Rollins

FINANCE

PCI DSS Policy

Rollins
FINANCE

Contents

Rollins
FINANCE

Purpose

This policy document provides information to ensure Rollins College complies with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the PCI DSS is to protect cardholder data. This document and additional supporting documents represents Rollins College's procedures to prevent loss or disclosure of customer information including credit card numbers. Any failures to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of the college. The PCI Compliance Team's purpose is to educate all entities in the College's payment environment and to enforce the PCI DSS Policies contained herein. Questions regarding this policy should be directed to the Rollins College PCI Compliance Office.

Scope/Applicability

Rollins College Payment Card Procedures applies 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). Any business on behalf of the College, is subject to this policy as well as administrative and technical policies located in the College Handbook. Payment card data includes primary account numbers (PAN), cardholder name, expiration date, service code, and sensitive authentication data.

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. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)

In order to accept credit card payments, Rollins College must prove and maintain compliance with the **Payment Card Industry Data Security Standards**. The **Rollins College Payment Card Policy** and additional supporting documents provides the requirements for processing, transmitting, storage and disposal of cardholder data of payment card transactions, to reduce the institutional risk associated with the administration of credit card payments by college departments and to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI-DSS).

Rollins
FINANCE

Authority

Rollins College requires all departments that accept payment card payments to do so only in compliance with payment card industry standards and in accordance with the following procedures.

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 Center for Inclusion and Campus Involvement office. Agents of the College are prohibited from accepting funds via PayPal, Venmo, Square or other methods which requires funds to flow through personal bank accounts.

PCI 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.

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, termination and could limit a department’s payment card acceptance privileges which can be found in the “Sanctions” section of this policy.

Management

This policy was approved by the PCI Compliance Team, in January 2017. The PCI Compliance Team may modify this policy from time to time. This policy is distributed to Rollins College employees and students that accept payment card data.

This management includes completion of annual responsibilities in January of every year. These responsibilities are:

1. Test Incident Response Plan
2. Complete PCI and Security Training
3. Obtain Staff Acknowledgement of Policy and Procedures
4. Complete SAQ’s.

Rollins
FINANCE

Responsibility

Rollins College is committed to complying with the Payment Card Industry Data Security Standards.

Rollins College requires:

- Rollins College members must follow Rollins' College PCI DSS administrative and technical policies.
- Any department accepting payment card data, either at the College 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. Acceptance methods include e-commerce, MOTO, or in-person transactions.
- All Rollins College departments accepting payment cards and all agents of the College designated to accept payments cards will be trained upon hire and annually on this **Rollins College PCI Policy** and must electronically sign the **PCI Security Awareness Training & Confidentiality Agreement** prior to performing that work.
- Rollins College will perform a background check on potential personnel who will handle payment card data prior to hire to minimize the risk of attacks from internal sources. This check is completed by Rollins College Human Resources Department.
- Any Rollins College department accepting payment cards will utilize only dedicated, PCI Compliance Office approved equipment to process card payments.
- Any Rollins College department accepting payment cards will never store cardholder data. Departments that have recurring payments will need to use tokenization.
- Ensure that all credit card transactions are reviewed and reconciled to daily merchant reports. Turn these daily merchant reports into 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.
- Rollins College employs up to date security measures in firewall configuration, network administration, and other areas that could affect our PCI Compliance.

Rollins
FINANCE

PCI DSS Policy

Merchant Department Responsible Person (MDRP)

Any department accepting payment card and/or electronic payments on behalf of Rollins College for gifts, goods or services ("Merchant Department") must designate an individual (staff or faculty member) within that department 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 Rollins College. 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 the College, with access to or whom 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 agents of the College that will have access to more than one payment card at a time, 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 method which requires 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 the College 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.

● 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. The PCI Compliance Office has a cellular card swipe terminal for loan to agents of the College that have completed the PCI Security Awareness and Confidentiality Statement.

● Ensure Point of Sale devices/terminals (cash registers, stand-alone swipe terminals etc.) are physically secured.

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 to 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

● 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 Rollins College 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). Student Organizations and Clubs are prohibited from obtaining a merchant account, please contact the Center for Inclusion and Campus Involvement for available options.

