THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PAYMENT CARD INDUSTRY COMPLIANCE POLICY

Number: 06.04.17

Division: Finance and Administration – Accounting and Business Services

Date: March, 2021 – Revised August 2, 2022

Purpose: The purpose of this policy is to protect payment card data and to comply with the Payment Card Industry Data Security Standards (PCI DSS) requirements for transmitting, handling, and storage of payment card data.

Scope

The PCI DSS requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data and any system that can alter a system that stores, processes, or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized.

What is PCI?

The PCI DSS are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The PCI SSC is responsible for managing the security standards, while compliance is enforced by the payment card brands. These standards include controls for handling and restricting credit card information, computer and internet security, as well as the reporting of a credit card information breach. The standards are updated as new technology and data breaches make it evident that new security metrics need to be in place to keep card holder data secure.

Related Documents

- UAH Payment Card Processing and PCI Compliance Procedures
- Payment Card Industry Data Security Standard (Current Version)
- 02.02.01 Protection of Data Policy

Responsibilities and Involvement

All departments and areas accepting credit cards either directly or through a third-party vendor or that maintain or have access to credit card information are required to meet the latest version of the PCI DSS and submit Self-Assessment Questionnaire (SAQ) to the UAH PCI Compliance Review Team annually. Achieving these requirements will serve to mitigate the potential of a data breach and remaining PCI compliant will allow them to continue to take payment cards as a method of payment.

Third-party Security Assurance/Risk Management

It is the responsibility of the Procurement Officers to ensure adequate safeguarding provisions are incorporated in contracts that include any external sharing of protected or private UAH data. Contracts for third-party outsourcing must require explicit provisions to meet PCI DSS safeguarding requirements as specified in law, rule, UAH policy, or contractual obligation.

PCI Compliance Review Team

UAHs PCI Compliance Review Team serves in an advisory capacity to the Associate Vice President for Finance & Business Services and Bursar in guiding and monitoring the University's cardholder data environment to ensure compliance with PCI DSS.

Functions

The PCI Compliance Review Team will perform the following functions:

a) Recommend University-wide policies and procedures to ensure compliance with PCI DSS
b) Assist with the evaluation and monitoring of the cardholder data
c) environment, payment card processes, and vendor relationships
d) Oversee annual PCI DSS self-assessment
e) Support and advise departments to comply with PCI DSS and the University's policies and procedures
f) Facilitate communication of PCI DSS changes and best practices
g) Review requests for new merchant locations and advise the University Controller on recommendations for approval or denial of requests

Membership

The PCI Compliance Review Team is comprised of representatives from several key areas of university operations:

- Associate Vice President for Finance & Business Services
- Office of Counsel
- Office of Risk Management and Compliance
- Procurement & Business Services
- Bursar Office
- Office of Student Affairs
- College of Professional and Continuing Studies
- Charger Card Operations
- Office of Information Technology
- Office of Marketing and Communication
- Office of Sponsored Programs
- Athletic Department

Noncompliance

Noncompliance can result in serious consequences for UAH, including reputational damage, loss of customers, litigation, and financial costs. Failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences which may include but are not limited to the loss of the ability to process payment card transactions.

The University Associate Vice President for Finance & Business Services and the Controller each have the authority to restrict and/or terminate merchant account status for noncompliance.

Any known or suspected breach, compromise, or unauthorized access of cardholder data shall be reported immediately to the Vice President for Finance and Administration, the Controller, or the Bursar.

Review: The Vice President for Finance and Administration is responsible for the review of this policy every five years (or whenever circumstances require).

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Payment Card Processing and PCI Compliance Procedures

Contents

Purpose

The University of Alabama in Huntsville ("UAH" or "University") is committed to complying with the Payment Card Industry Data Security Standards (PCI DSS). The purpose of the PCI DSS is to protect cardholder data. This document provides information to ensure UAH complies with the PCI DSS. The UAH Payment Card Industry Compliance Policy (06.04.17) and this accompanying procedures document constitute, in part, UAH's procedures to prevent loss or unauthorized disclosure of payment card information including credit card numbers. Any failure to protect payment card information may result in financial loss for UAH and/or members of the UAH community, suspension of credit card processing privileges, fines, and reputational harm to the University.

Scope and Applicability

The UAH Payment Card Industry Compliance Policy (06.04.17) and these accompanying procedures apply to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with the transmission, storage, or processing of payment card data (including systems that can impact the security of payment card data).

These procedures outline how to properly implement the Payment Card Industry Compliance Policy (06.04.17). Any business on behalf of UAH that involves processing, handling, collection, storage, or disposal of payment card information in any form is subject to policy 06.04.17 and these procedures.

Covered acceptance methods include, but are not limited to, e-commerce (web / online / mobile app payments), mail order/telephone order ("MOTO"), and in-person transactions.

PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. The PCI DSS is maintained by the PCI Security Standards Council, which is a global forum of payment industry stakeholders. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept payment cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org).

PCI DSS COMPLIANCE

In order to accept credit card payments, UAH must be able to demonstrate and maintain compliance with the PCI DSS. This procedures document provides the mechanism for compliance with policy 06.04.17, and thereby ensuring compliance with the PCI DSS for processing, transmitting, storage, and disposal of cardholder data of payment card transactions to reduce the risk associated with the administration of credit card payments by any entity at, or on behalf of, UAH and to ensure proper internal control and compliance with the PCI DSS.

PCI DSS Compliance is an ongoing process, not a one-time event. The PCI DSS emphasizes "Business as Usual" (BAU); performing continuous compliance activities in an ongoing manner 24 hours a day, 7 days a week, 365 days a year.

Authoritization to Process Payments

UAH requires all departments, units, and affiliated entities that accept payment card payments to be properly authorized to do so and must do so in compliance with PCI DSS and other relevant payment card industry standards and in accordance with policy 06.14.17 and this procedures document.

Student Organizations and Clubs are prohibited from obtaining a merchant account. Please direct questions regarding the use of payment card services by Student Organizations and Clubs to the Associate Vice President Finance & Business Services.

Employees and agents of UAH are prohibited from accepting funds via any payment method(s) which require funds to flow through personal bank accounts (e.g., PayPal, Venmo, Square, etc.).

Individuals found to have violated the Payment Card Industry Compliance Policy (06.14.17) or this procedural document, whether intentionally or unintentionally, may be subject to disciplinary action up to and including termination and could limit a department's payment card acceptance privileges. Reference the "Sanctions" section of this procedural document for additional information.

