Title: PCI Compliance Policy
Approved by: PCI Compliance Committee
Date Approved by PCI Compliance Committee: November 14, 2019
Effective Date: November 14, 2019
Responsible Official: Treasurer
Responsible University Office: Office of the Treasurer
Period Review: 3 Years

Purpose

This policy document provides information to ensure CWRU complies with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the PCI DSS is to protect cardholder data. This document represents CWRU's procedures to prevent loss or disclosure of customer information including credit card numbers. Any failures to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of the University. The PCI Compliance Team's purpose is to educate all entities in the University's payment environment and to enforce the PCI DSS policies contained herein. Questions regarding this policy should be directed to CWRU's Treasurer's Office.

Scope

This policy applies to all campus users, external merchants, systems and networks involved with the transmission, storage, or processing of payment card data which utilize the university IT infrastructure to perform payment card processing. Payment card data includes primary account numbers, cardholder name, expiration date, service code, and sensitive authentication data.

Cancellation

Not applicable.

What is PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council web site (https://www.pcisecuritystandards.org)

In order to accept credit card payments, CWRU must prove and maintain compliance with the Payment Card Industry Data Security Standards. This policy provides the requirements for processing, transmitting, storage and disposal of cardholder data of payment card transactions, to reduce the institutional risk associated with the administration of credit card payments by university departments and to ensure proper internal control and compliance with the PCI DSS.

Policy Statement

General

The university does not support payment card processing in university-owned systems. The strategy is to outsource all payment card processing to off-site, PCI-compliant vendors, thereby minimizing the PCI compliance scope for university owned business processes (where the University is the merchant). In particular cases, where merchants are on-campus facilities, or use IT infrastructure within the university's scope, these standards apply.

All PCI-DSS processing merchant activity must be approved annually by the University Treasurer's Office.

CASE WESTERN RESERVE UNIVERSITY EST. 1826

Standards

CWRU [U]Tech publishes technical standards approved by the University Treasurer's Office. The standards described here are generalized to cover current and possible future Payment Card Industry security standards.

- All payment card transmission will utilize fully encrypted pathways from the card entry to the payment processing merchant.
- Network transmission of payment card information must not occur on campus academic networks.
- No storage, processing, or archival of payment card data in university academic or business IT environments is permitted. This process keeps any university academic networks out of scope for PCI compliance, and ensures customers and merchants using payment cards of the integrity of their payment card information.
- Regular auditing using data loss prevention tools must be performed to ensure minimized risk of payment card data.
- Credit card activity must settle to a CWRU bank account. Settlement through **personal** bank accounts is prohibited.

Responsibility

- CWRU members must follow the university's PCI DSS administrative and technical policies.
- University departments: When credit card processing is part of the department business process, perform an annual PCI DSS self-assessment (SAQ) and submit the report to the University Treasurer's Office for approval.
- Any department accepting payment card data must designate an individual(s) who will have primary authority and responsibility for payment acceptance.
- All departments, users accepting payment cards will complete PCI training upon hire and annually thereafter. See UTECH Policy III-1e Controls – Restricted Information: Case Information Security Requirements for Restricted Information.
- Any CWRU department accepting payment cards will utilize only Treasurer's office approved equipment to process card payments.
- Campus merchants: Ensure all credit card processing is performed in accordance with PCI DSS policy. Complete annual reporting of attestation of compliance to the CWRU Treasurer.
- All payment devices that process credit cards must be stored in a locked space with limited access when not in use.
- CWRU Information Security Staff: Perform regular vulnerability scanning of network devices where PCI payments are scanned, submitting risk reports to the University Treasurer's Office. Support software for data loss prevention service for users to audit IT systems for presence of PCI data.
- CWRU Network Management: Address and correct any deficiencies or risks found in the network security evaluations; deny network services to non-approved merchant activities.

- Treasurer's Office: Maintain a list of all devices that capture payment card data to include the make, model, serial number (or other method of unique identification) and location of device. The list will be updated when devices are added, relocated or decommissioned.

PCI-DSS Policy

Designated Individual

Any department accepting payment card payments on behalf of CWRU for gifts, goods or services must designate an individual (staff or faculty) within the department who will have primary authority and responsibility for payment card transaction processing. Each department must have a designated individual at all times. It is up to the department head to ensure this role is filled.

The responsibilities of the designated individual include, but are not limited to the following:

- Ensure employees within their department who will be responsible for payment card transaction processing or have access to the processing devices complete annual PCI training and are aware of and understand the policies and procedures surrounding this activity.

- Ensure only approved hardware/software is utilized to process card payments.

- Ensure devices/terminals are protected from tampering when unattended and that portable devices are physically secured when not in use.

Credit Card Acceptance and Handling

In the course of doing business it may be necessary for a department or other business unit to accept payment cards. The opening of a new merchant account for the purpose of accepting and processing of payment cards is done on a case by case basis. Any fees associated with the acceptance of payment cards will be charged to that unit. Interested departments should contact the Treasurer's Office to begin the process of accepting credit cards.

Transmitting

- Employees must be discreet and use common sense when handling credit card data.

- Payment cards may be accepted in person, via telephone (have constituent verify data twice, should not read credit card data back to constituent), through a PCI DSS compliant system, or physical mail.

Non-compliance

In the event of non-compliance when CWRU is the merchant:

- Treasurer's office will send communication to the head of the responsible department.

- The communication will explain the reason the location is non-compliant, the plan of action to become compliant, and a timeframe in which to complete the action plan.

- If the department does not meet the timeline to get compliant, the matter will be escalated to Senior Management, and at that point the decision will be made to either suspend payment card processing or extend the timeline. Each occurrence will be evaluated on a case by case basis.

In the event of a breach or a PCI violation, the payment card brands may assess penalties to CWRU's bank which will be passed on to the university. A one-time penalty of up to $500,000 per branch per breach can be assessed as well as on-going monthly penalties. Any fines or assessments which may be imposed by the affected credit card company will be the responsibility of the impacted unit.

In the event of non-compliance with a third party:

- Notification will be sent out.
- Vendor replacement if necessary.

Security Incidents

An incident is defined as a suspected or confirmed data compromise. A data compromise is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted data is collected, processed, stored or transmitted; payment card data is prohibited data. A data compromise can also involve suspected or confirmed loss or theft of any material or records that contain cardholder data.

In the event of a security event or incident, anyone with knowledge or a reasonable suspicion of an incident is instructed to make an immediate report to any of the following:

- The CWRU Help Desk 216-368-HELP (4357)
- The CWRU Security Fusion Center at 216-368-0084
- The email addresses of security@case.edu or abuse@case.edu
- Note: These email addresses may be used but are less effective than the direct notification of the Help Desk via voice communication or voicemail.

Definitions

PCI-DSS- Payment Card Industry Data Security Standard, v3.2.1
SAQ- Security Assessment Questionnaire

References

CWRU Draft Policy: I - 3 Credit Card Management and PCI-DSS Policy
Payment Card Industry Data Security Standard, v.3.2.1
(https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf)

Standards Review Cycle

This policy will be reviewed every three years on the anniversary of the policy effective date, at a minimum. The policy may be reviewed on a more frequent basis depending on changes of risk exposure.