● 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 the Rollins College PCI Policy.

-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 ability 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 the College 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

● Cardholder data must not be accepted or sent via end user messaging technologies; email, text message, SMS, chat etc. Rollins Email will not allow the transmittance of cardholder data. Advise any potential clients that attempting to transit 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.

● 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 Rollins College must have the return address of the department that will process the cardholder data on the return vehicle. 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 a secure online forms, by check, or phone.

● In the rare instance that an agent of the College 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 Rollins College. For compliancy and security Rollins College 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.

● 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.

Rollins
FINANCE

Storage

● Rollins College does not store authorized cardholder data (media), in hardcopy or electronic form.

● Rollins College 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

Rollins
FINANCE

Physical Security and Skimming Prevention of Payment Card Processing Devices

Rollins College will maintain an up-to-date inventory of all devices that capture payment card data. Rollins College will protect card present processing devices from tampering or substitution in adherence to the below requirements:

The PCI Compliance Team will conduct the following:

● Maintain a list of all devices that capture payment card data, for which the list is to include the following:

-Make, model, serial number (or other method of unique identification) and location of device

-Ensure that the list of devices is updated when devices are added, relocated, decommissioned

-Physically secure all devices that capture payment card data

-Portable payment card processing devices must be stored securely in a locked area when not in use.

-Cashiers must perform a daily visual inspection of devices that capture payment card data

-A monthly physical inspection must be performed, documented and retained.

Rollins
FINANCE

Security Awareness Program

In accordance with Rollins College PCI Training Plan:

All persons with physical and logical access to Rollins College's environment, whether employees, third-parties, service providers, contractors, temporary employees, and/or other staff members, must be trained on their role in protecting Rollins from threats to help safeguard Rollins College's finances, operations, and brand name.

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

● Read the Rollins College PCI Policy.

● Attendance logs for those who attend PCI training, must be kept by the PCI Compliance Team.

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 Incident Response Team at pcicompliance@rollins.edu, 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 Incident Response Team 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 Incident Response Team will alert the merchant bank, the payment card associations, Campus Safety, local authorities, Rollins College Chief Financial officer and the Chief Information Officer. A detailed incident response plan (**Appendix 1**) will be maintained by PCI Compliance Team.

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 Rollins College'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 Human Resources.

Note: 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 PCI Compliance Office must obtain the appropriate PCI Compliance documentation, from Service Providers, on an annual basis prior to 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 Service Provider is attesting to.

The PCI Compliance Team 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 PCI Compliance office for possible payment processes. The MDRP for all Student Organizations must be a full-time employee for the Center of Inclusion and Campus Involvement.

Third Party Processor Procedures

When deciding on a third party processor make sure to include the PCI office. New processors must be approved through the PCI office before they can be used on behalf of Rollins College. Ensure contracts include language that states that the service provider or third party vendor is PCI complaint and will protect all cardholder data. In addition, the contract must be approved through the Contract Approval Process by Human Resources. Third-party processors must have a completed and current Attestation of Compliance form on file with Rollins College. 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.

PCI Compliance Office Duties

The PCI Compliance Team is responsible for duties enforcing and maintaining PCI security at Rollins College. These responsibilities include but are not limited to the following:

- Perform Monthly Physical Inspections, on payment card processing devices, as noted in the section on Physical Security and Skimming Prevention. Systems not in use must be secured in a locked facility and regularly inventoried. Retain inspection log for a minimum of one year.

- 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 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 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 the College's bank which will be passed on to the College. A one-time penalty of up to $500,000 per branch per breach can be assessed as well as on-going monthly penalties.

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. Rollins College will carry out its responsibility to report such violations to the appropriate authorities.

FAQ's

1. How do I contact the PCI Office?

The PCI Office can be contacted by email through pcicompliance@rollins.edu. During working hours, the PCI Office can be contacted at 407-628-6300. In case of an emergency after normal working hours, contact Campus Safety and they will alert the PCI Administrator.

2. 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. Rollins email is secured against sending or receiving cardholder data.

3. 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.

