COLORADO STATE UNIVERSITY
Financial Procedure Instructions
FPI 6-6

1. **Procedure Title:** PCI Compliance Program

2. **Procedure Purpose and Effect:** All Colorado State University departments that accept credit/debit card payments must process those payments in a manner compliant with the Payment Card Industry Data Security Standards (PCI DSS). This procedure is to provide guidance to departments on how to achieve and maintain PCI compliance.

3. **Application of Procedure:** This procedure applies to all departments that accept credit card payments.

4. **Exemptions:** None.

5. **Definitions:**

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. A key objective of PCI DSS is to help organizations ensure the safe handling of cardholder information at every step in the transaction process. Banking Services reserves the right to suspend merchant accounts if guidelines are not followed.

The requirements:

- **Build and Maintain a Secure Network**
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program**
  - Requirement 5: Use and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access

- Requirement 9: Restrict physical access to cardholder data

- **Regularly Monitor and Test Networks**
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes

- **Maintain an Information Security Policy**
  - Requirement 12: Maintain a policy that addresses information security for all personnel

A. Anti-Virus: Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.

B. Application: Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.

C. Cardholder: Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

D. Cardholder Data: At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See *Sensitive Authentication Data* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

E. Default Password: Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.

F. Encryption: Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

G. Firewall: Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.

H. Merchant: For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

I. **Payment Cards**: For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.

J. **PCI**: Acronym for "Payment Card Industry."

6. **Procedure Statement:** Depending on how your department accepts and processes credit/debit card payments, there are four main components to the CSU compliance program:

A. **Annual Self-Assessment Questionnaire (SAQ D)** for those merchants processing payments hosted on a University server or that touches the network. All merchants who have been deemed to complete this SAQ by Banking Services and ACNS must have a completed SAQ D on file. A new SAQ must be completed when the Payment Card Industry Security Standards Council (PCI SSC) releases a new version of the SAQ.

B. **PCI Attestation and Date Security Do's and Don'ts forms** for those merchants processing credit/debit card payments via standalone, dial-out analog terminals. These forms are for merchants that process credit cards with terminals connected via an analog phone line. The Attestation Form outlines best practices and PCI requirements for these types of merchants. The Data Security Do's and Don'ts summarizes what type of sensitive cardholder data can be stored and what cannot be stored. These forms are distributed on a yearly basis and are required for all merchants with terminals and who accept retail card present payments and payments accepted through the mail and or phone. Please see attachment 1 for the Policy Attestation Form and attachment 2 for the Data Security Do's and Don'ts.

C. **Annual review of credit card environment**. This requirement also includes the creation and maintenance of a departmental PCI Notebook. A representative from Banking Services and ACNS will meet with all e-commerce merchants on a yearly basis to review each credit card processing environment. This meeting includes the following activities; review and completion of any required PCI forms (SAQ D, etc.), changes in the way credit cards are accepted, and the creation and maintenance of a PCI Notebook. This notebook must contain the following items:

1. ACNS IT Security Policy.
2. PCI Forms – Policy Attestation Form and Data Security Do's and Don'ts. These forms are the used as reference only, unless instructed otherwise.
3. Network and payment application diagram.
4. Departmental policy and procedures for handling sensitive cardholder data.
5. Business Continuity/Disaster Recovery/Incident Response Plan. This requirement also includes an annual test (desktop exercise) of a "what if" scenario. Please record who participated in the activity, document any findings of the event and any changes and updates needed for this plan.
6. Certificates of Compliance from any vendors associated with the payment process.
7. Copies of any contracts with such parties (if requested).
   Once the PCI Notebook has been created, merchants are required to bring this information to the annual PCI meeting that is scheduled with Treasury Services and ACNS.

D. **Quarterly scans of all outward facing IP addresses** that fall within the scope of PCI. ACNS and the department will determine what IP addresses need to be part of this process.

7. Reference and Cross-References:

To obtain additional information on PCI DSS and the requirements please select the link below:
https://www.pcisecuritystandards.org/

8. Forms and Tools:

Attachment #1

Payment Card Industry Data Security Standards (PCI DSS)

CSU Campus Policy Attestation

Colorado State University

Treasury Services

6003 Campus Delivery

Please make sure the following practices are in place:

- Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of credit card).
- Do not send/receive sensitive cardholder data via unencrypted e-mail, instant messaging, chat, etc. This includes strict control over internal and external distribution of any kind of media that contains cardholder data.
- Limit access to cardholder data to only those individuals whose jobs require such access.
- Restrict physical access to cardholder data – strict control over the storage and accessibility of data.
- Media (terminal reports, registration forms, payment forms, etc.) containing cardholder data is destroyed when it is no longer needed for business or legal reasons.
- A formal security awareness program is in place to make all employees aware of the importance of cardholder data security.

I have read and understand the PCI Data Storage Do's and Don'ts and agree to abide by CSU's credit card acceptance policies.