Requirements

UAH requires that:

- UAH members must follow policy 06.14.17 and these accompanying procedures.
- Any department, unit, or other affiliated entity accepting payment card data, either at UAH or through a Service Provider, must designate an individual to serve as a Merchant Department Responsible Person (MDRP) who will have primary authority and responsibility for payment acceptance and overseeing PCI DSS compliance at the department/unit level.
- All UAH departments/units/entities accepting payment cards and all employees of the departments designated to accept payments cards will be trained upon hire and annually on PCI DSS, the UAH Payment Card Industry Compliance Policy (06.14.17), these procedures, and must electronically sign the **PCI Security Awareness Training & Confidentiality Agreement** prior to performing that work.
- UAH will perform a background check on potential personnel who will handle payment card data prior to hire or transfer to minimize the risk of attacks from internal sources. This check is completed by UAH Human Resources Department. Department/unit heads are responsible for notifying Human Resources when new or current employees are assigned payment card roles and responsibilities.
- UAH departments/units/entities accepting payment cards will utilize only dedicated, approved equipment to process card payments.
- UAH departments/units/entities accepting payment cards will never store cardholder data. Recurring payments will need to be configured to use tokenization.
- UAH departments/units/entities will ensure that all credit card transactions are

reviewed and reconciled to daily merchant reports. Merchant reports are to be submitted daily to the Bursar's Office.

- All payment devices that process credit cards must be stored in a locked space with limited access when not in use. Access to devices that are not deployed are kept in storage spaces with access limited to the PCI Coordinator and specified designates. All access to these spaces are tracked through door access. Access to deployed units while in use must be limited to the department merchant users and must not be left unattended.

- OIT and all distributed IT administrators employ up-to-date security measures in firewall configuration, network administration, and other areas that could affect our PCI Compliance.

PCI DSS Policy

Merchant Department Responsible Person (MDRP)

Any department/unit accepting payment card and/or electronic payments on behalf of UAH for gifts, goods, or services ("Merchant Department") must designate an individual (staff or faculty member) within that department/unit who will have primary authority and responsibility for e-commerce, payment card transaction processing, and third party Service Providers accepting payment cards on behalf of UAH. This individual will be referred to in the remainder of this policy statement as the Merchant Department Responsible Person or "MDRP".

Each Merchant Department must have a MDRP at all times. It is the responsibility of the MDRP and the MDRP's direct supervisor to ensure this role is filled. The direct supervisor must record and track any change in MDRP's.

MDRP Responsibilities include, but are not limited to, the following:

● Ensure agents of UAH, with access to or who can affect the security of payment card data, complete the PCI Security Awareness Training Computer Based Training program upon hire and annually.

● Ensure job descriptions, for employess and/or agents of UAH that will have access to any payment cards, include a background check prior to hire.

● Ensure only dedicated, approved hardware/software is utilized to process card payments. Payment solutions such as Paypal, Venmo, Square or other methods which require funds to flow through personal bank accounts are prohibited.

● Be aware of all payment processes and practices within their Merchant Department. All changes to processes and practices must be reviewed and approved by all affected parties.

● Ensure all agents of UAH receive, and are trained on, the Merchant Department Specific Standard Operating Practice(s) (**Appendix 5**) upon hire and annually. Ensure these department specific Standard Operating Practices are adhered to.

● Ensure that all payment card transactions are reviewed and reconciled to daily merchant reports. These transactions must be turned into the Bursar's Office daily.

● Ensure all Point of Sales (POS) devices, including cellular based stand-alone swipe terminals and point of sale systems, are maintained under a state of consistent control and supervision.

● Ensure Point-of-sale devices/terminals (cash registers, stand-alone swipe terminals etc.) are physically secured and inspected for tampering on a regular basis.

For Merchant Account requests, the MDRP must follow the processes noted in the Client Process Set-Up Outlines (**Appendix 4**). These steps must be completed at least two (and preferably four) weeks prior to the event.

Authorization

● Limit access to system components and cardholder data to only those individuals whose job requires such access.

● The level of access is determined by job requirements; based on the least privilege model

● Sensitive areas are physically secured and sign in logs are utilized.

● Sufficient controls are in place to identify individuals entering and exiting sensitive areas.

● Each Merchant Department must maintain a current list of employees and review monthly to ensure that the list reflects the most current access needed and granted.

Credit Card Acceptance and Handling

● In the course of doing business at UAH, it may be necessary for a department or other unit to accept payment cards. The opening of a new merchant account for the purpose of accepting and processing of payment cards is done on a case by case basis. Any fees associated with the acceptance of payment cards in that unit, will be charged to the unit (including but not limited to; infrastructure, security and management, i.e firewall, switch, network cables).

● See Transmitting for acceptable methods of payment card acceptance.

● Interested departments should contact the PCI Compliance Team to begin the process of accepting credit cards. Steps include:

- Contact the PCI Compliance Team

- Review the Client Set-up Processes (**Appendix 4**)

-Read UAH Payment Card Industry Compliance Policy (06.04.17) and these Payment Card Processing and PCI Compliance Procedures

-Completion of PCI Training Program

● All payment card transactions must be reviewed daily (business days) and reconciled to daily merchant reports. Daily reconciliation reports are to be sent to the Bursar's Office. Failure to reconcile payment card transactions in a timely manner is cause for the merchant department payment card processing privilege to be suspended. Specific details regarding processing and reconciliation will depend upon the method of payment card acceptance and type of merchant account.

Transmitting

● Employees must be discreet and use common sense when handling cardholder data.

● Payment cards may be accepted in the follow manner:

- In person (card present)

- Direct telephone contact (telephone order); the constituent on the telephone should verify the payment card information twice, agents of UAH should not read the payment card data back to constituent

-Through a PCI DSS compliant system that is entirely hosted by a PCI DSS compliant third party organization (e-commerce) and approved by the PCI Compliance Team

- Physical mail - which must be logged according to Cash Handling Policy

● Cardholder data must not be accepted or sent via end user messaging technologies; email, text message, SMS, chat etc. UAH Email will not allow the transmittance of cardholder data. Advise any potential clients that attempting to transmit cardholder data over email or any other user messaging technology will not be processed. Then educate him/her on the appropriate methods of conveying a credit card payment. See above for appropriate acceptance methods.

- Do not reply to an email which contains cardholder data;
- Delete the email and then subsequently remove it from the trash folder;
- Notify the sender that cardholder data cannot be accepted via email.

● Constituent Cardholder data must not be accepted or sent via fax. If a fax is received with cardholder data, immediately shred in a crosscut shredder. Notify the PCI Compliance Team with the name, date, location the cardholder data was received. Follow up with the constituent and advise this method of transmitting cardholder data is not secure. Advise the constituent we cannot process the payment and educate him/her on the appropriate methods of conveying a credit card payment. See above for appropriate acceptance methods.

● Merchant departments must maintain strict control over the internal and external distribution of any kind of media that contain cardholder data. No media containing cardholder data may leave the premises of the department that accepted it for processing. Materials sent to constituents, with a designated area for written cardholder data, to be returned to UAH must have the return address of the department that will process the cardholder data on the return instrument. Every effort should be made to eliminate the area for written cardholder data on appeals, instead noting a secure means to make a credit card payment on secure online forms, by check, or phone.