Rollins
FINANCE

Appendix 1- Incident Response Plan

Purpose

The Payment Card Security Incident Response Plan supplements the Rollins College 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 Rollins College.

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

Rollins College Credit Card Security Incident Response Team

Communication for the Response Team can be sent to pcicompliance@rollins.edu

Name	Department/Title	Telephone	Email
Miller, Alexander	PCI Compliance and R-Card Coordinator	407-628-6300	amiller@rollins.edu
DiGorio, Jeremy	Director, Finance and Treasury	407-628-6321	jdigorio@rollins.edu
Short, Bill	Associate VP of Finance and Assistant Treasurer	407-646-2125	bshort@rollins.edu

Rollins
FINANCE

Name	Department/Title	Telephone	Email
Schoknecht, Pat	Associate CP of Business Systems and CIO	407-646-2700	pschoknecht@rollins.edu
Thomason, Troy	Director of Networks and Operations	407-628-6317	tthomason@rollins.edu
Sanchez, Katharine	Director of Admin. Computing	407-628-6382	ksanchez@rollins.edu
Martinez, Maria	Associate VP of Human Resources and Risk Management	407-646-2577	mmartinez@rollins.edu
Booker, Mandy	Bursar	407-646-2540	mbooker@rollins.edu

Rollins
FINANCE

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 Rollins College Incident Response Plan.

The Rollins College 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…

   pcicompliance@rollins.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 Rollins College 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 college 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 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 and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the PCI Committee, depending on the nature of the data compromise, must notify the appropriate organizations that may include the following:
    a. Rollins College Chief Financial Officer and the Chief Information Officer
    b. Rollins College Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with the card brands (VISA, MasterCard)
        i. see Bank Breach Response Plan
        ii. see Visa – Responding to a Breach
        iii. see MasterCard – Responding to a Breach
    c. If American Express payment cards are potentially included in the breach the College 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 College 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
6. Assist card industry security and law enforcement personnel in 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 Rollins College's responsibility to notify their own bank (the financial institution(s) that issues merchant accounts to Rollins College) and the Rollins College's bank will be responsible for notifying Visa and MasterCard, where applicable.

