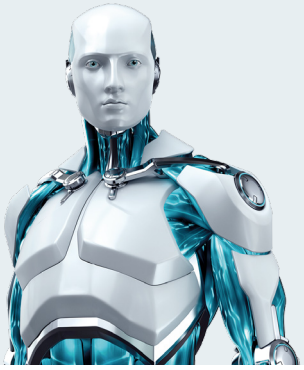
# PCI SECURITY CHECKLIST



If you store, process, or transmit payment card data in your retail business, then you are required to comply with the Payment Card Industry Data Services Standard (PCI DSS).

The latest version, *PCI DSS Version 3.2*, has requirements that are considered "best practices" through the end of January 2018. As of Feb. 1, 2018, they are requirements.

Use this checklist as a step-by-step guide through the process of understanding, coming into, and documenting compliance.*

## 1. Know the requirements of PCI DSS.

The heart of the PCI DSS standard is a set of six broad goals, achieved by meeting 12 requirements that are each supported by a number of best practices. The requirements and practices are, for the most part, simple commonsense security. For details, see the *PCI DSS Quick Reference Guide*.

## 2. Determine your merchant level for each card you accept.

A key component of PCI compliance is your "merchant level," based mainly on the number of transactions you handle annually, plus other criteria such as your number of ecommerce transactions. The card brands assess merchant levels differently, so be sure you know what level you have been assigned by each card brand you accept.

## 3. Contact your acquiring bank to assist you.

Acquiring banks are contracted to enforce the PCI DSS validation and reporting requirements on behalf of the card brands, so get in touch with them early on in the process for any special guidance or requirements. Note that in some cases, practices that are designated as "optional" by the card networks are required by acquiring banks.

## 4. Implement your security strategy with these steps and suggested products.

Track the flow of cardholder data through your systems so you know where and what you have to protect

Implement practices to protect against a data breach. Use layered security—firewalls, antivirus software, two-factor authentication, and encryption solutions— to protect your servers, endpoints, POS terminals and mobile devices.

### Note that two-factor authentication systems are now required for all "non-console" administrative access even when accessed by an employee from the company's internal network.

Implement bring your own device (BYOD) and social media policies.

- ESET Remote Administrator (included with ESET endpoint security solutions)
- ESET Endpoint Security
- ESET Secure Authentication (two-factor authentication)
- ESET Endpoint Encryption
- ESET Mobile Security for Android, ESET Mobile Device Management for Apple iOS

## 5. Make sure your payment processing vendors are approved.

Any PIN terminals you use, such as POS devices, encrypting PIN pads, and unattended payment terminals, must meet the PIN Transaction Security (PTS) requirements. Likewise, payment processing software must meet Payment Application Data Security Standard (PA-DSS). The *PCI Security Standards Council* maintains a list of approved devices and applications on its site.

## 6. Complete a Self-Assessment Questionnaire (SAQ).

The SAQ is the PCI DSS documentation of compliance for lower-transaction-volume merchants. There are five different versions of the SAQ, depending on the payment methods you use, whether you store cardholder data, and other factors. Refer to the *PCI DSS Quick Reference Guide* to determine which SAQ version you should use.

## 7. Perform an ASV scan (if required).

If required, based on your merchant level and standards set by either the card brand or your acquiring bank), contract with an Approved Scanning Vendor (ASV) to perform an ASV scan. Such a vendor scans your systems that connect to the internet for vulnerabilities. The PCI Security Standards Council maintains a list of ASVs on its site. Ask your acquiring bank whether the ASV vendor should send the results to you, or directly to your acquiring bank.

## 8. Submit your validation documentation (if required).

At the lower-volume merchant levels, you may not be required by the card brand to submit the SAQ or to perform an ASV scan. But either may be recommended or required at your acquiring bank's option. Regardless of whether you are required to validate, you are still potentially liable for data breaches if you do not meet the requirements of PCI DSS.

## 9. Put a plan in place to review your compliance efforts regularly.

PCI DSS compliance is a continuous process. When required, the SAQ is typically completed annually and the ASV scan quarterly. But security and protection against possible breaches are a year-round effort. Set up a system for regularly assessing your business processes for vulnerabilities. Plan to handle vulnerabilities immediately and document your actions to demonstrate that the required controls are in place.

## 10. Create an actionable employee education plan.

It's estimated that 25 percent of data breaches are due to human factors,[1] so be sure you provide ongoing cybersecurity education to reduce the risk. Your program should cover threats such as social engineering, phishing attacks, and web-borne malware and should include best practices such as using strong passwords as a way to prevent unauthorized access.

Also, because 30 percent of users open phishing messages and 12 percent open attachments in phishing messages,[2] consider email protection such as ESET Mail Security.

1—*2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute*

2—*Verizon 2016 Data Breach Investigations Report*

* *This document is intended as a general guideline, and does not replace or supersede the official standards and documents of the PCI Security Standards Council, or any requirements imposed by the card networks or your acquiring bank.*

ENJOY SAFER TECHNOLOGY®