● In the rare instance that an agent of UAH is offered payment card information during an off-site visit, the agent will provide the donor with a transmittal form or direct the constituent to an approved method of payment (i.e. online donation site, phone). The constituent may then fill out the form and mail it directly to the appropriate office at UAH. For compliance and security The University of Alabama in Huntsville employees must not store or take possession of cardholder data (CHD) while off-site.

● All equipment used to collect payment card data must be secured against unauthorized use or tampering in accordance with the PCI Data Security Standard.

Processing

● Cardholder Data received for manual processing (mail, hand delivered) must be processed in a credit card merchant account the same day it is received if possible; but absolutely no later than 1 business day (excluding calendar and fiscal year end periods). Cardholder data in written form is redacted immediately following authorization in the payment gateway. Acceptable forms of redaction are crosscut shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

● Refunds must be processed using the same credit card for the transaction. A different card may not be used; however a paper check may be issued through Accounts Payable.

● Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing card holder data.

● Mask the Primary Account Number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.

Storage

● The University of Alabama in Huntsville does not store authorized cardholder data (media), in hardcopy or electronic form.

● The University of Alabama in Huntsville does not store Sensitive Authentication Data; including the primary account number (PAN), expiration date and service code (CVV).

● Cardholder data that is collected but has not yet been processed (pending authorization in payment gateway), in addition to any USPS mail that hasn't been opened, must be stored in a secure location (locked safe, locked file cabinet), see Processing above. Only authorized staff shall have access to the keys/combination.

● Cardholder data may not be stored on any portable devices including but not limited to USB flash drives, cellular phones, personal digital assistants and laptop computers.

● Cardholder data may not be stored in logs (for example, transaction, history, debugging, error), history files, trace files or database contents.

Disposal

● Cardholder data must be disposed of in a certain manner that renders all data unrecoverable. This includes hard copy (paper) documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices.

● The approved methods of disposal for hardcopy media are:

-Cross-cut shredding

-Incineration

● The approved method of disposal, rendered unrecoverable, for electronic media:

-Secure wipe program

-In accordance with industry-accepted standards for secure deletion

-Physically destroying the media until it is rendered unrecoverable

Physical Security and Skimming Prevention of Payment Card Processing Devices

The UAH Bursar will maintain an up-to-date inventory of all devices that capture payment card data. The designees utilizing such devices are responsible for providing the following information to the Bursar immediately upon acquisition, relocation, or decommissioning of all such devices:

- Make
- Model
- Serial number (or other method of unique identification)
- Location

Designees utilizing such devices must ensure that device lists are updated as changes (additions, relocations, decommissioning) occur.

The designee utilizing these devices will protect card present processing devices from tampering or substitution in adherence to the below requirements:

- A monthly physical inspection must be performed, documented and retained by each department; inspection documentation must be made available for review by the PCI Compliance Review Team upon request.
- Systems not in use must be secured in a locked facility and regularly inventoried. Retain inspection logs for a minimum of one year.
- Cashiers must perform a daily visual inspection of devices that capture payment card data.
- Portable payment card processing devices must be stored securely in a locked area when not in use.

Security Awareness Program

All persons with physical and logical access to any UAH payment processing environment, whether employees, third parties, service providers, contractors, temporary employees, and/or other staff members, must be trained on their role in protecting UAH and the campus community from financial, operational, and reputational threats and risks.

● Upon hire and at least annually, all users connected to the UAH cardholder data environment (in any way), are to complete the UAH PCI Training program.

● Attendance logs for those who attend PCI training, must be kept by the PCI Compliance Team.
● Read this Payment Card Processing and PCI Compliance Procedures document.

Security Breach

An 'incident' is defined as a suspected or confirmed 'data compromise'. A 'data compromise' is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted data is collected, processed, stored or transmitted; payment card data is prohibited data. A 'data compromise' can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

In the event of a breach or suspected breach of security, the department must immediately execute each of the relevant steps detailed below:

● The MDRP or any individual suspecting a security breach must immediately notify the Office of Risk Management and Compliance, in accordance with the Incident Response Plan (**Appendix 1**), of an actual breach or suspected breach of payment card information. Email should be used for the initial notification and include a telephone number for the Office of Risk Management and Compliance to respond to. Details of the breach should not be disclosed in email correspondence.

● Notify the MDRP and the department head of the unit experiencing the suspected breach.

● The MDRP or any individual suspecting a security breach involving e-commerce also must immediately ensure that the following steps, where relevant, are taken to contain and limit the exposure of the breach:

-Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on at all to the machine and/or change passwords)

-Do not switch off the compromised machine; instead, isolate the compromised system(s) from the network by unplugging the network connection cable.

-Preserve logs and electronic evidence.

-Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation:

● Date and time

● Action taken

● Location

● Person performing action

● Person performing documentation

● All personnel involved

● Be on HIGH alert and monitor all e-commerce applications

If a suspected or confirmed intrusion / breach of a system has occurred, the Office of Information Technology will follow guidance from Office of Counsel. Actions may include alerting insurers, the merchant bank, the payment card associations, Campus Safety, local authorities, The University of Alabama in Huntsville Chief Financial officer and the Chief Information Officer. A detailed incident response plan (**Appendix 1**) will be maintained by the Office of Information Technology.

Service Provider Management

Service Providers (third parties) are contractually required to adhere to the PCI DSS requirements. Due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with UAH‘s cardholder data environment. The written agreement shall include an acknowledgement by the service providers of their responsibility for securing cardholder data and breach liability language, which will be evaluated by Legal Counsel: This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.

● The Office of the Bursar must obtain the appropriate PCI Compliance documentation, from Service Providers, on an annual basis prior to the expiration date of the current documentation.

● Service Providers must provide either an SAQD-Service Provider AOC or an On-Site Assessment AOC for Service Providers. AOC’s must note specific requirements the Service Provider is attesting to.

The Office of the Bursar will maintain a collective, current and accurate list of Service Providers with the following information:

- Service Provider Name
- Service being provided (description)
- PCI Validation Required
- Validation Date
- Expiration Date
- Assessor
- Functional Area

Student Organizations

Student Organizations are NOT ALLOWED to accept monies via Paypal, Venmo, Square or other method which requires funds to flow through personal bank accounts.

All money collected from fundraisers or dues must be deposited directly into the organization's university account. No organizational money should ever be deposited into a personal banking account.

Student Organizations must contact the Associate Vice President Finance & Business Services for possible payment processes. The MDRP for all Student Organizations must be a full-time employee for the Office of Student Life.

Third Party Processor Procedures

When deciding on a third party processor make sure to include the Bursar's office. New processors must be approved through the Bursar's Office before they can be used on behalf of UAH. Ensure contracts include language that states that the service provider or third party vendor is PCI compliant and will protect all cardholder data. In addition, the contract must be approved through the Contract Approval Process by the Office of Counsel. Third-party processors must have a completed and current Attestation of Compliance form on file with UAH. Annually audit the PCI compliance status of all service providers and third-party vendors. A lapse in PCI compliance should result in the termination of the relationship, and it is strongly recommended that contracts include such a cancellation clause.