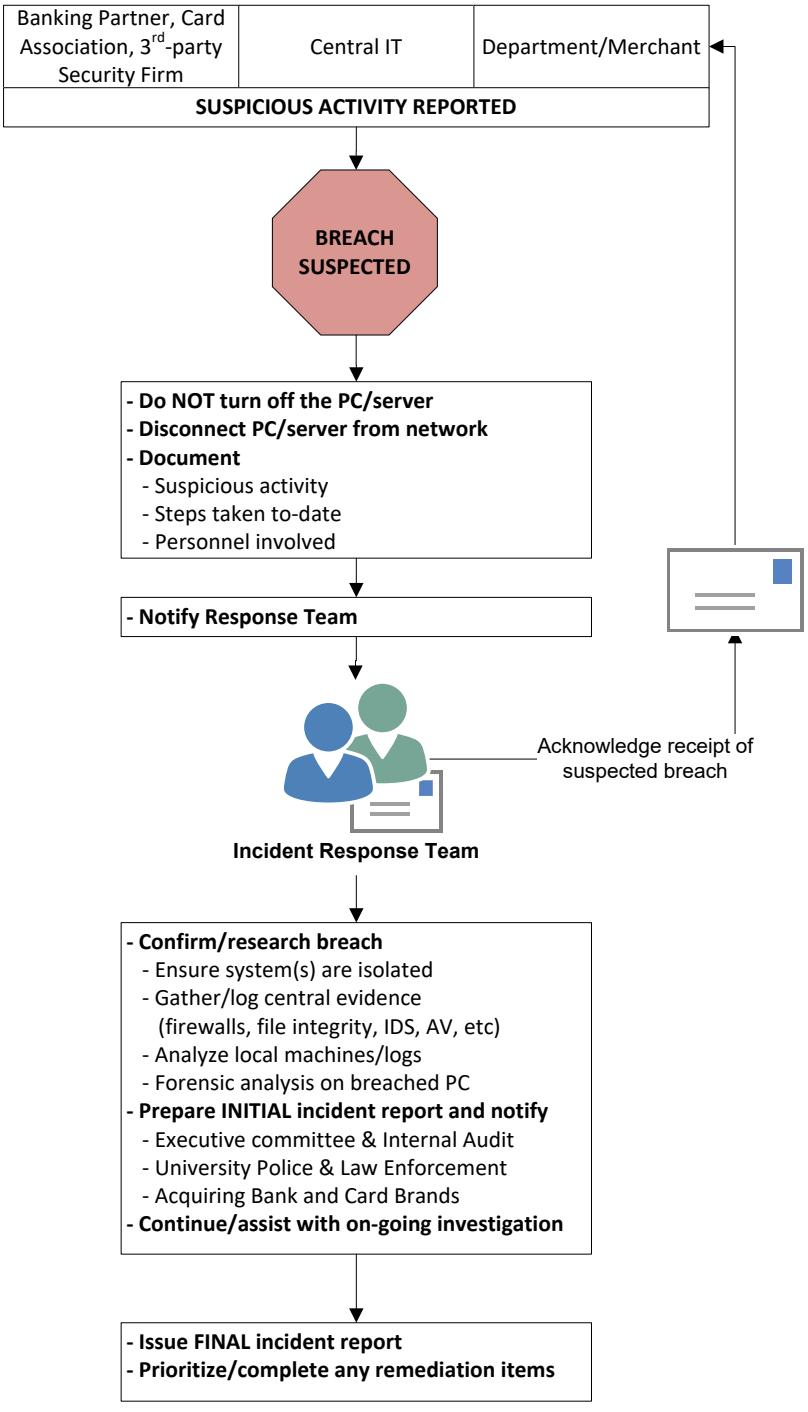
Rollins
FINANCE

Synovus Bank – Responding to a Breach

In issue of a card breach, Synovus Bank must be contacted by Rollins College. They are the primary bank for Rollins College and their Emergency Information Line is 1-888-796-6887.

Rollins
FINANCE

Flow Chart for Suspected Breach



Rollins
FINANCE

IRT Tool Kit

Preparing a tool kit for the IRT to use will enable them to respond promptly to any reported breaches. The kit should include:

- A voice recorder (can be a smart phone)
- External drive for backing up computer
- Boot media
- Small hub
- Laptop with security tools

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 logon 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

Rollins
FINANCE

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.

Rollins
FINANCE

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_Provider_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

Rollins
FINANCE

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

Rollins
FINANCE

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 Rollins College related products. We currently do not accept American Express.

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 Rollins College Policy.

Application must be submitted to PCI Compliance 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 bank, American Express and Discover Business Services to request merchant numbers. For assistance or questions regarding this form, please contact the PCI Compliance Office at pcicompliance@rollins.edu or call 407-628-6300.

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 Rollins College, 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 is stored or processed
    - This includes other Rollins College 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 insure 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.

Rollins
FINANCE

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: _____

Rollins
FINANCE

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 {ACCOUNTING OR CONTROLLER'S OFFICE CONTACT}.

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:

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

Rollins
FINANCE

DEPARTMENT ACCEPTS PAYMENT CARDS (Check all that apply):

( ) **IN PERSON**
( ) **BY PHONE**
( ) **BY MAIL**
( ) **BY FAX**
( ) **ON LINE PAYMENT VIA UNIVERISTY'S APPORVED INTERNET PROCESSOR** **(name of provider)** _____
( ) **ON LINE 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 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 not 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 Rollins College *"Payment Card Processing Procedures"* being followed by employees involved in payment card handling?
   YES ( ) NO ( ) If NO, please explain _____

Rollins
FINANCE

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 Rollins College 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 _____

Rollins
FINANCE

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 _____

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 _____

Rollins
FINANCE

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 _____

Rollins
FINANCE

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

Rollins
FINANCE

Appendix 3

Rollins College PCI Compliance Payment Card Procedures

Any department accepting payment cards on behalf of Rollins College 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 Rollins College policies. 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 PCI Compliance Office 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 Rollins College PCI Compliance Office.

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 Rollins College PCI Compliance Office.

Rollins
FINANCE

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 smart phones.
- Permit any unauthorized people to access stored cardholder data.

