CAPRI COLLEGE

Policy on Safeguarding Student Personally Identifiable Information (PII)

What is personally identifiable information?

Personally identifiable information (PII) is any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person. Such information can include educational, financial, legal and employment records.

Examples of personally identifiable information

Personally identifiable information can be anything that identifies an individual, such as a full name, an address, a home, office or mobile telephone numbers, an email address, a Social Security number or other form of national ID number, Internet Protocol address, a fingerprint or other biometric data, birthday, or age.

Protecting personally identifiable information

Capri College employs numerous security protocols to ensure that personally identifiable information is safe and secure at all times.

Capri College's security policy involves a combination of encryption, threat protection (Sophos firewall, segregated wireless permissions, managed GFI antivirus, and regular security updates), data-loss prevention (automatic secure backups stored on and off-site), and policy compliance. Employees must follow rules and common sense procedures regarding access to personal data.

Only collect and use information that is absolutely necessary. Never use, print, view or send Student SSNs, birthdates, or other PII unless necessary. If necessary, ensure information is secure or shredded after use.

Never send PII by email.

PII to be shredded must be in locked container until shredded.

Student data is stored in Fame program only, and is not allowed to be passed to third parties. Any printed personal info must be destroyed (shredded) after use and all print files are locked in secure area and never left out in unsecured area. All terminals with access to data are password protected (at least 9 characters, employing caps, numbers and symbols) not allowed to be used to visit social sites, and logged out when employee leaves station. Employees trusted to view sensitive data are required to sign that they follow and understand this policy and repercussions for non-compliance. If it is determined that an employee did not follow this policy, it is grounds for termination or criminal prosecution, depending on the specific actions and intent. If privacy breach occurs or is suspected, employee must inform management immediately.

Credit Card Policy

- It is against Capri Policy to store credit card numbers on any document, computer, server, or database. This includes Excel spreadsheets.
- Valid ID must be presented for use of credit card.
- Email is not an approved way to transmit credit card numbers.
- Fax transmittal of cardholder data is permissible only if the receiving fax is located in a secure environment and is credit card # is not visible.
- Paper receipts including PII or credit card # must be destroyed so that account information is unreadable and cannot be reconstructed.
- Regularly update anti-virus software, Java and Adobe.
- Do not use vendor-supplied defaults for systems passwords and other security parameters.
- Each computer with any sensitive information or access to Administrative network must be password protected (9 characters, employing caps, numbers and symbols).

All CAPRI COLLEGE employees that have access to PII must sign here

I have read and clearly understand these policies.

_____ _____

Name ***Date***

PII - Introduction and Scope

Introduction

This document covers our credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Our management is committed to these security policies to protect information utilized by us in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, our cardholder environment consists only of imprint machines or standalone dial-out terminals. The environment does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) B, ver. 3.0, released February, 2014. Should we implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ B, it will be our responsibility to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Commented [A1]: Add reference to definition of sensitive authentication data?

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

We will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show no more than the first six and the last four digits of the PAN. (PCI requirement 3.3)

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)

Privileges must be assigned to individuals based on job classification and function (also called “role-based access control). (PCI Requirement 7.1.3)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI requirement 9.9)

ABC Corporation must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI requirement 9.9.1)

- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI requirement 9.9.2)

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI requirement 9.9.3)

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

Our security policy addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1)

Critical Technologies

We shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)

Security Responsibilities

Our policies and procedures clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

Any who receive credit card payments hall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

Reporting an Incident

Matt Fiegen or Sara Fiegen should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or owners about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the owners

Document any information you know while waiting for owners respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response Policy (PCI requirement 12.10.1)

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

   Visa

   Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

   MasterCard

   Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

   Discover Card

   Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm
4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the owner will work with legal and management to identify appropriate forensic specialists.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

Our security policy is to establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Capri College

Credit Card Security Policies

PCI DSS 3.0

Revision History

Changes	Approving Manager	Date
Initial Publication	Matt Fiegen	12/31/14
Signatures by staff	Matt Fiegen	On-going
Updated Forms for PII	Matt Fiegen / Lois Leytem	8/31/16
Updated Forms for PII	Matt Fiegen / Lois Leytem	12/29/16