict physical access to cardholder data.

### **Regularly Monitor and Test Networks**

- Requirement 10: Track and monitor all access to network resource 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.

Information security must be a key component of all policies and practices related to payment card acceptance and transaction processing. The following sections provide a summary of the technical PCI DSS requirements not previously covered in this Handbook. Compliance with the following requirements will be dependent on the PCI Entity card processing environment. See Appendix D – Self Assessment Questionnaire Selection for an understanding of the various validation types and requirements for your card processing environment, and be prepared to meet and maintain the following applicable technical compliance requirements.

### 6.1 Build and Maintain a Secure Network

Firewalls are computer devices that control computer traffic allowed between an organization’s internal network and untrusted external networks, as well as traffic into and out of more sensitive areas within an organization’s internal trusted network.<sup>9</sup> The card processing environment is an example of a more sensitive area within the trusted network of an organization.

PCI Entities are responsible for developing and maintaining required compliance documentation within their Merchant Library on the [PCI Compliance web site](#), which includes but is not limited to a technical infrastructure spreadsheet (PCI Merchant Technical Questionnaire) and a network diagram that displays all connections to their card processing environment and cardholder data flows across systems and networks. The PCI Merchant Technical Questionnaire spreadsheet and network diagram should include wireless networks, a list of systems and system users, IP addresses, network Jack-ID, network ports, servers, firewalls, routers, wireless access points, and any other applicable information system resources part of the Entity’s card processing environment. All systems within an Entity’s trusted network must be protected from unauthorized access, and must adhere to the following requirements:

- Establishing firewall and router configuration standards that include:

---

<sup>9</sup> Untrusted networks are any networks that are external to the Entity network under review, and/or which the Entity has no ability to control or manage.



- A formal process for approving and testing all network connections and changes to the firewall and router configurations.
- A firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network.
- A documented description of groups, roles, and responsibilities for the logical management of network components.
- Documentation and justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
- Reviews of firewall and router rule sets at least every six months.
- Building firewall configurations that restrict connections between untrusted networks and any system components in the card processing environment.
  - Restrict inbound and outbound traffic to that which is necessary.
  - Specifically deny all other traffic.
  - Secure and synchronize router configuration files.
  - Install and configure perimeter firewalls between any wireless networks and the card processing environment to deny or control traffic.
- Prohibiting direct public access between the Internet and any system component in the card processing environment.
  - Implement a DMZ to limit inbound and outbound traffic to only those protocols that are necessary for the card processing environment.
  - Limit inbound Internet traffic to IP addresses within the DMZ.
  - Do not allow any direct routes inbound or outbound for traffic between the Internet and the card processing environment.
  - Implement anti-spoofing measures - Do not allow internal addresses to pass from the Internet into the DMZ.

- Restrict outbound traffic from the card processing environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.
- Permit only “established” connections into the network (stateful).
- Place databases in an internal network zone, segregated from the DMZ.
- Do not disclose private IP addresses and routing information to unauthorized parties – use RFC 1918 address space and network address translation (NAT) technologies.
- Installing personal firewall software or equivalent functionality on any mobile and/or employee-owned computers with direct connectivity to the Internet used to access the organization’s network.
- Ensure that security policies and operational procedures for managing firewalls are documented, in use and known to all affected parties.

Vendor-supplied defaults for system passwords and other security parameters must never be used. Malicious individuals often use vendor default passwords and other vendor default setting to compromise systems. These security vulnerabilities must be mitigated by adhering to the following standards:

- Always change vendor-supplied defaults **before** installing a system on the network, including passwords, SNMP strings, and unnecessary accounts.
- For wireless environments connected to the card processing environment or transmitting cardholder data, change wireless vendor defaults, including default wireless encryption keys, passwords, SNMP strings, and ensure wireless security settings are enabled for strong encryption for authentication and transmission.
- Develop configuration standards for all system components that address known security vulnerabilities and system hardening best practices.
  - Implement only one primary function per server.
  - Enable only necessary services and protocols.

- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
- Configure system security parameters to prevent misuse.
- Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- Encrypt all non-console administrative access using SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.
- Maintain an inventory of system components that are in scope for PCI.
- Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use and known to all affected parties.
- Require that shared hosting providers protect each Entity's hosted environment and cardholder data.

Third party vendor(s) that have a physical presence at UAB that process credit cards as the merchant of record are not permitted to use UAB voice or data resources, including but not limited to network, internet, telephone or facsimile. Such third party vendors are required to provide, maintain and secure any data and/or voice connection(s) required for their business operations and credit card processing.

## 6.2 Protect Cardholder Data

The primary objective is to keep cardholder data storage to a minimum (refer to Section 5.2 Protecting Cardholder Data in this Handbook). However, when using approved strong encryption techniques to protect electronically stored cardholder data, encryption keys must be protected against disclosure and misuse by restricting access to keys to the fewest number of individuals necessary, and storing keys securely in the fewest possible locations and forms. Encryption key management processes and procedures must be developed to document and implement the following:

- Generation of strong keys (only industry tested and accepted algorithms are allowed; proprietary algorithms from vendor products should not be accepted).
- Secure key distribution, storage, and periodic key changes done at least annually.

- Destruction of old keys.
- Split knowledge of dual control keys (that require 2 to 3 users to reconstruct the key).
- Prevention of unauthorized substitution of keys.
- Replacement of known or suspected compromise of keys.
- Revocation of old or invalid keys.
- Requirements that key custodians sign a form acknowledging their key custodian responsibilities.
- Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use and known to all affected parties.

Transmission of cardholder data across open, public networks must be encrypted using strong cryptography and security protocols, such as SSL/TLS and IPSEC, and must never be sent via unencrypted end-user messaging, such as email, instant messaging, or chat.<sup>10</sup> Wireless networks transmitting cardholder data, or that are connected to the card processing environment, must use industry best practices (802.11i) to implement strong encryption for authentication and transmission.

Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use and known to all affected parties.

### 6.3 Maintain a Vulnerability Management Program

Anti-virus mechanisms must be deployed on all systems commonly affected by viruses (PCs, servers) that store, process, or transmit cardholder data. All anti-virus mechanisms must remain current, actively running, and must be capable of detecting, removing, and protecting against all known types of malicious software and generating audit logs.

Perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm that systems that are not commonly affected by malicious software are protected and do not require

---

<sup>10</sup> Examples of open, public networks are the Internet, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).

anti-virus software. Ensure that security policies and operational procedures for protecting systems against malware are documented, in use and known to all affected parties.

PCI Entities must establish a process to identify newly discovered security vulnerabilities using reputable outside sources to assess risk rankings. Ensure that all system components and software, including payment applications, have the latest vendor-supplied security patches installed within one month of release.

Software applications used for payment card transaction services must be developed in accordance with PCI DSS and industry best practices, and shall incorporate information security throughout the software development life cycle, which includes:

- Testing of all security patches, and system and software configuration changes before deployment, including:
  - Validation of all input to prevent cross site scripting, injection flaws, and malicious file execution.
  - Validation of proper error handling.
  - Validation of secure cryptographic storage.
  - Validation of secure communications.
  - Validation of proper role-based access control.
- Separate development/test and production environments, and separation of duties for each.
- Production data are not used for testing/development.
- Removal of test data and accounts are complete before production systems become active.
- Removal of custom application accounts, user IDs, and passwords before becoming active or released to customers.
- Review of custom code prior to release to identify coding vulnerabilities by internal resources or third parties.

All web applications must be developed based on secure coding guidelines that include prevention of common coding vulnerabilities in software development, such as:

- Buffer overflows
- Cross site scripting (XSS)
- Injection flaws (SQL, LDAP, Xpath injection flaws)
- Malicious file execution
- Improper access control
- Insecure direct object references
- Cross site request forgery (CSRF)
- Information leakage and improper error handling
- Broken authentication and session management
- Insecure cryptographic storage
- Insecure communications
- Failure to restrict URL access
- All “high risk” vulnerabilities identified during the vulnerability identification process

For public-facing web applications, new threats and vulnerabilities shall be addressed on an ongoing basis to ensure they are protected against known attacks by either reviewing the application via manual or automated application vulnerability security assessment tools at least annually (or in the event of a significant change), or by installing an automated technical solution that detects and prevents web-based attacks (a web-application firewall) in front of public-facing web applications.