Rollins
FINANCE

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 cardholders 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 **Finance Department's Cash Receipting Policy Statement** 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 lock in a safe area when not in use or after hours.

Receiving payment information from a customer through the mail:

- Retrieve mail from secure mailbox.
- 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 call 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.

Finance Department Cash Receipting Policy Statement

All receipts must be deposited into the College bank account and recorded with the appropriate General ledger account(s). All incoming funds over $500 should be deposited within one day of receipt. Regardless of the amount (even less than $500) should be deposited weekly. A cash transmittal must be prepared to record the income at the time of deposit. Funds awaiting deposit must be kept in a secure, locked device until deposited. The method used to secure the funds should be appropriate for the amount. For example, a locked desk drawer would be adequate for $50; however a safe would be required for $1,000.

Reason for Policy

The purpose of this policy is to implement best-in-class revenue processing procedures that standardize revenue processing across the campus. This policy ensures efficient solutions characterized by strong controls to reduce the risk of fraud and/or loss while increasing the efficiency of its cash.

- Treasury has operational authority over the acceptance and deposit of all payments received by Rollins including those received at the individual department level.
- All units will employ consistent payment types across similar revenue generating activities.
- Revenue processing procedures should enable operational efficiency with an optimal cost structure.
- All revenue processing procedures must maintain the highest level of available operational controls to reduce the possibility of fraud, loss of assets and/or loss of sensitive college data.
- The fiscal officer or supervisor of the account receiving revenue will be responsible for implementing proper revenue processing procedures, payment methods, and assume responsibility for payment risks and compliance.
- Treasury possesses core competency relative to banking services, working capital management, credit card processing, electronic payment options and developing trends in payment technology.

- Treasury will provide ongoing education regarding accepting payments in compliance with Rollins' data security policies and the Payment Card Industry Data Security Standards (PCI DSS) requirements.

Appendix 4

PCI Project Team Charter

Background

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that store, process, or transmit cardholder data (CHD) in any format (e.g. electronic, paper-based, etc). This standard was created to better assist entities to increase overall security of CHD and reduce credit card fraud via its exposure.

The PCI DSS is comprised of 12 requirements that specify the framework for secure payment environments.

Rollins College will undertake steps to ensure the college is compliant with the PCI DSS by developing and implementing a service offering that includes the technology, training, policies, procedures, processes, and support to achieve compliance and mitigate risks, as outlined in the PCI DSS Compliance Roadmap Report.

The PCI Project Team is a cross-organizational working group of representatives from Rollins College that have interaction with the handling of CHD. This team will discuss findings and develop strategies that will ensure PCI DSS requirements are met.

Purpose

The PCI Project Team will assist Rollins College in getting compliant with the PCI DSS and reduce the scope of items that will need to be compliant with the PCI DSS by implementing the changes set by the strategic direction of the college.

Functions

- Meet monthly to address issues and findings.
- Develop strategies for remediation of non-compliant items.
- Monitor, support, and follow-up with merchant areas to ensure any and all corrective actions are applied.
- Report any feedback, concerns, and proposals from the merchant areas to the project team.
- Champion PCI DSS compliance across Rollins College.

Rollins
FINANCE

Structure

Name	Department/Title	Telephone	Email
Miller, Alexander	PCI Compliance and R-Card Coordinator	(407) 628- 6300	amiller@rollins.edu
DiGorio, Jeremy	Director, Finance and Treasury	(407) 628-6321	jdigorio@rollins.edu
Short, Bill	Associate VP of Finance and Assistant Treasurer	(407) 646-2125	bshort@rollins.edu

Operation

The PCI Project Team will conduct monthly meetings to discuss and act upon areas of non-compliance at the college. The direction will be based on a consensus, incorporating the requirement to be compliant with the PCI DSS. If consensus cannot be reached, the Chair will seek resolution with the PCI DSS Compliance Project Sponsor.

The PCI Project Team will be in-place for the duration of the PCI DSS Compliant Project.

Rollins
FINANCE

Client Process—Ecommerce MOTO Setup

When a department or student group would like to receive credit card payment in-person or over the phone from a customer and wants to use a website to enter information, in lieu of using a register. The group must contact the PCI Compliance Office four weeks prior to the event.