PCI Compliance Review Team Duties

The PCI Compliance Team is responsible for auditing PCI DSS compliance at UAH, and for advising University officials on matters related to PCI DSS compliance. These responsibilities include but are not limited to the following:

- Perform quarterly Physical Inspections on payment card processing devices, as noted in the section on Physical Security and Skimming Prevention.

- Ensure all Point of Sale (POS) devices have updated patches and antivirus with up to date logging. Retain logging and audit trail history for a minimum of one year.
- Verify and collect PCI DSS Compliance Certificates or PA-DSS Validation Certificate (POS systems) on all service providers within the relevant Merchant Department on an annual basis.
- Coordinate with the MDRP for each department on campus. Ensure user access to the cardholder data environment, within the relevant Merchant Department, is revoked when the individual's job no longer requires access to the Cardholder Data Environment (CDE). Maintain an audit log of user access to the cardholder data environment for a minimum of one year.
- Validate compliance for the merchant department on an annual basis.
- Complete the Self-Assessment Questionnaire (SAQ).

Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with payment cards for affected units. Additionally, if appropriate, any fines and assessments which may be imposed by the affected payment card company will be the responsibility of the impacted unit. In the event of a breach or a PCI violation the payment card brands may assess penalties to UAH which will be passed on to the unit. A one-time penalty of up to $500,000 per branch per breach can be assessed as well as on-going monthly penalties.

Additionally, the impacted unit may be responsible for data breach response costs not covered by insurance. The UA System currently maintains a $500,000 [KLB1]self-insured retention for data breaches (which include both electronic and hard-copy data breaches). First-party costs (costs to UAH to investigate and respond) for data breaches may not be covered under existing insurance programs and are subject to applicable retention and deductibles.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University of Alabama in Huntsville will carry out its responsibility to report such violations to the appropriate authorities.

FAQ's

1. What do I do if someone emails me credit card information?

Email should not be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information.

How long should I hold onto card holder data?

Cardholder data should not be retained any longer than a documented business need; after which, it must be deleted or destroyed immediately following the needed use. A regular

schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the time needed.

Definitions

Term	Definition
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Payment card Brands: ● Visa, MasterCard, American Express, Discover, JCB
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a payment card.
Card Holder Data (CHD)	Those elements of payment card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.
Cardholder Name	The name of the Cardholder to whom the card has been issued.
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media

	including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with the (Institution's) Electronic Data Disposal Policy). The approved disposal methods are: ● Cross-cut shredding, Incineration, Approved shredding or disposal service
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept payment cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for payment card transactions.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.

Appendix 1- Incident Response Plan

Purpose

The Payment Card Security Incident Response Plan supplements The University of Alabama in Huntsville Incident Response Plan.

To address credit cardholder security, the major card brands (Visa, MasterCard, Discover, American Express and JCB) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create a Security Incident Response Team (Response Team) and document an Incident Response Plan (IRP).

This document defines those responsible, the classification and handling of, and the reporting/notification requirements for incident response plan at UAH.

Scope/Applicability

A list of the merchants and operations with payment card acceptance and IP addresses has been provided to the Information Technology Security Office to identify the areas of accepting payment cards.

Authority

The University of Alabama in Huntsville Credit Card Security Incident Response Team and PCI Compliance Team

Communication for the Response Team can be sent to the Office of Counsel and copies to the Office of Risk Management and Compliance.

Name	Department/Title	Telephone	Email
Robert Leonard	Associate Vice President Finance & Business Services	256.824.2233	Robert.Leonard@uah.edu
Mike Huff	Office of Counsel	256.824.6633	Michael.Huff@uah.edu

Name	Department/Title	Telephone	Email
Kevin Bennett	Chief Risk and Compliance Officer	256.824.6875	Kevin.Bennett@uah.edu
Terence Haley	Director of Procurement & Business Services	256.824.6674	haleyt@uah.edu
Dani Hillman	Bursar	256.824.6223	Dani.hillman@uah.edu
Kristi Motter	Vice President for Student Affairs	256.824.5715	Kristi.Motter@uah.edu
Karen Clanton	College of Professional and Continuing Studies	256.824.6014	Karen.Clanton@uah.edu
Mallory Spragins	Charger Card Operations	256.824.2720	Mallory.Spragins@uah.edu
Russ Ward	Chief Security Officer	256.824.2623	Russ.Ward@uah.edu
Elizabeth Gibisch	Executive Director, Marketing and Communications	256.824.6926	Elizabeth.Gibisch@uah.edu
Gloria Greene	Office of Sponsored Programs	256.824.2657	Gloria.Greene@uah.edu
Laura Taube	Athletics	256.824.6332	Laura.Taube@uah.edu

Procedures

Incident Response Plan (IRP)

The Incident Response Plan needs to take into account that incidents may be reported/identified through a variety of different channels but the Incident Response Team will be the central point of contact and responsible for executing The University of Alabama in Huntsville Incident Response Plan.

The University of Alabama in Huntsville security incident response plan is summarized as follows:

1. All incidents must be reported to the Response Team.
2. The Response Team will confirm receipt of the incident notification.
3. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

An 'incident' is defined as a suspected or confirmed 'data compromise'. A 'data compromise' is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted data is collected, processed, stored or transmitted; Payment Card data is prohibited data. A 'data compromise' can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

In the event of a suspected or confirmed incident:

1. Contact the Response Team by sending an email documenting the incident to…

   riskmanagement@uah.edu

2. The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
3. If the incident involves a payment station (PC used to process credit cards):
   a. Do NOT turn off the PC.
   b. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
4. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
5. Assist the Response Team as they investigate the incident.

Incident Response Team Procedures

The University of Alabama in Huntsville Credit Card Security Incident Response Team must be contacted by a department in the event of a system compromise or a suspected system compromise. After being notified of a compromise, the Response Team, along with other designated staff from Information Technology, will implement their incident response plan to assist and augment departments' response plans.