Department: _____ Merchant Name: _____

Merchant ID: _____

Merchant Contact: _____ Merchant Contact Signature/Date: _____

Department Head: _____ Department Head Signature/Date: _____

Contact Zach Campain (1-7132) with questions. Please return completed form to Treasury Services – 6003 Campus Delivery

Attachment #2

PCI Security Standards Council

AT A GLANCE
PCI DSS DATA STORAGE

PCI DSS Data Storage Do's and Don'ts

Requirement 3 of the Payment Card Industry Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public expects that merchants and financial institutions will protect payment card data to thwart data theft and prevent unauthorized use. Requirement 3 addresses protection of stored cardholder data. Merchants who do not store any cardholder data *automatically* provide stronger protection by having eliminated a key target for data thieves. Remember if you don't need it, don't store it!

For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. In addition to PCI DSS requirements, PA-DSS and PTS require protection of stored cardholder data for payment applications and payment terminals. To prevent unauthorized storage, only PTS approved PIN entry devices and PA-DSS validated payment applications should be used. PCI DSS, PA-DSS and PTS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors

Basic Payment Card Data Storage Guidelines for Merchants

Cardholder data refers to any information contained on a customer's payment card. The data is printed on either side of the card and is contained in digital format on the magnetic stripe embedded in the backside of the card. Some payment cards store data in chips embedded on the front side. The front side usually has the primary account number (PAN), cardholder name and expiration date. The magnetic stripe or chip holds these plus other sensitive data for authentication and authorization.

In general, no payment card data should ever be stored by a merchant unless it's necessary to meet the needs of the business. Sensitive authentication data on the magnetic stripe or chip must never be stored. Only the PAN, expiration date, service code, or cardholder name may be stored, and merchants must use technical precautions for safe storage (see back of this fact sheet for a summary). The matrix below shows basic "do's" and "don'ts" for data storage security.

Data Do's	Data Don'ts
Do understand where payment card data flows for the entire transaction process	Do not store cardholder data unless it's absolutely necessary
Do verify that your payment card terminals comply with the PCI Personal Identification Number (PIN) Transaction Security (PTS) requirements	Do not store sensitive authentication data contained in a payment card's chip or magnetic stripe, including the 3-4 digit card verification code or value printed on the front or back of the payment card, after authorization.
Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS)	Do not have payment terminals print out personally identifiable payment card data; printouts should be truncated or masked
Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it's protected	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals	Do not locate servers or other payment card system storage devices outside of a locked, fully-secured and access-controlled room
Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PTS and/or PA-DSS as applicable. Have clear access and password protection policies	Do not permit any unauthorized people to access stored cardholder data

PROTECT STORED CARDHOLDER DATA

Use Encryption

Encrypted data is unreadable and unusable to a system intruder without the proper cryptographic keys. See the PCI DSS Glossary for more information: www.pcisecuritystandards.org/security_standards/glossary.php

Use Other Measures

Do not store cardholder data unless there is a legitimate business need; truncate or mask cardholder data if full PAN is not needed and do not send PAN in unencrypted emails, instant messages, chats, etc..

Use Compensating Controls as Alternatives

If stored cardholder data cannot be encrypted or otherwise rendered unreadable, consult PCI DSS Appendix B: Compensating Controls and Appendix C: Compensating Controls Worksheet.

Verify 3rd Party Compliance

Approved PTS Devices www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Validated Payment Applications www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Technical Guidelines for Stored Payment Card Data

PCI DSS Requirement 3 details technical and operational requirements for protecting stored cardholder data. Merchants should develop a data retention and storage policy that strictly limits storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.

Sensitive authentication data must never be stored after authorization – even if this data is encrypted.

- Never store full contents of any track from the card's magnetic stripe or chip (referred to as full track, track, track 1, track 2, or magnetic stripe data). If required for business purposes, the cardholder's name, PAN, expiration date, and service code may be stored as long as they are protected in accordance with PCI DSS requirements.
- Never store the card-validation code or value (three- or four-digit number printed on the front or back of a payment card used to validate card-not-present transactions).
- Never store the personal identification number (PIN) or PIN Block.
- Be sure to mask PAN whenever it is displayed. The first six and last four digits are the maximum number of digits that may be displayed. This requirement does not apply to those authorized with a specific need to see the full PAN, nor does it supersede stricter requirements in place for displays of cardholder data such as on a point-of-sale receipt.

Technical Guidelines for Payment Card Data Storage

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorization (even if encrypted)

[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Technical Guidelines for Protecting Stored Payment Card Data

PCI DSS requires PAN to be rendered unreadable anywhere it is stored – including portable digital media, backup media, and in logs. Solutions for this requirement may include one of the following:

- **One-way hash functions based on strong cryptography** – converts the entire PAN into a unique, fixed-length cryptographic value.
- **Truncation** – permanently removes a segment of the data (for example, retaining only the last four digits).
- **Index tokens and securely stored pads** – encryption algorithm that combines sensitive plain text data with a random key or "pad" that works only once.
- **Strong cryptography** – with associated key management processes and procedures. Refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms for the definition of "strong cryptography."

Some cryptography solutions encrypt specific fields of information stored in a database; others encrypt a singular file or even the entire disk where data is stored. If full-disk encryption is used, logical access must be managed independently of native operating system access control mechanisms, and decryption keys must not be tied to user accounts.

Encryption keys used for encryption of cardholder data must be protected against both disclosure and misuse. All key management processes and procedures for keys used for encryption of cardholder data must be fully documented and implemented. For more details, see PCI DSS Requirement 3.

October 2010