

PCI

Pre-SAQ Checklist



A service of Mercury Payment Systems®

The purpose of this checklist is to prepare you for the official Self-Assessment Questionnaire (SAQ). It is not intended to replace the official PCI SAQ.

If you are unsure of the answers to questions related to your point-of-sale system and network, or if you need help reconfiguring your point-of-sale system or network for PCI DSS compliance, please contact your POS dealer or IT professional for assistance.

▶ **START**



Install and maintain a firewall configuration to protect data

- Do you have a firewall device protecting your point-of-sale systems or IP terminals from the internet and any other “untrusted” networks?
 - If yes, or if you do not have an internet connection or connections to other untrusted networks, place check in box
 - If not, install one today
- Does the firewall device prohibit inbound access to your point-of-sale systems? (e.g. Port forwarding or application forwarding should not be configured in the firewall device: it’s considered inbound access.)
 - If yes, or if you do not have an internet connection, place check in box
 - If not, modify your firewall configuration to prohibit inbound access

Do not use vendor-supplied defaults for system passwords and other security parameters

- Are unnecessary accounts disabled and default account passwords changed to something complex? Consider operating system accounts, point-of-sale accounts, router management accounts, and firewall management accounts.
 - If yes, place check in box
 - If not, disable unnecessary accounts and change default passwords immediately
- Were the default configurations changed for wireless (WiFi) access points connected to your point-of-sale network? Consider the SSID (network name), encryption key, and passwords.
 - If yes, or if wireless is not connected to the point-of-sale network, place check in box
 - If not, change the default configuration of wireless access points
- Are your wireless access points configured to require strong encryption? WEP encryption is not secure. WPA or WPA2 with a strong encryption key/password must be used.
 - If yes, or if it’s not applicable, place check in box
 - If not, reconfigure your wireless access points to use WPA or WPA2 with a strong encryption key
- Is all non-console/web-based administrative access encrypted using strong encryption (e.g. SSL and HTTPS)? Consider VPN, remote desktop, and administrative web pages for your point-of-sale systems.
 - If yes, or if there is no remote administrative access, place check in box
 - If not, reconfigure your administrative access to use strong encryption



Protect stored cardholder data

- After payment authorization, do your systems store the track data read from the magnetic stripe on credit cards? Storing track data after authorization is prohibited.
 - If not, place check in box
 - If yes, upgrade to a PA-DSS compliant version of your point-of-sale system
- After payment authorization, do your systems store the three or four digit card-validation code printed on the front or back of credit cards? Storing card-validation codes after authorization is prohibited.
 - If not, place check in box
 - If yes, upgrade to a PA-DSS compliant version of your point-of-sale system
- After payment authorization, do your systems store the personal identification number (PIN) data used for PIN debit? Storing PIN data after authorization is prohibited.
 - If not, place check in box
 - If yes, upgrade to a PA-DSS compliant version of your point-of-sale system
- After credit cards are first entered, does your point-of-sale system properly mask card numbers when displayed so a maximum of the first six and last four digits are shown (e.g. 400300XXXXXX6781)? Consider reports, history, tip adjustment, error correction, etc.
 - If yes, or full card numbers only display when needed, place check in box
 - If not, upgrade to a PA-DSS compliant version of your point-of-sale system

Encrypt transmission of cardholder data across open, public networks

- Is cardholder data encrypted using strong encryption when sent over the internet (e.g. SSL and HTTPS) or wireless networks (e.g. WPA with a strong key)? Consider when your point-of-sale sends cardholder data for approval and how you may receive orders with cardholder data over the internet.
 - If yes, place check in box
 - If not, upgrade to a PA-DSS compliant version of your point-of-sale system and/or change how card data is transmitted so that it's protected using strong encryption
- Do you have policies, procedures, and practices in place to ensure credit card information is not being sent or received unencrypted? Consider technologies like email, instant messaging, and chat.
 - If yes, place check in box
 - If not, create the necessary policies, procedures, and practices