In response to a system compromise, the Response Team and Information Technology will:

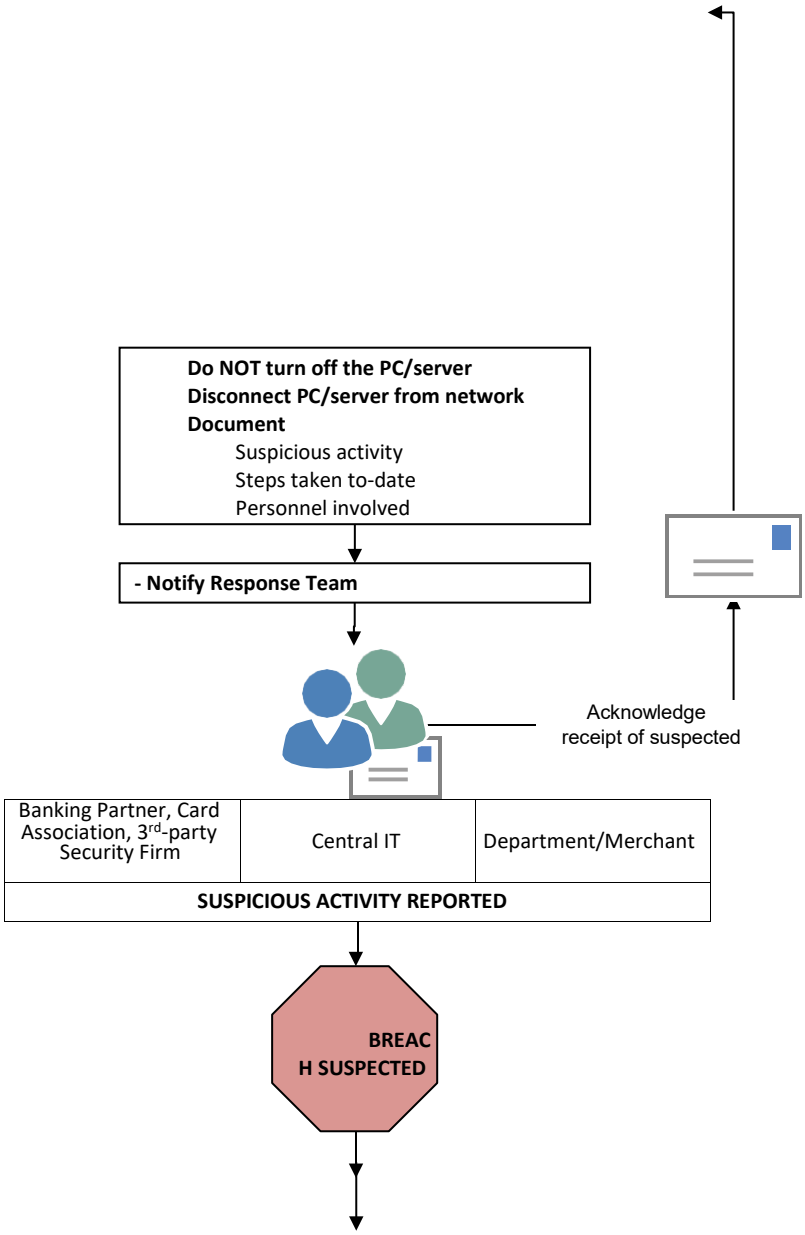
1. Ensure the compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs and alerts.
3. Assist department in analysis of locally maintained system(s) and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system(s).
5. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, Chief Risk and Compliance Officer, depending on the nature of the data compromise, must notify the appropriate organizations that may include the following:
    a. The University of Alabama in Huntsville Chief Financial Officer and the Chief Information Officer
    b. The University of Alabama in Huntsville's Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with the card brands (VISA, MasterCard)
        i. see Bank Breach Response Plan-find
        ii. see Visa – Responding to a Breach-find
        iii. see MasterCard – Responding to a Breach-find
    c. If American Express payment cards are potentially included in the breach the unit is responsible for notifying and working with American Express
        i. For incidents involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident.
            1. Phone number: (888) 732-3750
            2. Email: EIRP@aexp.com.
        ii. For more detail see American Express – Responding to a Breach
    d. If Discover Network payment cards are potentially included in the breach the unit is responsible for notifying and working with Discover Network.
        i. If there is a breach in your system, notify Discover Security within 48 hours.
            1. Phone Number: (800) 347-3083
        ii. For more details see Discover Network – Fraud Prevention FAQ
    e. Campus police and local law enforcement
    f. UA System Office of Risk and Compliance, and affected insurance providers
    g. Chief University Counsel
6. Assist card industry security and law enforcement personnel in the investigative process.

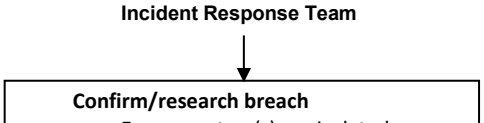
Bank Breach Response Plans

The credit card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. For Visa and MasterCard it is the unit's responsibility to notify their own bank (the financial institution(s) that issues merchant

accounts to UAH and the UAH bank will be responsible for notifying Visa and MasterCard, where applicable.

Flow Chart for Suspected Breach





Issue FINAL incident report
Prioritize/complete any remediation items

Symptoms of Data Breaches

The following are common symptoms to look for in a data breach.

- A system alarm or similar indication from an intrusion detection tool
- Unknown or unexpected outgoing Internet network traffic from the payment card environment
- Presence of unexpected IP addresses or routing
- Suspicious entries in system or network accounting
- Accounting discrepancies (e.g. gaps in log-files)
- Unsuccessful login attempts
- Unexplained, new user accounts
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Unexplained, new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system executable files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial of service or inability of one or more users to log in to an account
- System crashes
- Poor system performance
- Unauthorized operation of a program or sniffer device to capture network traffic
- Use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts
- Unusual time of usage
- Unauthorized wireless access point detected

Card Association Breach Response Plans

Visa – Responding to a Breach

Follow the steps set forth in the resource:

https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Initial Steps and Requirements for Visa Clients (Acquirers and Issuers)

(A full description of the steps is available at the link listed above)

Notification

1. Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region.
2. Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.

Preliminary Investigation

3. Perform an initial investigation and provide written documentation to Visa within three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

MasterCard – Responding to a Breach

The MasterCard Account Data Compromise User Guide sets forth instructions for MasterCard members, merchants, and agents, including but not limited to member service providers and data storage entities regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program.

http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

Initial Steps and Requirements for MasterCard Clients

(A full description of the steps is available at the link listed above)

Notification

1. Immediately report to MasterCard the suspected or confirmed loss or theft of cardholder data. Clients must submit a Report of Potential Account Data Compromise in the MasterCard Connect site.

Investigation

2. Perform an investigation and provide written documentation to MasterCard within fifteen (15) business days. The information provided will help MasterCard understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

American Express – Responding to a Breach

Merchants must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750/US only, or at 1-(602) 537-3021/International, or email at EIRP@aexp.com. Merchants must designate an individual as their contact regarding such Data Incident.

For more complete language on the obligations of merchants and service providers see the following 2 documents:

- American Express® Data Security Operating Policy for Service Providers https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Service_P rovider_US.pdf
- American Express Data Security Operating Policy – U.S.

https://icm.aexp-static.com//Internet/NGMS/US_en/Images/DSOP_Merchant_US_Apr15.pdf

Incident Classification, Risk Analysis and Action Matrix

Each incident should be reviewed based on the risk and action matrix, which attempts to reflect the severity of the incident and its impact. Then, decisions on whether to develop further controls and processes can be made so work-tickets can be created and prioritized so that identified vulnerabilities are addressed.