The Change Control procedures outlined in Section 4.4 Change Control (Technical) of this Handbook apply to implementation of security patches and software modifications. Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use and known to all affected parties.

#### 6.4 Implement Strong Access Controls

For assurance that cardholder data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job

responsibilities. Refer to Section 5.2.1 Cardholder Data Access in this Handbook for more information on limiting access.

Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use and known to all affected parties.

A unique user ID shall be assigned to each PCI Entity member to ensure that each individual is uniquely accountable for his or her actions. Actions taken with cardholder data on information systems are performed by, and can be traced to, known and authorized users. In addition to being assigned a unique user ID, all users shall be authenticated by the use of either a strong password or passphrase, or multi-factor authentication. All passwords/passphrases must be rendered unreadable during transmission and storage on all system components using strong cryptography.

Multi-factor authentication must be used for all remote access to the network by Entity members, employees, administrators, and third parties. Acceptable technologies include RADIUS, TACACS, or VPN using SSL/TLS or IPSEC. Accounts used by third parties to access, support, or maintain system components via remote access must only be enabled during the time period needed, monitored when in use and disabled when not in use.

Proper user authentication and password management shall include the following procedures:

- Control addition, deletion and modification of user IDs, credentials, and other identifier objects.
- Verify user ID before performing password resets.
- Immediately revoke access for any terminated users.
- Remove/disable inactive user accounts at least every 90 days.
- Enable accounts used by third parties for remote maintenance only during the period needed.
- Communicate password procedures to all users who have access to cardholder data.<sup>11</sup>
- Do not use group, shared or generic accounts and passwords/passphrases.

---

<sup>11</sup> See “What are the guidelines for creating a strong password?” at <http://www.uab.edu/it/home/about-uab-it/announcements/item/237>

- Change user passwords/passphrases at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords/passphrases containing both numeric and alphabetic characters.
- Do not allow the use of passwords/passphrases that are the same as the last four passwords/passphrases used.
- Limit repeated access attempts by locking out the user ID after no more than six attempts.
- Set the lockout duration to a minimum of 30 minutes or until reset by a system administrator.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to activate the terminal.
- Authenticate all access to any database containing cardholder data.

Ensure that security policies and operational procedures for identification and authentication are documented, in use and known to all affected parties. Authentication policies and procedures must be documented and communicated to all users and must include guidance on selecting strong passwords/passphrases and the reuse policy, protecting passwords/passphrases, and changing passwords/passphrases if their passwords/passphrases may have been compromised.

Refer to Section 5.2.4 Restricting Physical Access to Cardholder Data in this Handbook for more information on physical security requirements.

Each PCI Entity is responsible for security policies and operational procedures for the physical security of card-reading devices and terminals. At a minimum, the PCI DSS requires each PCI Entity to maintain a list of devices, periodically inspect devices to look for tampering or substitution and train personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

The UAB Payment Card Capture Device Security Procedures are included in this Handbook as Appendix L. The procedures include completing an annual risk assessment for the card-reader environment, maintaining an inventory, performing daily inspections and reviews of card-readers, updates and terminal disposal.



## 6.5 Regularly Monitor and Test Networks

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all PCI Entity card processing environments allows thorough tracking, alerting, and analysis in the event of a security incident. Therefore, all applicable PCI Entities must ensure the following standards are implemented:

- Establish a process for linking all access to system components to each individual user.
- Implement automated audit trails for all system components to reconstruct the following events:
  - All individual access to cardholder data.
  - All actions taken any individual with root or administrative privileges.
  - Access to all audit trails.
  - Invalid logical access attempts.
  - Use of identification and authentication mechanisms.
  - Initialization of audit logs.
  - Creation and deletion of system-level objects.
- Record at least the following audit trail entries for all system components for each event:
  - User ID
  - Type of event
  - Date and Time
  - Success or failure indication
  - Origination of event
  - Identity or name of affected data, system component, or resource
- Synchronize all critical system clocks and times using industry-accepted time sources.
- Secure audit trails so they cannot be altered.

- Limit viewing of audit trails to those with a business need-to-know.
- Protect audit trail files from unauthorized modifications.
- Back up audit trail files promptly to a centralized log server or media.
- Write logs for external-facing technologies onto a log server on the internal LAN.
- Use file-integrity monitoring or change-detection software on logs to ensure existing log data cannot be changed without generating alerts.
- Review logs for all system components at least daily that include servers that perform security functions, intrusion detection, authentication, authorization, and accounting.
- Review logs periodically of all other system components based on policy and risk management strategy.
- Retain audit trail history for at least one year, with a minimum of 3 months immediately available for analysis.

New and emerging vulnerabilities are continuously being discovered. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment, and shall include the implementation of the following standards:

- Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploy a wireless intrusion detection/prevention system to identify all wireless devices in use.
- Use up-to-date intrusion detection/prevention systems to monitor all traffic in the card processing environment and alert personnel to suspected compromise in accordance with Section 5.6 - Security Incident Handling Procedures.
- Deploy file-integrity monitoring software configured to perform critical file comparisons at least weekly to alert personnel to unauthorized modification of critical system files, configuration files, or content files.

Ensure that security policies and operational procedures for security monitoring and testing are documented, in use and known to all affected parties.

## 6.6 Maintain an Information Security Policy

The UAB Payment Card Processing and Security Policy establishes the primary organizational goals of meeting and maintaining compliance with the Payment Card Industry (PCI) Data Security Standards (DSS). This Handbook has been developed as a supplement to that policy in order to assist UAB PCI Entities in understanding and implementing those requirements. PCI Entities are charged with the responsibility of establishing Entity business process and procedures that are applicable to their specific card processing environments. Entity procedures should be developed in accordance with Section 5.1 – Business Process and Procedures, Appendix G – PCI Entity Payment Card Process and Procedure Guidelines, and the following standards:

- Develop security policies and daily operational security procedures that are consistent with the requirements in this Handbook and the PCI DSS.
- Develop and document an annual risk-assessment process that identifies assets, threats, vulnerabilities.
- Develop usage procedures for critical employee-facing technologies that require:<sup>12</sup>
  - Explicit management approval.
  - Authentication for use.
  - A list of all devices and personnel with access.
  - Labeling of devices with owner, contact information, and purpose.
  - Acceptable use.
  - Acceptable network locations.
  - List of UAB approved products.
  - Automatic disconnect of session for remote-access after a period of inactivity.
  - Activation of remote-access for third parties only when needed, with immediate deactivation after use.

---

<sup>12</sup> It is sufficient for PCI Entities to indicate in their local policy and procedures that they adopt standing UAB policies related to PCI compliance, for example Acceptable Use Policy, and Data Protection and Security Policy.

- Prohibit copy, move, and storage of cardholder data onto local hard drives and removable media when accessing via remote-access technology.
- Ensure that Entity procedures clearly define information security responsibilities for all Entity members and employees.
- Assign the following information security management responsibilities to an individual or team:
  - Establish, document, and disseminate Entity business process and procedures, including incident response handling and escalation procedures.
  - Monitor and analyze security alerts, and notify appropriate personnel.
  - Administer user account additions, deletions, and modifications.
  - Monitor and control all access to cardholder data.
- If cardholder data is shared with a service provider, maintain and implement procedures to manage service providers, to include:
  - Maintaining a list of service providers. Must include description of service provided and responsibilities break down. (Responsibility Matrix)
  - Maintain a written agreement that includes an acknowledgement that the service provider(s) is responsible for the security of cardholder data in their possession.
  - Ensure there is an established process to engage service providers in performing proper due diligence.
  - Maintain a program to monitor service providers' PCI DSS compliance status.

## 7. Definitions

**Card Processing Environment** – The area of computer systems and networks that possess cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the card processing environment.

**Cardholder** – Customer to whom a card is issued or individual authorized to use the card.

**Cardholder Data** – Any personally identifiable data associated with the cardholder, to include primary account number, cardholder name, expiration date, service code, address, social security number, card service verification code, or any other data stored on the magnetic stripe of the payment card.

**Information Security** – Encompasses both the UAB Enterprise Information Security Office (EISO) and the UAB Health System Information Security (HSIS) Office. Depending on the operating environment of the UAB PCI Entity, Entities are required to report to one of the two Information Security Offices for evaluation and approval for the implementation and maintenance of their payment card processing environments.

