Payment Card Industry-Data Security Standard (PCI-DSS) Summary

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-PCIDSS		strevena@csustan.edu	1.0	Stan Trevena	209.667.3137

What is PCI?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of information security requirements or standards that organizations processing credit card data must follow in order to enhance the security of payment card systems. The Security Standards Council (SSC) is responsible for administering the evolution of the PCI DSS standard. It is an independent body consisting of the five major payment card brands (MasterCard, Visa, American Express, Discover, JCB).

Why?

Stanislaus State is committed to privacy and security. Protection of credit card data processed in University commercial operations is the duty and mission of the University, and individuals handling this information play a critical role in helping not only improve security, but help safeguard sensitive cardholder data. The University has a history of leadership in establishing improvements in privacy and security of sensitive information for universities. Finally, Stanislaus State commercial operations process customer credit card information, so they are in scope and must comply with PCI. Therefore, Stanislaus State is mandated by the Security Standards Council (SSC) to comply with the PCI Data Security Standard (DSS), to provide security for the protection of cardholder data and key systems and applications processing this data. Any merchant that processes, stores, or transmits credit card data receives a merchant ID (MID), and must comply with the standard in order to maintain a secure credit card environment. Failure to comply with PCI can have serious short and long-term consequences for the University. In some cases, data breaches of credit card data will result in damaged reputation, fines by the payment card issuer, government fines, lawsuits, and insurance claims.

Finer Points

PCI DSS defines “cardholder data” as any personally identifiable information associated with a cardholder. This can include the credit card number, expiration date, name, address, and social security number. Any personally identifiable information associated with the cardholder that is stored, processed, or transmitted by the merchant is considered cardholder data, and within the “scope” for PCI. Merchants, within the context of PCI, are entities that accept payment cards as payment for goods and services, when those cards are bearing the logos of any one of the payment card brands (Visa, MasterCard, Discover, JCB, and American Express). There are four levels of PCI merchants, and the levels are determined by the annual number of credit card transactions processed by the merchant. Level 1 Merchants process over 6 million transactions per year, and must meet the most stringent security requirements of PCI DSS. The latest version of the standard is version 3, and it specifies 12 security requirements that must be met for compliance. For noncompliance violations of PCI, the payment brands can fine an acquiring bank up to $100,000 per month.

The banks will normally pass these fines downstream until it hits the merchant. For more information, refer to the website for the PCI Security Standard [1].

What You Need to Know

At Stanislaus State, individuals that handle PCI cardholder data play a key role in helping to safeguard sensitive personal information of students, faculty, and campus guests who use the goods and services at Stanislaus State. It is the responsibility of everyone involved to help protect this information. Being proactive with security in mind can help prevent PCI data breaches from taking place.

- Stanislaus State must comply with the PCI Data Security Standard (PCI DSS), for any cardholder data processed, stored, and transmitted in Stanislaus State commercial operations.
- Protect PCI cardholder data with encryption: Cardholder data (Primary Account Number (PAN), Cardholder name, Service Code, Expiration Date) must be stored encrypted on any laptop or computer processing this sensitive data.
- The Primary Account Number must be masked when displayed: Under PCI, the 16 digit PAN must be masked when displayed. The maximum number of displayed digits is the first 6 and the last 4. Pay close attention to web applications that display PAN, and report any violations to the Information Security Officer.
- Protect computers with Security Best Practices in Mind: For any computers processing PCI information, keep in mind some security best practices:
    - Robust passwords: Follow robust password guidelines outlined by the university. For more information on the password standard requirements, refer to the Stanislaus State "Password Standard" [2].
    - Never share or disclose your password to a 3rd party.
    - Malicious Emails and Attachments: Follow common sense and avoid clicking on suspicious links and opening suspicious attachments via email.
    - Use Anti-Virus program: Ensure to keep Anti-Virus programs up to date, active, and periodically scanning your computer for malicious software and attachments.

- University PCI information is classified as Level 1 information, and must meet University security requirements for protection of Level 1 information. For more information on the requirements for encryption and handling of PCI restricted information, refer to the Stanislaus State "Information Classification and Handling" security standard [3].
- Organizations are required to report PCI data breaches, and California is a leader in establishing these data breach notification laws. For suspected PCI data breaches, refer to the Stanislaus State Information Security Officer.

More Information

[1] PCI Data Security Standard (External Link) https://www.pcisecuritystandards.org/security_standards/

[2] Stanislaus State: "Password Standard"

[3] Stanislaus State: "Security Standard for Information Classification and Handling"