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 and Division of Information and Technology (DoIT) 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 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 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.

C. **Annual review of credit card environment**. This requirement also includes the creation and maintenance of a departmental Teams channel for PCI A representative from DoIT 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 Teams channel for PCI. This channel 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 Teams channel for PCI has been created, merchants are required to bring this information to the annual PCI meeting that is scheduled with DoIT.

D. **Quarterly scans of all outward facing IP addresses** that fall within the scope of PCI. DoIT 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:**

N/A