	Security Problem Family				
Security Problem	**Unlawful Activity**	**Violation of Appropriate Usage Policy**	**Data Disclosure**	**Network Device Compromises**	**Vulnerabilities**
PCI-DSS Breach Distribution of Copyrighted Material Breach of HIPPA Breach of Telecommunications Act	1				
Confidential data at risk of disclosure to the Internet. Highly Confidential of a personal nature data at risk of disclosure to the network.			1		
Confidential data, of a personal nature at risk of disclosure to network.			2		
Network resources providing un-authenticated access to data not intended for public distribution.			3		
Tools installed which present a significant risk to network stability				1	
Malicious Software. E.g. Virus/Trojan. No User Interaction Required for infection				1	
Port Scanning		2		2	
Unauthorized Publishing Service that can be used for content distribution. E.g. FTP Server.				2	
Malicious Software. E.g. Virus/Trojan. User interaction required for infection.				3	
Vulnerability more than one week old that allows arbitrary code to be run					4
Highly Insecure Configuration					4
Vulnerability less than one week old that allows arbitrary code to be run					5

Action Class	Actions to be taken by Response Team	Escalation Process	Default Action Period
1	- If required, completely block all network access. - Phone call to Response Team to notify of the problem, if IT Security and Risk Officer unavailable, call to CIO or Senior Manager. - If required, duplicate disks. - For network device compromise notify Regional CERT (US-CERT or AUS-CERT) of suspected source IP.	- If action not completed in required time, Alert CIO and/or Senior Management of the affected Area.	1 hour
2	- If required, block direct Internet access. - E-mail sent to Response Team. - Phone call to IT Security and Risk Officer to notify of the problem. - For network device compromise notify Regional CERT (US-CERT or AUS-CERT) of suspected source IP. - If required, duplicate disks.	- If action not completed in required time, escalate to Class 1 - Alert Service, System or Application Manager as appropriate.	2 Hours
3	- E-mail sent to Response Team. - Phone IT Security Officer for region. - For network device compromise notify Regional CERT (US-CERT or AUS-CERT) of suspected source IP.	- If action not completed in required time, escalate to Class 2	4 Hours
4	- E-mail sent to Response Team.	- If action not completed in required time, escalate to Class 3	1 Day
5	- E-mail sent to Response Team.	- If action not completed in required time, escalate to Class 4 - If a network device is compromised escalation is to Class 3	1 Week

Appendix 2

Department Application for New Payment Card Merchants and Renewal Survey

Purpose

To be completed by Departments that would like to accept payment cards (Visa, Master Card, American Express, Discover cards and debit cards) as a form of payment for goods and/or services, receipt of donations, non-tuition courses, conferences, seminars, tickets and other approved The University of Alabama in Huntsville related products.

Please read Payment Card Handling Policy and Payment Card Procedures prior to completing this application to make sure that your Department will be able to comply with all the requirements listed in The University of Alabama in Huntsville procedures.

Application must be submitted to Bursar's Office. Once the application has been approved, please allow at least two weeks for electronic terminals and four weeks for web based setup prior to the desired "live" date. The information provided on this application will be used to create an "Information Profile" that will be submitted to our processor, Elavon.

Best Practices for Offices Accepting Payments Cards

We understand that complying with the PCI DSS may be difficult and confusing for some departments. If you have identified a business need that requires you accept credit card payments we recommend that you review this set of high-level best practices before you complete this application.

1. If you don't need it, don't store it!
   - Many offices retain cardholder data (CHD) "just because." If you keep the transaction number and date, you can always ask the acquiring bank for the CHD if you need it.
   - This includes paper and forms. Once the transaction has been processed, destroy the CHD on the form. This may require a redesign of the form to move the CHD to the bottom where it can be properly removed and cross-cut shredded.
2. Proper destruction
   - All forms or paper with CHD should be shredded in a "cross-cut" type shredder.
   - Third-party shredding services may be used, providing the bins that they provide are secure and cannot be removed from the area.
3. Online Payment Card Systems

- Many departments employ the use of third-party payment systems to outsource card processing to an online process. Many times it is considered good customer service to take phone calls, emails or some other form of communication to process a credit card transaction.
    a. It is not recommended to act as the customer and input their data for them.
    b. When it is necessary to provide this service: transactions should be conducted on a separate (isolated) payment terminal.

4. Maintain clean desk policy
    - CHD should not be left out on desks or in open areas when not needed. Even if leaving the desk for a short period, staff should keep material in a folder and lock the folder in the desk when they leave temporarily. At the end of the day, all CHD should be stored in a secure file cabinet or safe.
5. Electronic storage of CHD
    - Do not copy or type CHD into spreadsheets or documents on general use workstations even for temporary use. Even if you don't save the document, an image or file of the data is stored on the hard drive.
6. Never email Credit Card information
    - Staff should never use email as a manner of transmitting Cardholder data
    - Should a customer email their credit card information:
        a. Reply to the sender, deleting the credit card information from the reply and inform them that "for their protection and the protection of UAH, policies dictate that credit card information shall not be accepted via email. Please use one of our accepted methods of processing your information: (in-person, online, fax, form, etc)."
7. Do not allow unauthorized persons unaccompanied access to areas where credit card data are stored or processed
    - This includes other The University of Alabama in Huntsville staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This sometimes requires a change in service times.
8. Document Desk Procedures
    - To ensure continuity when office personnel are out, have all individuals' document daily procedures for their role in the handling of confidential data. Include such items as receipt and processing procedures, disposition and destruction of CHD. Storage and transfer of forms within the office.

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

1. DEPARTMENT INFORMATION:

DEPARTMENT NAME: _____

MERCHANT (LOCATION) NAME: _____

Note: The merchant (location) name will appear on your customer's monthly statements and on the bank statements sent to the Controller's Office

INTERNET ADDRESS: _____

MERCHANT (LOCATION) ADDRESS: _____

Note: Merchant address must include Building & Room number. Statements will be mailed to this address.

2. PRIMARY CONTACT INFORMATION:

CONTACT NAME: _____ MAIN TELEPHONE #: _____

CONTACT TITLE: _____ ALT. TELEPHONE #: _____

EMAIL ADDRESS: _____ FAX NUMBER: _____

Note: Primary contact will be responsible for the overall process of accepting payment cards at this location and must be a full time employee. (Work Study employees are not allowed).

3. MERCHANT INFORMATION:

GIVE A BRIEF DESCRIPTION OF YOUR PAYMENT CARD BUSINESS:

(What is the main purpose of this merchant account? For example, registration fees, tuition for non-credit courses, tickets for events)

DATE SUBMITTED: _____ DESIRED "LIVE" DATE: _

TRANSACTION TYPE TO BE ACCEPTED (Mark with an X):

Note: Debit cards will be processed the same as credit cards.

