highradius

# PCI DSS Compliance Checklist

# Requirement 1:

## Install and Maintain a Firewall Configuration to Protect Cardholder Data

# Related Goal:

## Build and Maintain a Secure Network

- Establish and implement firewall and router configuration standards that formalize testing whenever configurations change.
- Build firewall and router configurations that restrict all traffic, inbound and outbound, from “untrusted” networks (including wireless) and hosts.
- Prohibit direct public access between the Internet and any system component in the cardholder data environment.
- Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the Internet when outside the network and which are also used to access the cardholder data environment.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 2:

## Do not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters

# Related Goal:

## Build and Maintain a Secure Network

- Always change all vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
- Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions.
- Using strong cryptography, encrypt all non-console administrative access.
- Maintain an inventory of system components that are in scope for PCI DSS.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.
- Shared hosting providers must protect each entity’s hosted environment and cardholder data.

# Requirement 3:

## Protecting Cardholder Data During Storage

# Related Goal:

## Protect Cardholder Data

- Limit cardholder data storage and retention time to that which is required for business. Purge unnecessary stored data at least quarterly.
- Do not store sensitive authentication data after authorization.
- Mask PAN when displayed, so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN.
- Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks.
- Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.
- Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 4:

## Encrypt Transmission of Cardholder Data Across Open, Public Networks

# Related Goal:

## Protect Cardholder Data

- Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.
- Never send unprotected PANs by end user messaging technologies.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 5:

## Protect All Systems Against Malware and Regularly Update Antivirus Software or Programs

# Related Goal:

## Maintain a Vulnerability Management Program

- Deploy anti-virus software on all systems commonly affected by malicious software. For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.
- Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7.
- Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 6:

## Develop and Maintain Secure Systems and Applications

# Related Goal:

## Maintain a Vulnerability Management Program

- AEstablish a process to identify security vulnerabilities, using reputable outside sources, and assign risk ranking.
- Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches.
- Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices.
- Follow change control processes and procedures for all changes to system component.
- Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines.

- Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerability assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 7:

## Restrict Access to Cardholder Data by Business Need to Know

# Related Goal:

## Implement Strong Access Control Measures

- ELimit access to system components and cardholder data to only those individuals whose job requires such access.
- Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 8:

## Identify and Authenticate Access toSystem Components

# Related Goal:

## Implement Strong Access Control Measures

- Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components.
- Employ at least one of these to authenticate all users such as a password or passphrase; a token device or smart card and biometric.
- Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication.
- Develop, implement, and communicate authentication policies and procedures to all users.
- Do not use group, shared, or generic IDs, or other authentication methods.

- Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account.
- All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 9:

## Restrict Physical Access to Cardholder Data

# Related Goal:

## Implement Strong Access Control Measures

- EUse appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
- Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.
- Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based on individual job function; access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled.
- Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel.
- Physically secure all media; store media back-ups in a secure location, preferably off site.
- Maintain strict control over the internal or external distribution of any kind of media.
- Maintain strict control over the storage and accessibility of media.
- Destroy media when it is no longer needed for business or legal reasons.
- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 10:

## Track and Monitor All Access to Network Resources and Cardholder dData

# Related Goal:

## Regularly Monitor and Test Networks

- EImplement audit trails to link all access to system components to each individual user.
- Implement automated audit trails for all system components for reconstructing these events.
- Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.
- Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.
- Secure audit trails so they cannot be altered.
- Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.
- Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
- Service providers must implement a process for timely detection and reporting of failures of critical security control systems.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 11:

## Regularly Test Security Systems and Processes

# Related Goal:

## Regularly Monitor and Test Networks

- AImplement processes to test for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
- Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

- Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification.
- Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network.
- Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

# Requirement 12:

## Maintain a Policy that Addresses Information Security for all Personnel

# Related Goal:

## Maintain An Information Security Policy

- Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.
- Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.
- Develop usage policies for critical technologies to define their proper use by all personnel.
- Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
- Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.
- Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.
- Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.
- Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of the customer, or to the extent they could impact the security of the customer’s cardholder data environment.
- Implement an incident response plan. Be prepared to respond immediately to a system breach.
- Service providers must perform and document reviews at least quarterly to confirm personnel are following security policies and operational procedures.