PAYMENT CARD INDUSTRY SOFTWARE SECURITY FRAMEWORK

PCI SECURE SOFTWARE STANDARD

CORE REQUIREMENTS & OBJECTIVES

Applies to all types of payment software submitted for validation under the PCI Software Security Framework, regardless of the software's functionality or underlying technology

Secure Objective 1 :

Minimizing the Attack Surface

Critical Asset Identification

All software critical assets are identified and classified.

Secure Defaults

Default privileges, features, and functionality are restricted to only those necessary to provide a secure default configuration.

Sensitive Data Retention

Retention of sensitive data is minimized

Secure Objective 2 :

Software Protection Mechanisms

Critical Asset Protection

Critical assets are protected from attack scenarios.

Authentication and Access Control

Software implements strong authentication and access control to help protect the confidentiality and integrity of critical assets.

Sensitive Data Protection

Sensitive data is protected at rest and in transit.

Use of Cryptography

SHA-256

Cryptography is used appropriately and correctly.

Secure Objective 3 :

Secure Software Operations

Activity Tracking

All software activity involving critical assets is tracked.

Attack Detection

Attacks are detected, and the impacts/effects of attacks are minimized.

Secure Objective 4:

Secure Software Lifecycle Management

Threat and Vulnerability Management

Software vendor identifies, assesses, and manages threats and vulnerabilities to its payment software.

Secure Software Updates

Software vendor facilitates secure software releases and updates.

Vendor Security Guidance

Software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of the software.

Module A
Account Data Protection

Applies to software that stores, processes, or transmits cardholder data (CHD) and/or sensitive authentication data (SAD).

A.1
Sensitive Authentication Data

Sensitive authentication data is not retained after authorization.

A.2
Cardholder Data Protection

Protect stored cardholder data.

Sources : PCI SSC Document Library

www.qrcsolutionz.com