**Magnetic Stripe Data (Track Data)** – Data encoded in the magnetic stripe used for authentication during transactions when the card is presented. Entities must **not** retain full magnetic stripe data subsequent to transaction authorization. Only the PAN, expiration date, name, and service code may be retained if needed for business purposes.

**Merchants** - Authorized acceptors of payment cards for the purchase of goods, services, or information.

**Network members** – Acceptors of payment cards for the purchase of goods, services, or information that have been granted direct authorization to perform payment card transactions by the major credit card companies. Generally these include banking and financial institutions.

**Payment Application Data Security Standards (PA-DSS)** - The Council-managed program established to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV/CVV2 or PIN data, and to ensure their payment applications

support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements.

**Payment Card Industry Data Security Standards (PCI DSS)** - A multifaceted set of comprehensive requirements and security standards developed to enhance payment account data security, 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.

**Penetration Test** – Security-oriented probing of computer systems or networks to seek out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect and identify vulnerabilities and suggest security improvements.

**Primary Account Number (PAN)** – Payment card number (credit or debit) that identifies the issuer and the particular cardholder account.

**Separation of Duties** – The practice of dividing steps in a function among different individuals to keep a single individual from being able to subvert established processes.

**Senior Management** - Persons in the positions of dean, chair, or division or program director, or persons specifically designated by a dean, chair, or division or program director, that make executive decisions and are authorized to accept risks for the administrative unit in the area of information security.

**Sensitive Areas** - Any data center, server room, or area that houses systems that store, process, or transmit cardholder data. This excludes areas where only point-of-sale terminals are present, such as cashier areas in a campus retail store.

**Sensitive Authentication Data** – Security-related information that includes Card Validation Codes/Values, complete track data, PIN numbers and PIN blocks used to authenticate cardholders. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device or information system, or cardholder information could be used in a fraudulent transaction.

**Service Code** – The three or four-digit number on the magnetic stripe of a payment card that specifies acceptance requirements and limitations for a magnetic stripe read transaction.

**Service Provider** – Any business entity that is not a payment card brand network member or a merchant directly involved in the processing, storage, transmission, and switching of transaction data or cardholder information, or both. This includes companies that provide services to merchants, service providers, or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, Intrusion Detection Systems, and other services, as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

**Strong Cryptography** – General term to indicate cryptography that is extremely resilient to cryptanalysis.

**Multi-factor Authentication** – Authentication that requires users to produce multiple credentials to access a system. Credentials consist of something the user knows (UserID, Password), something the user has in their possession (smartcard, hardware token), or something the user is (biometric characteristic). To access a system, the user must produce at least two of the three credentials.

**UAB Enterprise** - The University of Alabama at Birmingham, the University of Alabama at Birmingham Health System, University Hospital, The Kirklin Clinic, the University of Alabama Health Services Foundation, the UAB Health Centers, the Ophthalmology Services Foundation, and Callahan Eye Foundation Hospital.

**UAB PCI Entity** - Any UAB department, office, section, or affiliated association or group that has been approved to accept, process, transmit, or store payment card transactional or cardholder data as a member, merchant, or service provider operating on behalf of UAB, or in use of the UAB brand name.

**Verification Code** – The three or four digit value printed on the front or back of a payment card; Card Validation Code CVC2 (Mastercard), Card Verification Value CVV2 (VISA), Card Member ID (Discover), or the Card Identification Number CID (American Express).

**Vulnerability** – A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

**Vulnerability Scan** – Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target an organization's private network.

**This Page Intentionally Left Blank**



## 8. Acronyms

<b>AMEX</b>	American Express, Inc.
<b>AOC</b>	Attestation of Compliance
<b>ASV</b>	Approved Scanning Vendor
<b>AV</b>	Anti-Virus
<b>AVS</b>	Address Verification Service
<b>CAV</b>	Card Authentication Value (JCB)
<b>CAV2</b>	Card Authentication Value 2 (JCB)
<b>CHD</b>	Cardholder Data
<b>CID</b>	Card Identification Number (American Express/Discover)
<b>CNP</b>	Card-not-present
<b>CSC</b>	Card Security Code (American Express)
<b>CSRF</b>	Cross Site Request Forgery
<b>CVC</b>	Card Validation Code (MasterCard)
<b>CVC2</b>	Card Validation Code 2 (MasterCard)
<b>CVV</b>	Card Verification Value (Visa/Discover)
<b>CVV2</b>	Card Verification Value 2 (Visa)
<b>DBA</b>	Doing Business As
<b>DMZ</b>	Demilitarized Zone
<b>DSS</b>	Data Security Standard
<b>HR</b>	Human Resources
<b>HSIS</b>	Health System Information Security
<b>IDS/IPS</b>	Intrusion Detection System/Intrusion Prevention System
<b>IP</b>	Internet Protocol
<b>IPSEC</b>	Internet Protocol Security
<b>EISO</b>	Enterprise Information Security Office
<b>IT</b>	Information Technology
<b>JCB</b>	Japan Credit Bureau
<b>LAN</b>	Local Area Network
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MC</b>	MasterCard, Inc.
<b>NAT</b>	Network Address Translation
<b>OVPFAA</b>	Office of the Vice President for Financial Affairs & Administration
<b>OVPIT</b>	Office of the Vice President for Information Technology
<b>PA</b>	Payment Application
<b>PA-DSS</b>	Payment Application Data Security Standards
<b>PAN</b>	Primary Account Number
<b>PCI</b>	Payment Card Industry
<b>PED</b>	PIN Entry Device
<b>PIN</b>	Personal Identification Number
<b>POS</b>	Point of Sale
<b>QSA</b>	Qualified Security Assessor

<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>SAQ</b>	Self Assessment Questionnaire
<b>SNMP</b>	Simple Network Management Protocol
<b>SQL</b>	Structured Query Language
<b>SSC</b>	Security Standards Council
<b>SSH</b>	Secure Shell
<b>SSID</b>	Service Set Identifier
<b>SSL</b>	Secure Sockets Layer
<b>TACACS</b>	Terminal Access Controller Access-Control System
<b>TLS</b>	Transport Layer Security
<b>URL</b>	Uniform Resource Locator
<b>VbV</b>	Verified by Visa
<b>VPN</b>	Virtual Private Network
<b>XSS</b>	Cross Site Scripting

## APPENDIX A - PCI Entity Payment Card Account Request Form

### CREDIT CARD MERCHANT ACCOUNT REQUEST FORM

Use of a credit card terminal requires an analog telephone line. Contact UAB Communications at [uabcomm@uab.edu](mailto:uabcomm@uab.edu) in order to install an analog line if you do not have one available.

If you have any questions or need assistance completing this form, contact Sonya Nickolson at [sonyan@uab.edu](mailto:sonyan@uab.edu) or 205-975-8315.

#### Merchant Account Contact Information

<b>Vice President/Dean</b>	<b>Name</b>	_____
	<b>Physical Office Address</b>	_____
	<b>Campus Mailing Address</b>	_____
	<b>Phone Number</b>	_____
	<b>BlazerID</b>	_____
	<b>Email</b>	_____
<b>Business/Fiscal Officer</b>	<b>Name</b>	_____
	<b>Physical Office Address</b>	_____
	<b>Campus Mailing Address</b>	_____
	<b>Phone Number</b>	_____
	<b>BlazerID</b>	_____
	<b>Email</b>	_____
<b>Account Manager</b>	<b>Name</b>	_____
	<b>Physical Office Address</b>	_____
	<b>Campus Mailing Address</b>	_____
	<b>Phone Number</b>	_____
	<b>BlazerID</b>	_____
	<b>Email</b>	_____
<b>Department Deposit Contact</b>	<b>Name</b>	_____
	<b>Physical Office Address</b>	_____
	<b>Campus Mailing Address</b>	_____
	<b>Phone Number</b>	_____
	<b>BlazerID</b>	_____
	<b>Email</b>	_____
<b>Department Technical Contact</b>	<b>Name</b>	_____
	<b>Physical Office Address</b>	_____
	<b>Campus Mailing Address</b>	_____
	<b>Phone Number</b>	_____
	<b>BlazerID</b>	_____
	<b>Email</b>	_____

**Merchant Account Information**

DBA (Doing Business As) Account Name (24 character Limit) \_\_\_\_\_  
 Oracle GL Account Number (to debit processing fees) \_\_\_\_\_  
 Estimated Annual Sales Volume \_\_\_\_\_  
 Estimated Average Sales Ticket Amount \_\_\_\_\_  
 Type of Services Provided or Products Sold \_\_\_\_\_

**Card Types to Accept:**  
 \_\_\_ Visa/MasterCard/Discover  
 \_\_\_ American Express

**Quantity of First Data Credit Card Terminals Needed.**  
 \_\_\_ Wired  
 \_\_\_ Wireless (Cellular)

If you are using a POS system, or processing payments through the internet, please complete the question below.  
  
