PCI v4.0 Compliance Checklist

STEP 1

Determine the Scope of Your Cardholder Data Environment (CDE)

□ Determine your PCI scope by identifying the people, processes, and technologies that touch or could otherwise impact your cardholder data.

□ As you're conducting your scoping exercise, you can sort systems into three buckets:

- **In-scope:** Systems that relate to, impact, or connect to the security of cardholder data
- **Connected:** Systems not directly involved in processing of cardholder data but are connected to your CDE
- **Out-of-scope:** Systems that to not interact with or connect to your CDE

STEP 2

Install and Maintain Network Security Controls

□ Protect the system that transmits cardholder data with a firewall or similar security measure

□ Schedule regular maintenance and upgrades to the firewall

STEP 3

Apply Secure Configurations to All System Components

□ Replace default passwords with strong passwords on every device and system

STEP 4

Encrypt Stored Account Data

□ Protect stored cardholder data in internal systems with robust security protocols

□ Do not store sensitive authentication data after authorization (even if it is encrypted)

□ Document your data retention policy for cardholder data storage and retention time to that which is required for business, legal, and/or regulatory purposes

□ Securely delete unnecessary stored data at least quarterly

STEP 5

Protect Cardholder Data with Strong Cryptography During Transmission Over Public Networks

□ Encrypt all in-transit cardholder data using an approved method of encryption

□ Protect cardholder data across open networks

STEP 6

Protect All Systems Against Malware

□ Employ antivirus and anti-malware software

□ Ensure software is regularly updated with the latest versions

STEP 7

Deploy and Maintain Secure Systems and Applications

- □ Secure your systems and applications
- □ Schedule regular maintenance and updates to your systems and applications
- □ Install applicable vendor-supplied security patches for system components and software within one month of release

STEP 8

Restrict Access to System Components and Cardholder Data by Business Need to Know

- □ Define strict roles that require access to cardholder data outlined in an authorization policy

STEP 9

Identify Users and Authenticate Access to System Components

- □ Set up a unique user ID for each person that requires access to your systems
- □ Assign a system administrator to oversee and manage user permissions
- □ Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography
- □ Periodically align user IDs with your authorization policy

STEP 10

Restrict Physical Access to Cardholder Data

☐ Restrict, monitor, and log all access to the physical facility that stores card holder data

STEP 11

Log and Monitor All Access to System Components and Cardholder Data

☐ Log and secure your processes for providing reliable audit trails

☐ Review logs and security events for all system components to identify anomalies or suspicious activity

STEP 12

Test Security of Systems and Networks Regularly

☐ Conduct internal and external network vulnerability tests at least quarterly and after any significant change in the network

☐ Create and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or change

☐ Implement network intrusion detection and/or intrusion prevention techniques

☐ Deploy a change detection mechanism to alert personnel of unauthorized modifications

STEP 13

Support Information Security with Organizational Policies and Programs

□ Develop an information security policy for the company and distribute it to all employees

□ Review the information security policy annually

□ Implement a risk assessment process that is performed at least annually and upon significant changes to the environment

□ Implement a formal security awareness program to train all employees on cardholder data security best practices

□ Screen potential employees prior to hire via background tests or reference checks

□ Develop an incident response plan in case of a data breach