Maintain a Vulnerability Management Program



Use and regularly update anti-virus software or programs

- Do you have anti-virus software on all of your point-of-sale computers, business computers, servers and personal computers that connect full time or part time to the point-of-sale network?
 - If yes, place check in box
 - If not, install anti-virus software

- Does your anti-virus software keep up-to-date with virus definitions?
 - If yes, place check in box
 - If not, renew subscriptions and/or configure it to automatically update daily

- Does your anti-virus software run at all times and generate activity logs?
 - If yes, place check in box
 - If not, keep anti-virus software enabled and configure it to log activity

Develop and maintain secure systems and applications

- Do your systems have the latest vendor supplied security patches? Consider operating system security updates, point-of-sale software updates, and security updates for other installed applications.
 - If yes, place check in box
 - If not, keep all systems and software updated with security patches

- Are security patches installed within one month of release?
 - If yes, place check in box
 - If not, configure automatic updates or have a process in place to install patches at least monthly

Implement Strong Access Control Measures



Restrict access to cardholder data by business need-to-know

- Do you limit access to cardholder data and systems to only those users that have a business reason for access?
- If yes, place check in box
 - If not, reduce user privileges to only what they need to perform their job

Assign a unique ID to each person with computer access

- For remote access, are point-of-sale dealers, IT professionals, and other service providers only allowed to connect during time periods needed for maintenance after which access is disabled?
- If yes, place check in box
 - If not, work with them to meet this requirement

Restrict physical access to cardholder data

- Are all paper and electronic documents containing cardholder data physically secure?
- If yes, place check in box
 - If not, make immediate changes by locking up paper documents in fire proof safe and contact IT professional or point-of-sale dealer for assistance securing electronic data
- Is strict control maintained over internal and external distribution of media containing cardholder data? Consider backup tapes, CDs, DVDs, USB drives.
- If yes, place check in box
 - If not, make immediate changes
- Is media containing cardholder data classified and labeled as confidential?
- If yes, place check in box
 - If not, make immediate changes
- Is media containing cardholder data sent securely and tracked when transported?
- If yes, place check in box
 - If not, make immediate changes
- Do you have a process and procedure in place to ensure management approval prior to moving media containing cardholder data?
- If yes, place check in box
 - If not, make immediate procedural changes
- Is strict control maintained over the storage and accessibility of media containing cardholder data?
- If yes, place check in box
 - If not, make immediate changes
- Is paper containing cardholder information securely destroyed once it is no longer needed (i.e. shredded, incinerated, etc.)?
- If yes, place check in box
 - If not, make immediate changes
- Is media containing cardholder information securely deleted or wiped once it is no longer needed?
- If yes, place check in box
 - If not, make immediate changes

Regularly Monitor and Test Networks



Regularly test security systems and processes

- Do you search for the presence of unauthorized wireless access points on your point-of-sale network at least quarterly using a wireless analyzer?
 - If yes, place check in box
 - If not, start immediately and implement a schedule to do this at least quarterly

- Do you currently run quarterly internal and external network vulnerability scans to test changes in network, firewall modifications, product upgrades, etc.?
 - If yes, place check in box
 - If not, enroll in the Mercury Payment Systems PCI Partner Program



Maintain a policy that addresses information security for employees and contractors

- Do you currently have an established, published and maintained security policy that is dispersed to employees that covers the following:
1. An acceptable usage policy for all employees to define proper use of technologies and programs such as laptops, email, internet usage, wireless devices, remote-access technologies, etc.
 2. The policy clearly defines security responsibility for all employees.
 3. The policy defines the importance of protecting cardholder information.
 4. The policy defines security incident escalation procedures.
 5. Updates are made to the policy as changes occur.
 6. A review of the policy is given to employees at least once a year.
 7. If cardholder data is shared with service providers (e.g. payment gateways), do you have procedures and a policy in place to ensure they maintain PCI DSS compliance? Is there is a signed written agreement with them acknowledging responsibility for PCI DSS compliance and the security of your customers' cardholder data? Note: Mercury is a PCI DSS validated service provider, listed on Visa's website.
- If yes, place check in box
 - If not, establish a security policy and procedures immediately and provide employee training