 Software Name \_\_\_\_\_

UAB is committed to complying with all commercial standards regarding the security and privacy of payment card transactions. Go to the [UAB PCI Compliance website](#) to review the Payment Card Processing and Security Policy as well as the UAB PCI Entity Handbook. The security policy applies to all UAB employees and any unit that processes payment card information in a physical or electronic format on behalf of the UAB enterprise. The UAB PCI Entity Handbook provides step-by-step instructions on requesting a new merchant account, approval and registration procedures, compliance certification, entity responsibilities and technical security requirements.

\_\_\_\_\_  
Dean Associate Vice President - Signature

\_\_\_\_\_  
Dean Associate Vice President - Print Name

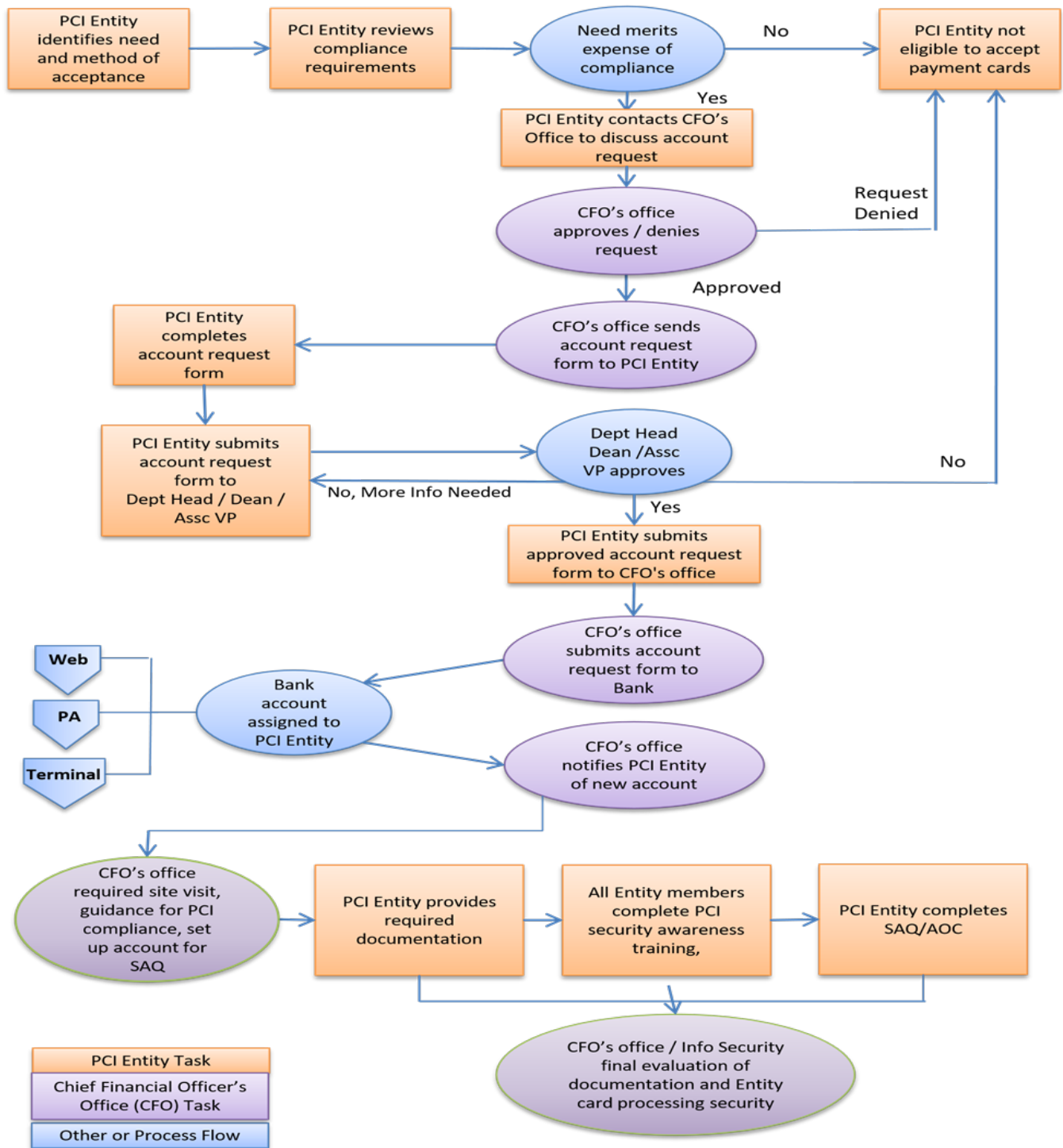
\_\_\_\_\_  
Department Head - Signature

\_\_\_\_\_  
Department Head - Print Name

\_\_\_\_\_  
Merchant Account Manager - Signature

\_\_\_\_\_  
Merchant Account Manager - Print Name

## APPENDIX B – PCI Entity Payment Card Account Request Workflow



## APPENDIX C – PCI Entity Account Agreement



---

### PCI Entity Account Agreement

#### Purpose of the PCI Entity Account Agreement

This University of Alabama at Birmingham PCI Entity Account Agreement represents the acknowledgement of the undersigned that they have read, understand, and will comply with:

- The UAB Cash Receipts Policy
- The UAB Payment Card Processing and Security Policy
- The UAB PCI Entity Handbook
- The Payment Card Industry Data Security Standards, version 3.2

#### UAB PCI Account User Responsibility

This acknowledgement shall be completed by UAB PCI Entity members as part of approval and registration of new Entities, and annually thereafter.

#### UAB PCI Account User Acknowledgment

As an employee of \_\_\_\_\_, I acknowledge the following statements. Department

- I have read the above named UAB and PCI policies and standards regarding payment card security.
- I have received and read my department's standards and procedures regarding payment card security.
- I am required to complete Payment Card Security Awareness training upon hire, and annually thereafter.
- I understand how these policies related to my job duties and will comply with these policies, standards, and procedures.

\_\_\_\_\_  
Merchant Account Contact Name – Type or Print

\_\_\_\_\_  
Merchant Account Contact - Blazer ID

\_\_\_\_\_  
Merchant Account Contact Name – Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Immediate Supervisor - Typed

## APPENDIX D – Self Assessment Questionnaire Selection

The Payment Card Industry (PCI) Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist UAB PCI Entities and service providers in evaluating their compliance with the PCI Data Security Standards (DSS). There are multiple versions of the PCI DSS SAQ to meet various scenarios. This appendix has been developed to help organizations and Entities determine which SAQ best applies to them.

The PCI DSS SAQ consists of the following components:

- Questions correlating to the PCI DSS requirements appropriate for PCI Entities and service providers.
- The Attestation of Compliance (AOC), which is an Entity’s certification that they are eligible to perform and have performed the appropriate Self-Assessment.

There are eight SAQ Validation categories, shown briefly in the table below and described in more detail in the following paragraphs. Use the table to gauge which SAQ applies to your Entity or organization, and then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) Entities, all cardholder data functions outsourced. <i>This would never apply to In-Person Transactions.</i>	A
2	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn’t directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises. Applicable only to e-commerce channels.	A-EP
3	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial – out terminal merchants with no electronic cardholder data storage. This would never apply to e-commerce merchants. Imprint-only Entities with no cardholder data storage.	B
4	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.	B-IP
5	Entities using only web-based virtual terminals, no electronic cardholder data storage. This would never apply to e-commerce merchants.	C-VT
6	Entities with payment application systems connected to the Internet, no local cardholder data storage.	C
7	Merchants using only hardware payment terminals included in a PCI SSC-listed, validated, P2PE solution, no electronic cardholder data storage. This would never apply to e-commerce merchants.	P2PE-HW
8	All other Entities (not included in descriptions for SAQ A-C above) and <b>all service providers</b> defined by a payment brand as eligible to complete an SAQ.	D

**SAQ Validation Type 1 / SAQ A: Card-not-present, all cardholder data functions outsourced.**

SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of all payment pages delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

***This SAQ is not applicable to face-to-face channels.***

**SAQ Validation Type 2 / SAQ A-EP—Partially Outsourced E-Commerce Merchants Using a Third-Party Website for Payment Processing.**

SAQ A-EP has been developed to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process, or transmit any cardholder data on their systems or premises.

