Payment Card Data Security Compliance

PURPOSE

Due to rapidly-evolving financial crimes and computer-related security challenges, the payment card industry has published specific Payment Card Industry Data Security Standards (PCIDSS) in an effort to better secure payment account data in a globally consistent manner. The payment card industry includes MasterCard Worldwide, Visa International, and American Express. Departments and business units throughout the Washington State University system may need to enter into WSU's master merchant agreement with credit card processors as part of their business transaction services.

All University departments which process credit card transactions are required to adopt and implement tools, practices, and policies to comply with these data security standards. Failure to comply may result in financial penalties or security breaches with the consequence of loss of acceptance of credit cards.

This policy helps ensure that Payment Card Industry Data Security Standards compliance requirements are met by University business units and departments. Contact Finance and Administration regarding University requirements and procedures for using and reporting contracted payment card services, and procedures for obtaining and maintaining merchant agreements.

POLICY

See Definitions for definitions of terms and acronyms used in this policy.

Payment Card Industry Data Security Standards (PCIDSS)

All University departments that process credit card transactions are required to comply with and support the Payment Card Industry Data Security Standards (PCIDSS).

Each year, all departments which process credit card transactions are required to submit completed payment card data security compliance surveys to the E-Commerce Coordinator. The E-Commerce Coordinator sends the surveys to all credit card processing departments annually.

Merchant Agreements

University departments must coordinate any merchant agreement participation through the Associate Vice President for Finance.

Transaction Service Providers

All departments which process credit card transactions are required to use PCIDSS-compliant transaction service providers approved by the Associate Vice President for Finance or designee.

Transaction Service Technology

WSU-hosted transaction service technology deployments must comply with all relevant University security policies, procedures, and practices in addition to the Payment Card Industry Data Security Standards.

Payment Card Data Security Compliance

Policy Exceptions

Any existing or future University credit card processing department with a specific need or operational requirement which is an exception to this policy must submit a formal written request for the exception to the Associate Vice President for Finance.

The Associate Vice President for Finance or designee performs the following actions:

- Reviews the request while consulting with the Information Technology Services Security Office.
- Notifies the requesting party regarding whether or not the exception is allowable.
- Notifies the requesting party of any specific conditions that must be honored as part of the exception.

APPLICABILITY

All current and future University departments that process credit card transactions and all temporary transaction services established to accept credit card transactions for specific activities or events are required to comply with this policy.

ENFORCEMENT

Failure to comply with this payment card data security policy results in both of the following:

- Restrictions on use or closure of merchant-account-related services.
- Disciplinary action up to and including termination of employment at Washington State University.

RESPONSIBILITIES

Assistant Vice President for Finance

The Associate Vice President for Finance is responsible for:

- Conducting oversight of the entire merchant credit card process.
- Implementing payment card data security policy and procedures across all campuses.
- Determining whether or not vendor/third parties meet industry certification.
- Maintaining master merchant agreements with WSU's financial institutions.

Payment Card Data Security Compliance

E-Commerce Coordinator

The E-Commerce Coordinator is responsible for:

- Departmental training.
- Communicating changes to all merchants.
- Sending and reviewing annual payment card data security merchant compliance surveys.

University Information Security Officer

The University Information Security Officer is responsible for:

- Executing final approval of methods of credit card processing through websites and third-party software.
- Serving as a resource for Finance and Administration Systems Support and/or merchants regarding electronic-security-related issues.

University Controller

The University Controller is responsible for enforcing this policy.

DEFINITIONS

Merchant Agreement Holder

A merchant agreement holder is defined as any business unit or department which holds a merchant agreement with any payment card industry (PCI) service provider. This includes terminal-based payment system owners and online web-based application system owners.

Payment Card Industry Data Security Standards (PCIDSS)

The Payment Card Industry Data Security Standards (PCIDSS) are defined as information security standards published by the PCI Security Standards Council that all merchant agreement holders are required to adopt and implement. Failure to comply may result in serious fines, penalties, and/or restrictions on merchant account activity.

The specific data security standards compliance requirements are available on the PCI Security Standards Council website, at:

www.pcisecuritystandards.org/

Transaction Service Provider

A transaction service provider is defined as a third party which provides a secured processing connection with the merchant agreement holders transaction processing bank.