Planning:

1. Determine who will be taking payments and how many stations will be needed.
2. Review available Point to Point Encryption (P2PE) technology by contacting pcicompliance@rollins.edu.
3. Determine budget to account for payment gateway services, physical devices, and associated credit card processing fees.
4. Consider if payments are considered gift or non-gift related.
5. Consider timeline needed to setup e-commerce website, including hardware purchases.
6. Consider what documentation is needed for PCI Compliance. Reference can be found in the Rollins College PCI Policy.
7. Prepare the information for PCI Compliance office will need, which is:
    a. List of representatives participating.
    b. If payments are gift or non-gift related.
    c. Amount of P2PE devices that will need to be ordered.

Steps to take:

1. Create and maintain list of representatives participating in e-commerce.
2. Create and maintain documentation for credit card handling from “cradle to grave”.
3. Contact PCI Compliance office with necessary information.
4. PCI Office will contact you with receipt of request and inform you of the next steps.
5. To ensure your request is handled in a timely manner, please make sure to respond to the PCI office as information is needed.
6. Confirm it is okay to move forward with purchase and setup of P2PE hardware/software.
7. Once necessary payment gateway and hardware has been delivered, PCI Office will schedule training.
8. Contact PCI Office if any questions remain after training.
9. Review documentation and update as new policies and procedures come into play.

PCI Process

1. Upon receipt of request, review information and determine feasibility and if additional information is needed.
2. Send confirmation receipt to user, identifying polices and associated fees.
3. Await confirmation that is okay to move forward.
4. Order necessary hardware and perform initial setup of payment gateway for P2PE
5. Contact user for training
6. Follow-up on a scheduled basis to determine if any documentation needs to be updated.

Rollins
FINANCE

Client Process—Longer Term Ecommerce Solution

When a department or student group would like to accept credit card payments through a Rollins website for a recurring activity or event. The group must contact the PCI Compliance Office four weeks prior to the event.

Planning:

1. Determine registration page that will connect to payment piece with event information.
2. Decide on the fields and type of data you will be charging (Ex: Credit, Debit, E-Check, etc.) Rollins College does not directly accept American Express.
3. Allow for 4 weeks after submitting your request to the PCI Compliance office.
4. Prepare the information the PCI Compliance office will need, which is:
    a. Budget Codes for Deposits to be made
    b. The amount the customers will be charged
    c. The fields of data to be collected (Ex: Name, Address, Grade Level, etc.)
    d. The email address of the person to be notified when a charge is complete

Steps to take:

1. Contact the PCI Compliance office 4 weeks in advance for setup of this site
2. The PCI Compliance office will send you a confirmation of receipt and will inform you of the next steps.
3. To ensure your request is handled in a timely manner, please make sure to respond to the PCI office as information is needed.
4. Once you are satisfied with the commerce page and it is tested you will need to link it to the page you want to process from.

PCI Compliance Office Process

1. Upon receipt of request, review request information and determine feasibility and if additional information is needed.
    a. Thierry Lechler (pcicompliance@rollins.edu) will review information for completeness.
2. Send a confirmation receipt to user, identifying policies and associated processing fee.
3. Once IT has a test created, send information to user and follow up.
4. Once site is approved by user, ensure PCI policies and procedures are reviewed by merchant.

Rollins
FINANCE

Client Process—Mobile POS Setup

When a department or student group would like to accept credit card payments for events on the go or in a location where wired devices aren't feasible. The group must contact the PCI Compliance Office two to four weeks prior to the event.