( ) VISA ( ) AMERICAN EXPRESS ( ) DEBIT

( ) MASTERCARD ( ) DISCOVER

ESTIMATED ANNUAL CREDIT CARD VOLUME:

Total Annual Dollar Amount: $___

Average Amount per Transaction: $___

Annual Number of transactions: ____

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

PROCESSING TYPES (Check the types of system currently being used or will be used):

( ) POS Terminals ( ) Internet (Online) ( ) Other

If Other, describe in detail: _____

Current Third Party Vendor, if applicable: _____

CHARGEBACK INFORMATION:

Mail "Chargebacks" to (Provide name, title, and address including building and room #)

CONTACT NAME: _____ ADDRESS: _

CONTACT TITLE: _____ _

Note: Chargebacks are created when a customer disputes a charge. If action is not taken by the merchant within the time frame indicated on the letter, the {INSTITUTION NAME} will be charged by the payment card company. A journal entry must be made by the merchant to record such chargeback. If assistance with Chargebacks is needed, please call the Bursar's Office.

IF PROCESSING USING A POINT OF SALE (POS) ELECTRONIC TERMINAL, PLEASE PROVIDE:

MODEL	FIRMWARE/SOFTWARE VER.	SERIAL NUMBER

IF PROCESSING OVER THE INTERNET, PLEASE PROVIDE:

CONTACT NAME:
(Technical) _____ TELEPHONE #:

CONTACT TITLE: _____ EMAIL ADDRESS:

_____

_____

FOR PROCESSING JOURNALS, PLEASE PROVIDE:

CONTACT NAME: _____ TELEPHONE #:

CONTACT TITLE: _____ EMAIL ADDRESS:

_____

_____

FOR PROCESSING CHARGEBACKS, PLEASE PROVIDE:

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CONTACT NAME: _____ TELEPHONE #:
CONTACT TITLE: _____ EMAIL ADDRESS:

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

DEPARTMENT ACCEPTS PAYMENT CARDS (Check all that apply):

( ) **IN PERSON**
( ) **BY PHONE**
( ) **BY MAIL**
( ) **BY FAX**
( ) **ONLINE PAYMENT VIA UNIVERISTY'S APPROVED INTERNET PROCESSOR** **(name of provider)** _____
( ) **ONLINE PAYMENT VIA OTHER, NAME:** _____

---

4. PROCESSING INFORMATION

1. Have you, or your employees, received training on how to operate an electronic terminal?

YES ( ) NO ( ) If NO, please explain _____

2. Do you, or your employees, have written instructions on how to operate an electronic terminal?

YES ( ) NO ( ) If NO, please explain _____

3. Do you cross-cut shred documents that contain sensitive payment card information immediately after the transaction is processed?

YES ( ) NO ( ) If NO, please explain _____

4. Are payment card numbers truncated on the receipt?

YES ( ) NO ( ) If NO, please explain _____

5. Is the electronic terminal kept in a secured and restricted area, away from public access?

YES ( ) NO ( ) If NO, please explain _____

6. Is a "unique code" assigned to each person with access to payment card processing and is this code <u>not</u> shared with another person?

YES ( ) NO ( ) If NO, please explain _____

7. Is the electronic terminal connected to an analog line?

YES ( ) NO ( ) If NO, please explain _____

8. If accepting payment card information by fax, is the fax machine in a secured area and are the faxed documents destroyed immediately after the transaction is processed?

YES ( ) NO ( ) If NO, please explain _____

9. Are The University of Alabama in Huntsville*"Payment Card Processing Procedures"* being followed by employees involved in payment card handling?

YES ( ) NO ( ) If NO, please explain _____

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

10. Do you educate employees on practices for accepting and processing payment cards and closing out batches?

YES ( ) NO ( ) If NO, please explain _____

11. Do you, or your employees, audit transactions and settle batches daily?

YES ( ) NO ( ) If NO, please explain _____

12. Do you have a back-up to process transactions daily in your absence?

YES ( ) NO ( ) If NO, please explain _____

13. Do you, or your employees, take every measure possible to prevent duplicate entries?

YES ( ) NO ( ) If NO, please explain _____

14. Have employees responsible for processing journals received payment card journal training?

YES ( ) NO ( ) If NO, please explain _____

15. Do you educate employees on common types of payment card fraud and how to counteract them?

YES ( ) NO ( ) If NO, please explain _____

16. Do you educate employees on common types of merchant mistakes and how to avoid them?

YES ( ) NO ( ) If NO, please explain _____

17. Do you request background checks for employees involved in payment card processing, or employees that have access to such data?

YES ( ) NO ( ) If NO, please explain _____

18. Do you have background check documentation on file?
YES ( ) NO ( ) If NO, please explain _____

19. Do you require employees to acknowledge, at least annually, that they have read and understood the The University of Alabama in Huntsville policies and procedures on payment card processing by completing the Employee Statement of Understanding

(link)?

YES ( ) NO ( ) If NO, please explain _____

20. Do you have the ability to process payment cards if normal modes of processing are down?

YES ( ) NO ( ) If NO, please explain _____

21. Do you limit the number of employees who process payment cards to appropriate employees based on their job duties?

YES ( ) NO ( ) If NO, please explain _____

22. Do you keep the Office of the Controller aware of any changes in your payment card program?

YES ( ) NO ( ) If NO, please explain

23. Is access to payment cardholder information restricted to users on a need to know basis?

YES ( ) NO ( ) If NO, please explain

24. When an employee leaves the Department, is his/her access to payment card processing immediately revoked?

YES ( ) NO ( ) If NO, please explain

25. Do you prohibit storage of cardholder data and other sensitive information electronically or otherwise?

YES ( ) NO ( ) If NO, please explain

26. Do you prohibit storage of the full contents of any track from the magnetic stripe (on the back of the card) in a database, log files, or point of sale products?

YES ( ) NO ( ) If NO, please explain

27. Do you prohibit storage of the card validation code (3 digit value printed on the signature panel of a card) in a database, log files, or point of sale products?

YES ( ) NO ( ) If NO, please explain

28. Do you update the “Privacy Policy” to reflect changes and keep it current?

YES ( ) NO ( ) If NO, please explain

29. Do you update the “Refund Policy” to reflect changes and keep it current?

YES ( ) NO ( ) If NO, please explain

22. Do you keep the Office of the Controller aware of any changes in your payment card program?

5. TECHNICAL INFORMATION:

1. Are employees who process payment cards aware of the "Emergency Contact Plan" in case the system has been breached or compromised?

YES ( ) NO ( ) If NO, please explain _____

2. Do you train employees and test the Emergency Contact Plan, at least annually? (same as #1)

YES ( ) NO ( ) If NO, please explain _____

3. Are default security settings, accounts, and passwords changed on production systems before taking the system into production?

YES ( ) NO ( ) If NO, please explain _____

4. Is transmission of cardholder data and other sensitive information across public networks encrypted using SSL or other industry acceptable methods?