SAQ A-EP merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Your company accepts only e-commerce transactions;



- All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
- Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
- If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
- Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

***This SAQ is applicable only to e-commerce channels.***

**SAQ Validation Type 3 / SAQ B: Merchants with Only Imprint Machines or Only Standalone, Dial-Out Terminals. No Electronic Cardholder Data Storage.**

SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals.

SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system. SAQ B merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Your company uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- Your company does not transmit cardholder data over a network (either an internal network or the Internet);
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Your company does not store cardholder data in electronic format.

***This SAQ is not applicable to e-commerce channels.***

**SAQ Validation Type 4 / SAQ B-IP—Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) terminals, No Electronic Cardholder Data Storage.**

SAQ B-IP has been developed to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor.

SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B-IP merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Your company uses only standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to your payment processor to take your customers' payment card information;
- The standalone, IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs);
- The standalone, IP-connected POI devices are not connected to any other systems within your environment (this can be achieved via network segmentation to isolate POI devices from other systems);
- The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor;
- The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Your company does not store cardholder data in electronic format.

***This SAQ is not applicable to e-commerce channels.***

**SAQ Validation Type 5 / SAQ C-VT—Merchants with Web-Based Virtual Terminals, No Electronic Cardholder Data Storage.**

SAQ C-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet.

A virtual payment terminal is web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Payment card transactions are entered manually.

SAQ C-VT merchants process cardholder data only via a virtual payment terminal and do not store cardholder data on any computer system. These virtual terminals are connected to the Internet to access a third party that hosts the virtual terminal payment-processing function. This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits cardholder data to authorize and/or settle merchants' virtual terminal payment transactions.

This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution. SAQ C-VT merchants may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

SAQ C-VT merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Your company's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
- Your company's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company accesses the PCI DSS-compliant virtual payment terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);
- Your company's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
- Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
- Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Your company does not store cardholder data in electronic format.

***This SAQ is not applicable to e-commerce channels.***

**SAQ Validation Type 6 / SAQ C—Merchants with Payment Application Systems Connected to the Internet, No Electronic Cardholder Data Storage.**

SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via DSL, cable modem, etc.).

SAQ C merchants process cardholder data via a point-of-sale (POS) system or other payment application systems connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

SAQ C merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Your company has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
- The payment application system/Internet device is not connected to any other systems within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single store only;
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Your company does not store cardholder data in electronic format.

***This SAQ is not applicable to e-commerce channels.***

**SAQ Validation Type 7 / SAQ P2PE—Merchants using Only Hardware Payment Terminals in a PCI SSC-listed P2PE Solution, No Electronic Cardholder Data Storage.**

SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data only via payment terminals included in a validated and PCI SSC-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE merchants do not have access to clear-text account data on any computer system, and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a P2PE validated hardware device.

SAQ P2PE merchants will confirm that they meet the following eligibility criteria for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC;
- The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution;
- Your company does not otherwise receive or transmit cardholder data electronically.
- There is no legacy storage of electronic cardholder data in the environment;
- If your company stores cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; and
- Your company has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

***This SAQ is not applicable to e-commerce channels.***

**SAQ Validation Type 8 / SAQ D for Merchants – All Other SAQ-Eligible Merchants.**

SAQ D for Merchants applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type.

Examples of merchant environments that would use SAQ D may include but are not limited to:

- E-commerce merchants who accept cardholder data on their website;
- Merchants with electronic storage of cardholder data;
- Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type;
- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

**SAQ D for Service Providers –SAQ-Eligible Service Providers**

SAQ D for Service Providers applies to all service providers defined by a payment brand as being SAQ-eligible.

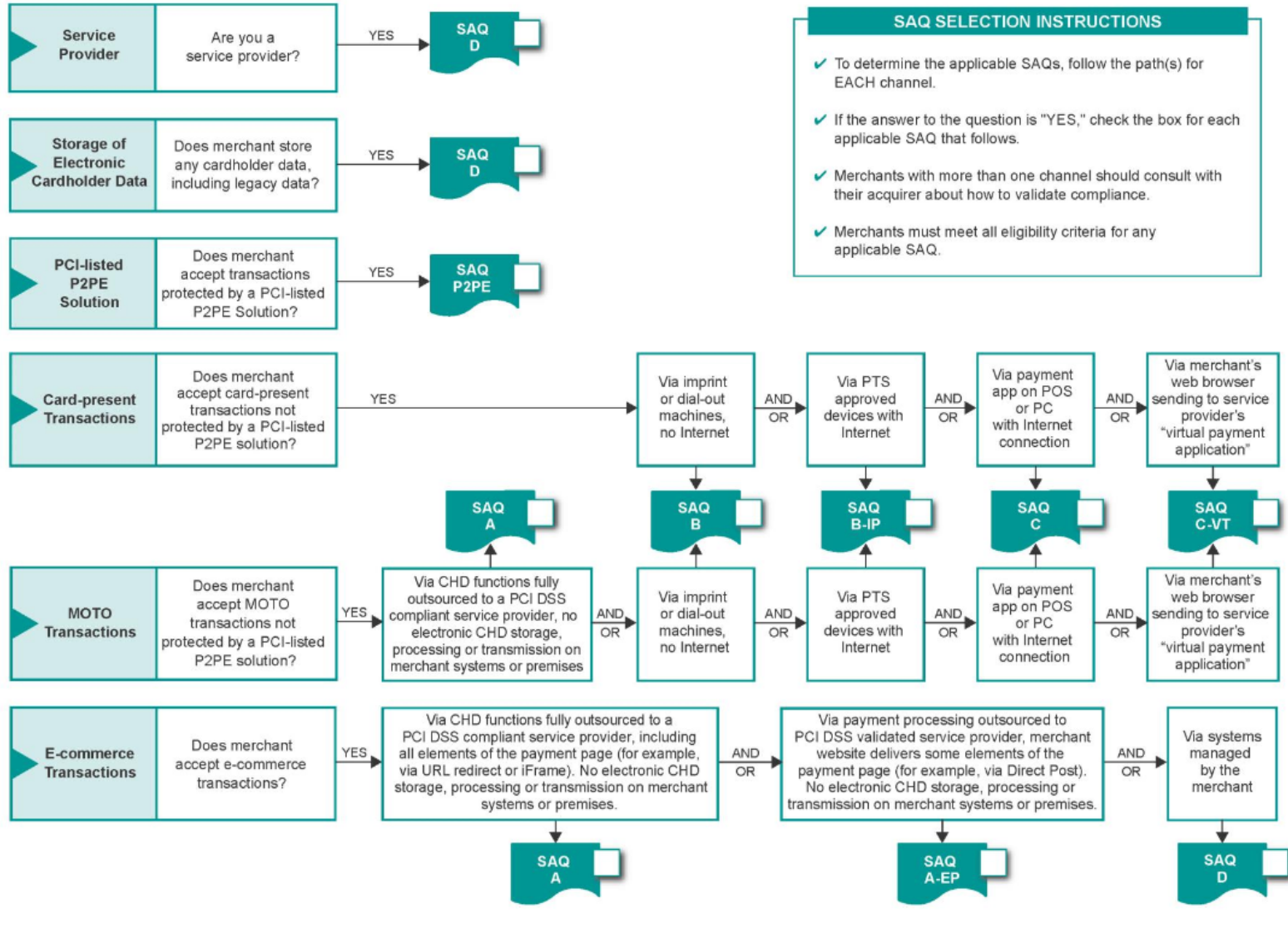
Note for SAQ D for Merchants and SAQ D for Service Providers:

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology. See the specific guidance in the respective SAQ D for information about the exclusion of other, specific requirements.

**Non-Applicability:** For all SAQs, these and any other requirements deemed not applicable to your environment must be indicated with "N/A" in the "Special" column of the SAQ. Accordingly, complete the "Explanation of Non-Applicability" worksheet in the Appendix for each "N/A" entry.

**Note:** For the SAQ for P2PE-HW, the "Special" column has been replaced with an "N/A" column to record any not-applicable requirements.

