

COLORADO STATE UNIVERSITY-PUEBLO
Financial Procedure Statements
FPI 6-6

1. **Procedure Title:** PCI Compliance Program
2. **Procedure Purpose and Effect:** All Colorado State University-Pueblo 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-Pueblo 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 Office of Financial Management and DoIT 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 Data 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 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 CSU-Pueblo IT Security 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. CSU-Pueblo IT Security Policy.
2. PCI Forms – Policy Attestation Form and Data Security Do's and Don'ts. These forms are used as references 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 CSU-Pueblo IT Security.

D. Quarterly Scans of All Outward Facing IP Addresses that fall within the scope of PCI. CSU-Pueblo IT Security 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

The Prioritized Approach to Pursue PCI DSS Compliance

Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The following table summarizes the high-level goals of each milestone.

Milestone	Goals
1	Do not store sensitive authentication data and limit cardholder data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other account data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	Protect systems and networks and be prepared to respond to a system breach. This milestone targets controls for points of access to most compromises and the response processes.
3	Secure payment applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas are easy prey for compromising systems and obtaining access to cardholder data.
4	Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning access to your network and cardholder data environment.
5	Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, this milestone targets key protection mechanisms for the stored data.
6	Complete remaining compliance efforts, and ensure all controls are in place. This milestone completes PCI DSS requirements and finishes all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS

PARTICIPATING ORGANIZATIONS

Merchants, service providers, banks, processors, developers, and point of sale vendors.

Protect Account Data

Payment account data refers to any information printed, processed, transmitted, or stored in any form on a payment card. Account data refers to both cardholder data and sensitive authentication data, and protection of the account data is required where account data is stored, processed, or transmitted. Entities accepting payment cards are expected to protect account data and to prevent its unauthorized use - whether the data is printed or stored locally, or transmitted over an internal or public network to a remote server or service provider.

Requirement 3: Protect stored account data

Payment account data should not be stored unless it is necessary to meet the needs of the business. Sensitive authentication data must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable. If your company stores sensitive authentication data prior to completion of authorization, that data must also be protected¹.

- 3.1 Processes and mechanisms for protecting stored account data are defined and understood.
- 3.2 Storage of account data is kept to a minimum.
- 3.3 Sensitive authentication data (SAD) is not stored after authorization.
- 3.4 Access to displays of full PAN and ability to copy PAN are restricted.
- 3.5 Primary account number (PAN) is secured wherever it is stored.
- 3.6 Cryptographic keys used to protect stored account data are secured.
- 3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

¹ This requirement is a best practice until 31 March 2025, after which it must be fully considered as part of a PCI DSS assessment.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

ENCRYPTION PRIMER

Cryptography uses a mathematical formula to render plaintext data unreadable to people without special knowledge (called a "key"). Cryptography is applied to stored data as well as data transmitted over a network.

Encryption changes plaintext into ciphertext.

Decryption changes ciphertext back into plaintext.

This is secret stuff, please do not...

→ 5a0 (k\$hQ% ...

→ This is secret stuff, please do not...

Illustration: Wikimedia Commons

25

Elements of Account Data and Storage Requirements

Table 3 in PCI DSS (see below) identifies the elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be rendered unreadable - for example, with strong cryptography - when stored. This table is not exhaustive and is presented to illustrate only how the stated requirements apply to the different data elements.

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable
Account Data	Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum as defined in Requirement 3.2	Yes, as defined in Requirement 3.5
		Cardholder Name	Storage is kept to a minimum as defined in Requirement 3.2 ²	No
		Service Code		
		Expiration Date		
	Sensitive Authentication Data	Full Track Data	Cannot be stored after authorization as defined in Requirement 3.3.1 ³	Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
		Card verification code		
		PIN/PIN Block		

² Where data exists in the same environment as PAN.

³ Except as permitted for issuers and companies that support issuing services. Requirements for issuers and issuing services are separately defined in Requirement 3.3.3.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

26