Planning:

1. Determine the specifics of your event and how you want to take payments.
2. Review Point to Point Encryption hardware/software listed at: Bluefin and their partners.
3. Plan ahead to make sure there is available equipment for check-out.
4. Prepare the information that the PCI Compliance office will need, which is:
    a. Location of event
    b. Time of event
    c. Name of Rollins sponsoring group
    d. Whether they will need the full kit or just the adapter (listed on website)
    e. People that will be using the device
    f. Budget Code

Steps to take:

1. Reserve Event Space:
    a. Select you'd like to accept credit card payments on a mobile device.
2. PCI Office will send confirmation of request and will inform you of the next steps.
3. Please respond to the PCI office as information is needed.
4. Once approved, the PCI Compliance office will send an approval notification and instructions for any additional steps needed. Steps will include picking up equipment and training.
5. Proceed with event.
6. Return equipment.
7. After event, complete a cash transmittal form online to deposit funds into the specified budget code. Specific payment receipting policies for Rollins College can be found in the Cash Receipting Policy Statement (Appendix).
    a. Student Organizations will turn in receipts to the PCI Compliance Office.
    b. Departments will turn in form directly to the Bursar's Office.

PCI Process

1. Upon receipt of request, review request information and determine availability of equipment and if additional information may be needed.
2. Send confirmation receipt to user, identifying policies, associated processing fees, and agreement form for using mobile device for credit card payments.
3. Once agreement form is returned, gather necessary equipment and test to make sure devices are working.
4. Send approval notification along with training documentation and time for equipment pick-up.
5. Train end user on device features and usage when they arrive for pick-up. Also cover PCI responsibilities.
6. Review equipment after it has been returned for evidence of tampering.

Rollins
FINANCE

Client Process—Physical Register

When a department or student group uses an area that needs a physical register to handle multiple types of tenders. The group must contact the PCI Compliance Office four weeks prior to the event.

Planning:

1. Determine what is going to be sold
2. Determine what kind of payments are to be accepted (Ex: Credit Cards, Cash, etc.)
3. Determine location.
4. Determine any peripherals, such as a barcode scanner or a cash box, that may be needed
5. Determine when device will be needed including the time and date.
6. Determine budget
7. Review POS options listed on: http://www.rollins.edu/finance/pci-compliance/index.html

Steps to take:

1. Submit request for POS to PCI Compliance office. Include budget and POS information from planning.
2. PCI Compliance office will send confirmation of request and inform area of next steps.
3. To ensure the request is handled in a timely manner, please make sure to respond to the PCI office as information is needed.
4. Once approved, PCI office will send notification and a timeline on any additional steps.

PCI Process

1. Upon receipt of request, review request information, determine feasibility and if ask for additional information if needed.
2. Determine POS device that meets needs of the area.
3. Purchase POS device and peripherals.
4. Determine upgrade cycle for POS device (every five years).
5. Determine possible security risks.
6. Get budget code and perform fund transfer for device, including funds for the upgrade cycle.
7. Inventory equipment.
8. Setup training for users.
9. Deliver and setup device.

Rollins
FINANCE

Client Process—Secure Third Party Website

When a department or student group would like to accept credit card payments through a non-Rollins website for a special event or other activity. The group must contact the PCI Compliance Office four weeks prior to the event.

Planning:

5. Determine the specifics of your event and how you want to take payments
6. Review the list of preapproved PCI compliant vendors, by contacting the PCI Compliance Office, to determine if one of these vendors will meet your needs. **NOTE:** Using a preapproved vendor will allow you to have the quickest turnaround time for setup.
7. Plan ahead to make sure the setup of your event will be successful, this may take anywhere from 1 week to 4 weeks after submitting your request to the PCI Compliance office.
8. Prepare the information the PCI Compliance office will need, which is:
    a. Location of event
    b. Time of the event
    c. Name of the Rollins sponsoring group
    d. Type of credit card processing that will happen (only online, or online and in person)
    e. Amount of assistance needed (the group will do all of the event website setup or you need assistance in the setup of the event website)

Steps to take:

5. Decide on a vendor and contact the PCI Compliance office: 1 week in advance for a preapproved vendor or 4 weeks in advance for a new vendor
6. The PCI Compliance office will send you a confirmation of receipt and will inform you of the next steps.
7. To ensure your request is handled in a timely manner, please make sure to respond to the PCI office as information is needed.
8. Once the event is approved by the PCI Compliance office, you will receive an approval notification and instructions for any additional steps needed.
9. Proceed with setting up your event online.
10. After the event, complete a reconciliation of the event income and submit this to the PCI Compliance office

PCI Process

5. Upon receipt of request, review request information and determine feasibility and if additional information is needed.
6. Send a confirmation receipt to user, identifying policies and associated processing fees

    IF Approved Vendor:

    1. Setup user in system with proper information
    2. Send the user there information, to login and customize event.

IF New Vendor:

1. Contact the Vendor for AOC form
2. Review vendor fees and contracts with the requesting user and Risk Management Office
3. If it is decided to move forward, setup an account with the vendor
4. Send the user their information, to login and customize event

7. After the event, review the reconciliation and submit a Cash Transmittal Form to move the money from the Bursar's Office to the specified budget code.