### Which SAQ Best Applies to My Environment?



## APPENDIX E – Software Requirements

Any UAB PCI Entity that plans to use payment application software for payment card related services must use a vendor or third party application that is a PCI Validated Payment Application that meets the Payment Application Data Security Standard (PA-DSS) requirements. Authorizations to use payment applications must be approved through the established UAB contract review process. Enterprise Information Security will verify that the payment application being requested for use is validated to be compliant with the PCI PA-DSS. Payment applications that do not meet PA-DSS requirements cannot be used. Any use of payment applications that have not been validated by PCI must be approved through the following exception process.

It is recognized that some internally (UAB) developed software, or software purchased from a vendor to perform a specific function, may have payment card acceptance built into the functionality. If modifying internally developed or purchased software to use the TouchNet service is either not feasible or not practical (e.g., cost to modify to use TouchNet is greater than the cost of the software package) then exceptions to use that software must be requested and approved by the Office of the Chief Financial Officer and the Office of Information Technology. The Entity wishing to develop or purchase the software is responsible for ensuring that the software meets all applicable PCI DSS and PCI PA-DSS requirements, and that the systems on which it will run are complaint with all PCI requirements regarding payment card acceptance. Software can only be considered for exception if it meets the below requirements.

### Requirements

PCI Entities wishing to use payment applications for payment card processing services must provide written documentation from the vendor stating that the software is certified to be compliant with all PCI DSS and PA-DSS requirements, that the vendor will provide support for resolving any compliance issues discovered by UAB or our scanning vendor (TrustWave), 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 Standards are changed, and that there will be no cost to upgrade to a version compliant with the PCI DSS.
- Vendor must agree that its software is currently certified to run on the latest release of the operating system for which it was designed.
- Vendor agrees to support its product and rectify any problems quickly if the local Entity installs security patches supplied by the operating system vendor when such patches are released.
- Vendor provides support for PCI compliance issues either through a standard helpdesk or through a different contact that they are contractually obligated to maintain.

Any request for exception to the above requirements by a requesting PCI Entity must demonstrate that using TouchNet is not practical and that they have reviewed previously approved exceptions of similar

software. The requesting Entity must cooperate with Enterprise Information Security in their review of the software's compliance with the above requirements.

### Process




- The PCI Entity must fully document a request for exception for the use of payment application software, as outlined above.
- The CFO's office will review the expected use and, where applicable, will compare it to software previously exempted. If the software exception is comparable to previous exceptions, the CFO's office will provide the information to the requesting Entity to review. The Entity may continue their request for an exception, but existing software that meets their need will be considered in the review by the CFO's office and Enterprise Information Security.
- The CFO's office and Enterprise Information Security will review the exception.
- Enterprise Information Security will meet with the requesting Entity and compare the software against current PCI and UAB criteria.
- Enterprise Information Security will forward the completed request, and report of compliance and recommendation to the Vice President of Information Technology (VPIT).
- The VPIT will review the request and provide an approval or rejection decision to the CFO's office.
- The CFO's office will review the VPIT recommendation for approval or rejection of the request.
- The CFO's office has authority to approve or reject all exception requests in coordination with the Vice President of Information Technology.



## APPENDIX F – Web Hosting Requirements

Web sites that accept credit cards must meet and maintain full compliance with PCI Data Security Standard (DSS) requirements. This document outlines web hosting requirements based on the category of web site maintained by UAB, a PCI Entity, or a PCI compliant service provider. In some cases as noted below, the data center hosting the web site must be evaluated by Enterprise Information Security to ensure compliance with the PCI DSS.

### Categories of Web Sites

-  1. Web site that links/redirects to TouchNet or another PCI certified service provider hosted site to process payment cards for card-not-present transactions and no local storage of cardholder data (SAQ-A).
-  2. Web site used to process payment card transactions by a local user that is hosted by UAB or a PCI certified compliant service provider that does not store any cardholder data locally. This applies to card-not-present and card-present transactions (SAQ-C).
-  3. Web site accepting payment cards directly and storing payment card numbers locally (SAQ-D).

### Requirements By Category

#### Category 1

- Local systems and processes must be fully compliant with applicable PCI and UAB information security standards.
- The web server must be isolated from the network and only allow outside access using the following protocols or ports: hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN). Any other protocols or ports required for a specific business purpose must be requested and approved by Enterprise Information Security.
- The local system must be scanned for vulnerabilities prior to being placed in production, and monthly thereafter.
- The system used to link to the hosted service provider must be physically secured.

#### Category 2

Includes all of the Category 1 requirements, as well as:

- The web server must be housed in the UAB computer center in the Rust Research Center or in another approved site.
- The system used to access the web site must be isolated from non-payment card applications on the network.
- The PCI Entity must have sufficient technical resources devoted to monitoring the systems and maintaining the secure card processing environment as required by the PCI DSS.

**Category 3 – PCI Entities operating within this card processing environment are required to meet compliance with ALL of the PCI Data Security Standards that include the below web hosting criteria.**

Includes all of the Category 1 and 2 requirements, as well as:

- The PCI Entity must document a compelling business need to locally store credit card numbers to be reviewed and approved by the CFO's office and Enterprise Information Security.
  - Requests to locally store payment card account numbers must have approval by the Entity Department Head, and Dean or Associate Vice President.
- The web server and database servers must be housed in the UAB computer center in the Rust Research Center or in another approved site.
- The payment card account numbers must be stored on a separate database server that is not Internet accessible. This separate server must also be protected by a firewall.
- The database server(s) must be isolated from non-payment card applications on the network.
- PCI Entities in this category are subject to routine monitoring and auditing.

\*Note: UAB offers the TouchNet Marketplace service, which allows all cardholder data storage to be outsourced within the secure TouchNet data center. This is the preferred method to meet the business needs of PCI Entities that process credit cards over the Internet.

### **Approved Data Centers**

PCI Entities wishing to house web servers or databases in a data center other than the Rust Research Center must contact Enterprise Information Security to have their data center evaluated and approved. Enterprise Information Security will evaluate the data center based on the following requirements:

- Physical security of the data center
- Local procedures supporting PCI compliance in their IT architecture
- Ability to support 24/7 incident response
- Appropriate logging at the operating system level and established log review procedures

## **APPENDIX G – PCI Entity Payment Card Process and Procedure Guidelines**

This document represents an outline of items that should be covered in PCI Entity process and procedures regarding payment card transactional activities. These guidelines should be viewed as a starting point for developing Entity procedures and not as a finished product. Due to the significant differences in each individual Entity's business processes and procedures, this outline may include items that are not relevant to your payment card processing environment. In addition, these guidelines may not include recommendations for areas within your business process that should be included in your local procedures. If you wish to get feedback on your individual business process and procedures, please contact the CFO's office for assistance.

### **All PCI Entities**

#### **Authorizations of Transactions**

Include descriptions of those Entity positions that can approve refunds. If your Entity members are authorizing and settling at different times, you should identify positions that can authorize settlements as well.

#### **Separation of Duties**

Describe how tasks within your unit are segregated for control purposes. For example, the person reconciling the account should not be the one creating transactions.

#### **Reconciliations**

Identify those positions within your Entity that are responsible for reconciling accounts, and what local systems are used to reconcile data to the payment card transactions. Outline all of the steps to be taken by the Entity and timeframes for completing reconciliations.

#### **Charge backs**

Outline Entity procedures taken upon notification from the Student Accounting Services office or the bank that a charge has been disputed by the cardholder. Identify the following:

- The research to be performed to rectify the transaction
- Those positions authorized to approve refunds

Procedures should include steps for challenging the cardholder's dispute, issuing refunds, and notifications to the bank of actions taken. Failure to notify the bank can result in the refund being issued twice (once by you, once by the bank).

#### **Record Retention**

Document record retention procedures for both electronic and paper-based cardholder data records that are specific to your business process, and meet any required legal, regulatory, business retention requirements. Full payment card numbers (PAN) should never be stored and should be masked to reveal

only the last four digits of the card number in both electronic and paper-based records. For paper records, specify how and where cardholder data will be secured when not in use.

Entity procedures should document processes for both electronic media and paper-based destruction when the media (computers, hard drives, portable storage, USB “thumb” drives, etc.) and paper-based records that contain cardholder data are no longer needed. Procedures must comply with UAB policies for destruction of media and paper-based records.