YES ( ) NO ( ) If NO, please explain _____

5. Is there an anti-virus scanner installed on all servers and all workstations and is the virus scanner regularly updated?

YES ( ) NO ( ) If NO, please explain _____

---

6. THIRD PARTY PROCESSORS OR GATEWAYS INFORMATION:

If you are not using a 3rd Party Processor or Gateway, please go to PART 6.

1. Do you have a written agreement with an acknowledgment that indicates that the service provider (vendor) is responsible for the security of cardholder data?

YES ( ) NO ( ) If NO, please explain _____

2. Has the written agreement been reviewed and approved by our Legal Department?

YES ( ) NO ( ) If NO, please explain _____

3. Has the written agreement been reviewed and approved by Information Technology?

YES ( ) NO ( ) If NO, please explain _____

4. Has the service provider (vendor) supplied you with a certificate of Payment Card Industry Data Security Standards (PCI DSS) compliance?

YES ( ) NO ( ) If NO, please explain _____

5. Do you request a certificate of PCI DSS compliance annually from the service provider (vendor)?

YES ( ) NO ( ) If NO, please explain _____

6. Are development, testing, and production systems updated with the latest security-related patches released by the vendor?

YES ( ) NO ( ) If NO, please explain _____

7. Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?

YES ( ) NO ( ) If NO, please explain _____

8. Are unused services/applications on servers completely disabled/removed from all production environments, for security, increased system performance, and to improve system stability (for carrying out database, FTP, email, or web-hosting related task(s)?

YES ( ) NO ( ) If NO, please explain _____

Appendix 3

The University of Alabama in Huntsville PCI Compliance Payment Card Procedures

Any department accepting payment cards on behalf of The University of Alabama in Huntsville for goods or services should designate a full-time employee, known as the MDRP, within that department who will have primary authority and responsibility for payment card and/or e-commerce transaction processing within that department. This individual will be responsible for the department complying with the security measures established by the payment card industry and The University of Alabama in Huntsville procedures. In addition, they are responsible to ensure any employee who processes transactions takes the employee PCI training/acknowledgement and, if applicable, have the appropriate background check completed before any access is granted to the employee.

Departments may only use the services of vendors which have been approved by the UAH Bursar to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order or internet based.

Department Procedures

Each department that handles credit and debit card information must have written procedures tailored to its specific organization that are consistent with this policy and PCI-DSS. Departmental procedures should be reviewed, signed and dated by the MDRP on an annual basis. These procedures also must be submitted to and approved by their Department Head and The University of Alabama in Huntsville PCI Compliance Review Team.

Departmental procedures must thoroughly describe the entire transaction process and will include, but are not limited to, the following:

- Segregation of duties
- Deposits
- Reconciliation procedures
- Physical security
- Disposal
- Cash register procedures (if applicable)

Departmental procedures and controls are to be reviewed annually by The University of Alabama in Huntsville PCI Compliance Review Team.

General Payment Card Procedures

Do...

- Verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements.
- Verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS).
- Ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable.

Do not...

- Store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card, after authorization.
- Have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked.
- Store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smartphones.
- Permit any unauthorized people to access stored cardholder data.

Payment Card Procedures (In-Person/Mail Order/Telephone)

Receiving in-person payment from a customer:

- Only approved staff should be handling credit card transactions.
- Card Handling Guidelines:
    - Review Card Security
        - Is the Card valid? The card may not be used after the last day of the expiration month embossed on the card.
        - Only the actual card/account holder should be using the card.
        - Does the customer's signature on the charge form match the signature on the back of the card? Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.
        - Does the signature panel on the card look normal? Check to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.
        - Does the account number on the front of the card match the number on the back of the card and the terminal receipt display? If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.
        - Does the name on the customer receipt match the embossed name on the front of the card? If the name is different, this could indicate an altered card.
    - Risks of Keyed Transactions
        - Manually keying in the Card account information to get an authorization carries a higher risk of fraud since many of the built-in Card security features cannot be accessed. If the magnetic stripe on the back of the Card is unreadable, or if you choose to process transactions manually, follow these steps:
            - Key the transaction and expiration date into the terminal for Authorization approval.
            - Ask the cardholder to sign the paper receipt and compare the signature.
    - Report Suspected Card Fraud
        - If you suspect card fraud, report it to your bank using their established procedures.
- Receipt Guidelines:
    - Retain the signed merchant copy of the swipe machine generated receipt, the cardholder's copy should be returned to the cardholder.
    - Registration form with some verification of type of payment and date is forwarded to individual managing the event or class, etc. (use a reference point to locate the original merchant receipt if credit is later issued)
    - Place merchant copy of payment card receipt in envelope until the end of the day batch process has been run.

    - Reference the 06.04.02 policy for a basic guide on processing a cash transmittal.
- Oversight of the swipe machine during business hours:
    - Periodically check the machine (verify stickers have not been removed and re-affixed, same model, etc) to determine if it has been tampered with or exchanged. Report any tampering as a security breach, see below.
    - Keep the machine in a location not easily accessible to the public,
    - Keep the machine in a locked area when not in use or after hours,
    - Machines that are deemed NOT tamper-proof are disconnected and locked in a safe area when not in use or after hours.

Receiving payment information from a customer through the mail:

- Retrieve mail from a secure mailbox.
- Record pertinent information on Mail Log
- Form with payment card information handed over to individual responsible for key entering CC data (attach cover sheet with date, count and initials of mail clerk)
- Key enter card information as prompted through P2PE device.
- Obtain two copies of swipe machine generated receipt
- The payment card information is removed and cross-cut shredded or disposed in another approved method after the transaction has been processed
- The customer copy is faxed/mailed/emailed back to the customer.
- The form with some verification of type of payment and date is forwarded to individual managing the event or class, etc. (use a reference point to locate the original merchant receipt if credit is later issued)
- Place merchant copy of payment card receipt in secure location until the end of the day batch process has been run.

Receiving payment information from a customer through telephone orders:

- Answer calls and record customer's information.
- Form with payment card information handed over to individual responsible for key entering CC data (attach cover sheet with date, count and initials of mail clerk)
- Key enter card information as prompted through P2PE device.
- Obtain two copies of swipe machine generated receipt
- The payment card information is removed and cross-cut shredded or disposed in another approved method after the transaction has been processed
- The customer copy is faxed/mailed/emailed back to the customer.
- The form with some verification of type of payment and date is forwarded to individual managing the event or class, etc. (use a reference point to locate the original merchant receipt if credit is later issued)

- Place merchant copy of payment card receipt in secure location until the end of the day batch process has been run.

Batching out process at end of day:

- Follow the bank's procedure to settle transactions at the end of the work day.
- Staple the settlement sheet in front of the sales receipts and
  Store in a secure location (safe) until morning or
  Submit cash transmittal form along with receipts to Bursar's Office.