Client Process—Tarbuc$ Reader

When a department or student group would like to sell a product on a mobile device and accept TarBu$s tender. The group must contact the PCI Compliance Office two weeks prior to the event.

Planning

1. Determine what is being sold and if sales tax has to be applied. Contact Teresa Williams at (twilliams@rollins.edu) for questions.
2. If student event, determine information Student Involvement will need for Get Involved.
3. Determine what information the PCI/R-Card office will need, which is:
    a. Location of event
    b. Time of event
    c. Items being sold
    d. Pre-tax amount and sales tax
    e. Budget code
    f. People that will be using the reader

Steps to take:

1. Reserve event space through the EMS system two weeks prior to the event and select to handle Tarbucs$ as a form of payment during the event.
2. The PCI Compliance/R-Card office will send confirmation of receipt and will inform you of the next steps.
3. To ensure your request is handled in a timely manner, please make sure to respond to the PCI/R-Card office as information is needed.
4. Once approved, you'll receive an approval notification with instructions on any additional steps needed.
5. Keep track of all sales during your event for reconciliation purposes.
6. Tarbuc$ reconciliation reports occur at the beginning of each month and will be handled by the PCI Compliance Office and sent to the specific budget code.

PCI Process

1. Upon receipt of request, review information and send confirmation.
2. If additional information is needed, contact requester.
3. Configure Tarbuc$ device to handle products with pricing.
4. Schedule training and delivery time for device.
5. Recover devices after event.
6. Include events in Tarbuc$ reconciliation for the correct month.

Rollins
FINANCE

Client Process—Stationary Credit Card Terminals

When a department or student group would like to accept credit card payments through a stand-alone/stationary credit card processing terminal, and needs it to be installed in an area. The group must contact the PCI Compliance Office four weeks prior to the event.

Planning:

1. Determine if P2PE, Point to Point Encryption, solution would work in lieu of a stand-alone terminal
    a. If yes, refer to MOTO, Mail Order Telephone Order, setup.
    b. If no, continue onto next steps.
2. Scout location where terminal will be located and determine the following:
    a. Determine necessary wiring needs and whether power and/or Ethernet outlets will be need to be added.
    b. Check cellular signal strength to see if it's an option for chosen location
3. Determine budget for hardware, software, and security needs for setup.
4. Prepare the information that the PCI Compliance office will need, which is:
    a. Location of terminal
    b. Who will access the terminal
    c. When terminal will be needed
    d. Security requirements for area

Steps to take:

1. Review PCI Compliance requirements in the PCI DSS Policy located at: http://www.rollins.edu/finance/pci-compliance/index.html
2. Create and maintain list of who has access to area
3. Read documentation for policies and procedures for credit card handling from "cradle to grave".
4. Request PCI Compliance training.
5. PCI Compliance office will send confirmation receipt and will inform you of the next steps.
    a. Please respond in a timely manner to the PCI Compliance office as information is needed.
6. Once terminal is approved, the PCI Compliance office will send out an approval notification and instructions for any additional steps needed.
7. Annually review PCI policies.

PCI Process

1. Review request information and determine feasibility and if additional information is needed.
2. Determine if P2PE solution would not be more suitable.
3. Send confirmation receipt to user, identifying polices and associated fees.
    a. If P2PE solution is suitable, follow MOTO setup
    b. If stand-alone terminal is needed, perform the following steps
4. Determine MID user will be using and physical security of the location.
5. Purchase, inventory, and setup device
6. Train Users
7. Collect documentation from area on card handling policies and procedures.