### **Data Access**

Identify those positions within your unit that are authorized to access systems or files containing cardholder data, and how that access is controlled.

### **Training**

Specify the requirements for Entity personnel to attend PCI security awareness training upon hire, and annually thereafter. It is recommended that Entity management provide local security awareness training that includes all aspects of local Entity procedures, as well as UAB policies and PCI DSS requirements.

### **Background Checks**

Identify those positions within your Entity that have an established business need to access cardholder data, and include in those position descriptions the requirement for applicable background checks to be conducted by your local HR office before personnel assume the responsibilities of the position. Your local HR department should be made aware of which positions require background checks.

### **Physical Security**

Describe physical security measures employed within your Entity card processing environment for systems, files, and facilities.

### **Annual Certification**

Identify those Entity management or members responsible for completing the annual compliance certification requirements for PCI, including completing the Self-Assessment Questionnaire (SAQ) on behalf of the Entity. This may be a combination of Entity management and technical support contacts.

### **Incident Response**

Identify those Entity positions responsible for responding to a known or suspected breach or compromise of cardholder data, and the Entity procedures for carrying out the requirements in the UAB Data Protection and Security Policy and the UAB IT Incident Handling Procedures. Provide procedural guidance for Entity personnel in identifying, assessing, and responding to a potential security incident.

## **Web & POS PCI Entities**

### **Security Standards and Procedures**

Identify specific security standards and procedures which deal with the technical infrastructure supporting your card processing environment. Your local standards and procedures should be consistent with the security policies found on <http://www.uab.edu/it/home/it-related-policies> and the PCI DSS requirements for maintaining information security procedures.

### **Change Control**

Describe the process of how changes to your card processing environment are managed. Include those Entity positions authorized to make changes, those authorized to approve them, and the procedures for testing changes in a test environment prior to being placed in production. This section should also outline procedures for implementing new releases and patches supplied by vendors.

### **Business Continuity**

Describe procedures for responding to a disaster or other incident in a manner that will maintain the security of cardholder data.

### **Monthly Scans**

Identify those Entity positions responsible for working with Enterprise Information Security to address vulnerabilities after a monthly scan has been conducted, and the requirements for correcting vulnerabilities discovered during the scan.

### **Penetration Tests**

Identify those Entity positions responsible for working with Enterprise Information Security to address vulnerabilities after an annual penetration test has been conducted, and the requirements for correcting vulnerabilities discovered during the pen test.

### **System Monitoring**

Identify those Entity positions responsible for monitoring systems involved in payment card acceptance or storage of cardholder data. Identify logging and other monitoring activity specific to your card processing environment.

## APPENDIX H – MasterCard Incident Response Requirements

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to [compromised\\_account\\_team@mastercard.com](mailto:compromised_account_team@mastercard.com).
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

## APPENDIX I – VISA USA Incident Response Requirements

In the event of a security breach, the Visa USA Operating Regulations require entities to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the VISA USA Cardholder Information Security Program. If VISA USA determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating loss of this information, VISA USA may require immediate corrective action.

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, VISA may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in VISA programs.

VISA has provided the following step-by-step guidelines to assist an entity in the event of a compromise. In addition to the following, VISA may require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records.

### Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.  
To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
  - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).
  - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
  - Preserve logs and electronic evidence.
  - Log all actions taken.
  - If using a wireless network, change Service Set Identifier (SSID) on the access point 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 all VISA systems.
2. Alert all necessary parties, including:
  - Internal information security group and Incident Response Team, if applicable
  - Legal department
  - Merchant bank

- VISA Fraud Control Group at (650) 432-2978 in the U.S.
  - Local FBI Office, U.S. Secret Service, or RCMP local detachment, if VISA payment data is compromised.
3. Provide the compromised Visa account to VISA Fraud Control Group at (650) 432-2978 within 24 hours.
    - Account numbers must be securely sent to VISA as instructed by VISA. It is critical that all potentially compromised accounts are provided. VISA will distribute the compromised VISA account numbers to Issuers and ensure the confidentiality of entity and non-public information.
  4. Requirements for Compromised Entities
    - All merchant banks must:
      - Within 48 hours of the reported compromise, provide proof of Cardholder Information Security Program compliance to VISA
      - Provide an incident report document to VISA within four business days of the reported compromise
      - Provide an additional incident report document to VISA no later than fourteen days after initial report (See template: Appendix C)
      - Depending on the level of risk and data elements obtained, complete within four days of the reported compromise
        - An independent forensic review
        - A compliance questionnaire and vulnerability scan upon VISA's discretion

### Steps for Merchant Banks

1. Contact Visa USA Fraud Control Group immediately at (650)432-2978
2. Participate in all discussions with the compromised entity and VISA USA
3. Engage in a VISA approved security assessor to perform the forensic investigation
4. Obtain information about compromise from the entity
5. Determine if compromise has been contained
6. Determine if an independent security firm has been engaged by the entity
7. Provide the number of compromised VISA accounts to Visa Fraud Control Group within 24 hours
8. Inform Visa of investigation status within 48 hours
9. Complete steps necessary to bring entity into compliance with CISP according to timeframes described in "What to do if Compromised"
10. Ensure that entity has taken steps to prevent future loss or theft of account information, consistent with the requirements of the VISA USA Cardholder Information Security Program

### Forensic Investigation Guidelines

Entity must initiate investigation of the suspected or confirmed loss or theft of account information within 24 hours of compromise.

The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk



- a. Number of accounts at risk, identify those stored and compromised on all test, development and production systems
- b. Type of account information at risk
- c. Account number
- d. Expiration date
- e. Cardholder name
- f. Cardholder address
- g. CVV2
- h. Track 1 and Track 2
- i. Any data exported by intruder
2. Perform incident validation and assessment
  - a. Establish how compromise occurred
  - b. Identify the source of the compromise
  - c. Determine timeframe of compromise
  - d. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any third-party connections
  - e. Determine if compromise has been contained
3. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.)
4. If applicable, review VisaNet endpoint security and determine risk
5. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed
6. Perform remote vulnerability scan of entity's Internet facing site(s)

## **APPENDIX J – Discover Incident Response Requirements**

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
4. Obtain additional specific requirements from Discover Card

## **APPENDIX K – American Express Incident Response Requirements**

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the US
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
4. Obtain additional specific requirements from American Express

## **APPENDIX L – UAB Payment Card Capture Security Procedures**

(PCI DSS v3.2.1 Requirement 9.9)

UAB Merchants that have Point-of-Sale (POS) card-reading devices (card-present) environments are required to implement security best practices associated with the protection of those devices. These procedures are best practices and security guidelines and based on established countermeasures established by the Payment Card Industry Security Standards Council.

UAB Merchants with card-reading devices are required to:

Maintain an inventory of swipe devices

(Use the attached form – Terminal Inventory Form)

1. Record its make, model, and serial number.
2. Record its location in the store (unless the terminals are removed and secured when the store is closed).
3. Record the condition and location of any labels.
4. Record the exact details of any security labels.
5. For PIN pads and POS PED devices connected to an electronic cash register, or separate host system, record how the terminal is connected.
6. Record how many connections (leads, plugs, aerials, etc.) are normally associated with each terminal. Record the style, type, and color of each connector, or take a photograph to show the number and the type of connectors used.
7. Mark each terminal with an ultra-violet (UV) security pen to provide a unique identifier for that terminal.
8. Use PCI SSA approved terminals.

Perform terminal reviews

1. Use the attached form – Terminal Review Checklist – to review terminals on an ongoing basis.
2. Daily procedure should include documenting and monitoring your terminal environment.
3. Train your staff of the importance of terminal and terminal infrastructure security.

Terminal Purchases and Updates

1. Any process that involves changes to the terminal must have correct authorizations and only legitimate personnel should be involved in the process.
  - a. Business Unit Manager, CFO's office and Enterprise Information Security must be involved in any purchases or updates to terminals.
2. When performing updates, especially the loading of new keys, it is essential that you:
  - a. Maintain dual control at all stages.
  - b. Complete and retain proper logs and control sheets.
3. When purchasing new terminals, they must be approved and meet the requirements of the PCI PTS Security Evaluation Program and the PCI DSS.

### Terminal Disposal

Merchants are to return old terminals to the CFO's Office.

### Perform Annual Risk Assessment Analysis on their card-reader infrastructure

A risk analysis process for skimming attacks and the POS, at a minimum, should include the identification of assets, the identification of threats, and the probability of the threat's taking place. This in turn should lead to the identification of those countermeasures and controls that best mitigate the threat at a specific merchant location and POS environment.

The identification of assets is a critical first step to any risk analysis process. In this case we are focused on the terminal and terminal infrastructure. Once you have used the Terminal Inventory Form to identify your terminals, use the attached Terminal Risk Assessment Form to complete you risk analysis.

Other Inventory Forms are available if merchant has more than 3 terminals or P2PE terminals

**Terminal Inventory Form**

**Swipe Terminal Inventory List and Detail Form**

Merchant ID #: \_\_\_\_\_ Date: \_\_\_\_\_  
 Merchant Name: \_\_\_\_\_  
 Contact Name: \_\_\_\_\_ Blazer ID: \_\_\_\_\_  
 Additional Info if needed: \_\_\_\_\_

List and describe each terminal in use below.

Terminal Details	Swipe Terminal #1	Swipe Terminal #2	Swipe Terminal #3
Make			
Model			
TID No. (Terminal ID No.)			
Serial No. (printed on label)			
Location when in use:			
Location when not in use:			
General condition and appearance (color, existing marks, scratches, etc.):			
Location of manufacturer's security seals or labels:			
Details of manufacturer's security markings or reference numbers:			
Describe each terminal connections below: (i.e. power/black and phone/gray, etc)			
Connection #1: Connector type, color of lead:			
Connection #2: Connector type, color of lead:			
Connection #3: Connector type, color of lead:			
How many connections in total (all leads, plugs, aerials, etc)?			
Describe any display stands, charity boxes, or other merchandising materials that are normally placed within the vicinity of this terminal.			
Describe the "normal" condition of the ceiling above the terminal (include scuffmarks, fingerprints, dislodged tiles, etc.).			

**Other Checklist Forms are available if merchant has more than 3 terminals or P2PE terminals  
Terminal Review Checklist**

**Swipe Terminal Review Checklist**

Date: \_\_\_\_\_  
 Merchant ID #: \_\_\_\_\_  
 Merchant Name: \_\_\_\_\_  
 Merchant Contact: \_\_\_\_\_  
 Inspected By: \_\_\_\_\_  
 Add'l Info if Needed: \_\_\_\_\_

Complete a copy of this checklist each time you evaluate your terminals and terminal environment.  
 (This form will accommodate three terminal inspections, T1–T3.)

No.	With reference to the relevant Terminal Inventory Form, for each terminal:	Yes / No	T1 TID #	T2 TID #	T3 TID #
<b>Enter the TID # for each terminal here:</b>					
1	Is the terminal in its usual location?	Yes			
		No			
2	Is the manufacturer's name correct?	Yes			
		No			
3	Is the model number correct?	Yes			
		No			
4	Is the serial number printed on the label correct?	Yes			
		No			
5	Is the color and general condition of the terminal as described on the inventory list, with no additional marks or scratches (especially around the seams)?	Yes			
		No			
6	Are the manufacturer's security seals and labels present, with no signs of peeling or tampering?	Yes			
		No			
7	Are the manufacturer's security markings and reference numbers as described on the inventory list?	Yes			
		No			
8	Are all connections to the terminal the same type and color as stated on the inventory, and with no loose wires or broken connectors?	Yes			
		No			
9	Count the number of connections to the terminal. Does this agree with the number stated on the inventory list?	Yes			
		No			
10	Is the condition of the ceiling above the terminal the same as described on the inventory list, with no additional marks, fingerprints, or holes?	Yes			
		No			
11	Is the total number of terminals in use the same as the number of terminals officially installed?			Yes <input type="checkbox"/>	
				No <input type="checkbox"/>	
12	Where surveillance cameras are used, is the total number of cameras in use the same as the number of cameras officially installed?			Yes <input type="checkbox"/>	
				No <input type="checkbox"/>	
				NA <input type="checkbox"/>	

**Swipe Terminal Risk Assessment Form**

**Swipe Terminal Risk Assessment Form**

Date: \_\_\_\_\_  
 Merchant ID #: \_\_\_\_\_  
 Merchant Name: \_\_\_\_\_  
 Contact Name: \_\_\_\_\_  
 Blazer ID: \_\_\_\_\_  
 Add'l Info if Needed: \_\_\_\_\_

This Form enables you to determine the risk category that applies to your particular merchant location. Complete the following questionnaire to determine a "vulnerability score," and therefore the risk category applicable to your merchant premises. For each question, there are two or more possible answers, each of which has a particular value. For each question, enter the relevant value in the "Your Score" column.

No.	Question	Finding	Value	Your Score
1	Where are your merchant premises located?	Office within building (multi-tenant)	1	
		Separate facility/building (single-tenant)	1	
		Remote location (off-campus)	2	
2	Are your merchant premises located in a remote; i.e., low traffic area away from campus?	Yes	1	
		No	0	
3	Are your premises located in an area with quick access to the Interstate?	Yes	1	
		No	0	
4	Are your merchant premises open...	24 hours	2	
		Extended hours	2	
		8-5 (or similar)	1	
5	How many days per week are your premises open?	7	2	
		6 or less	1	
		Seasonal	2	
6	While premises are open, how many staff are on duty?	<3	3	
		4 to 10	2	
		>10	1	
7	During opening hours, do your premises have a duty manager working on site?	Yes	0	
		No	2	
8	Are your staff...	Skilled	0	
		Semi-skilled	1	
		Unskilled	2	
9	Do you employ seasonal staff?	Yes	1	
		No	0	
10	Do you employ casual staff?	Yes	1	
		No	0	
11	Do you have a high turnover of staff (>20 per year)?	Yes	1	
		No	0	
12	Do your premises have a high, regular, or low throughput of customers per day, or do you have peak periods at certain times of the day?	High	3	
		Regular	1	
		Low	1	
		Peak periods	2	
13	Are there particular days in the week when you are very busy?	Yes	1	
		No	0	
14	Are there special times throughout the year when you are particularly busy?	Yes	1	
		No	0	
15	During public holidays, are your merchant premises...	Open	1	
		Closed	0	



No.	Question	Finding	Value	Your Score
16	If you open during public holidays, are these particularly busy days for you?	Yes	1	
		No	0	
		N/A – do not open	0	
17	When your business is closed, are contract cleaners (Non-UAB employees) allowed onto the premises?	Yes	1	
		No	0	
18	If the answer to # 17 is "Yes," are the cleaners escorted?	Yes	0	
		No	1	
19	Do your premises have a camera(s) to monitor & record workstations where payments are processed?	Yes	0	
		No	1	
20	If the answer to # 19 is yes, do staff have access to the camera(s) and the recorded data?	Yes	1	
		No	0	
		N/A – No camera(s)	0	
21	Do you have checkout desks that are not used during normal business hours?	Yes	1	
		No	0	
22	Are checkout desks that are not in use monitored and recorded by a camera(s)?	Yes	0	
		No	1	
		N/A - No camera(s)	0	
23	When not in use, do your POS PED devices remain at the checkout desk?	Yes	1	
		No	0	
24	Are your swipe terminals stand-alone? (separate terminal connected to phone line)	Yes	0	
		No	1	
25	Are your swipe terminals attached to an office workstation? <u>(If using PCI certified P2PE device check No)</u>	Yes	1	
		No	0	
26	If the answer to # 25 is Yes; Can you perform daily office duties on the workstation (i.e., access the Internet, email, etc.)?	Yes	3	
		No	0	
27	Do you have any chip card readers or P2PE swipes already deployed within your infrastructure?	Yes	0	
		No	1	
28	Are all your terminals PCI POS PED approved?	Yes	0	
		No	1	
		Don't know	1	
29	Has your business been approved to PCI Data Security Standards?	Yes	0	
		No	1	
		Don't know	1	
30	Have your premises already been the subject of a payment card fraud attack?	Yes	1	
		No	0	
		Don't know	1	
31	Have your premises been burgled within the last six months?	Yes	1	
		No	0	
<b>TOTAL SCORE:</b>				<b>0</b>

**Risk Category**

When you have answered all questions, the total in "Your Score" column will determine your overall vulnerability score and therefore your risk category.

Complete Terminal Review Checklist:	Risk Category	Score
Weekly	High Risk	More than 25
Monthly	Medium Risk	17-25
Quarterly	Low Risk	16 or Less