PCI Compliance Overview

Credit card fraud and data security are constant threats to businesses, large and small. The payment card industry developed the Payment Card Industry Data Security Standard (PCI-DSS) to decrease credit card fraud and tighten potential data exposure. This standard applies to businesses that manage cardholder information for the major credit, debit, prepaid, ATM, and point of sale (POS) cards.

Objectives

- PCI Compliance Overview.

PCI Compliance Overview.

Before you can manage cardholder security, you need to set up your system. This is a multi-step process.

The first step is to ensure that you have role-based security configured. You must have Role-Based Security enabled before you can create roles and assign users to them. Once you have Role-Based Security enabled, you can have as many users as necessary for your business, but there should be at least two roles with six specific security bits set. We will explain more about the required security bits in another course.

Typically, you might assign these two roles to a system administrator and a supervisor. But why two roles? This is to avoid being locked out of the system if the password expires or if there are too many failed attempts for one of those *High-Security Password* Users.

Next, you need to create and maintain a secure network. Creating a secure network is like putting a fence around your business to prevent unauthorized people from accessing your data. Because not every employee needs access to cardholder data, you can also create a second secure network *within* your network. This helps protect cardholder data and regulate access to different groups or users within your organization.

Then you need to verify the RF Guns have *Secure Shell (SSH)* installed and turned on. Secure shell gives users and devices like these a safe method to access other computers over an unsecure network.

Next, you will set the server's IP address and ensure that the system is using *Secure Access*, not *Network Access.*

Then you will *Encrypt cardholder data* for transmission over unsecure networks. This reduces the likelihood of hackers stealing sensitive and valuable card information. An added security measure is to set a time frame for credit card information deletion in QuickRecall to 180 days or fewer. The system deletes any Credit Card information older than this date.

Once you have the PCI flag server and credit card encryption configured, you turn on the PCI flag in your system in System Options. With these settings in place, your system is *Payment Application Data Security Standard* (PA-DSS) compliant.

However, there are still a couple of steps to complete the process. First, you need to reboot the system and reload offline POS.

Then, to maintain current data, you must execute Create Offline Refresh (COR) every night. Be aware that *Create Offline Refresh* can take time to complete, and it must finish before updating offline files.

This completes the process of activating PCI flags.

To summarize the PCI procedure, you should complete the following steps: Role-Based Security Configuration, Create and Maintain Secure Network, Secure Shell (SSH), Server's IP Address, Encrypt Cardholder Data, Enable PCI Flag, System Reboot, Reload Offline POS, and Create Offline Refresh.

Recap

Configuring your system to comply with Payment Card Industry security standards helps keep your customer's financial data secure and build confidence in your business.

About Epicor

Epicor Software Corporation drives business growth. We provide flexible, industry-specific software that is designed around the needs of our manufacturing, distribution, retail, and service industry customers. More than 40 years of experience with our customers' unique business processes and operational requirements is built into every solution—in the cloud, hosted, or on premises. With a deep understanding of your industry, Epicor solutions spur growth while managing complexity. The result is powerful solutions that free your resources so you can grow your business. For more information, connect with Epicor or visit www.epicor.com.

EPICOR

Corporate Office
804 Las Cimas Parkway
Austin, TX 78746
USA
Toll Free: +1.888.448.2636
Direct: +1.512.328.2300
Fax: +1.512.278.5590

Latin America and Caribbean
Blvd. Antonio L. Rodriguez #1882 Int. 104
Plaza Central, Col. Santa Maria
Monterrey, Nuevo Leon, CP 64650
Mexico
Phone: +52.81.1551.7100
Fax: +52.81.1551.7117

Europe, Middle East and Africa
No. 1 The Arena
Downshire Way
Bracknell, Berkshire RG12 1PU
United Kingdom
Phone: +44.1344.468468
Fax: +44.1344.468010

Asia
238A Thomson Road #23-06
Novena Square Tower A
Singapore 307684
Singapore
Phone: +65.6333.8121
Fax: +65.6333.8131

Australia and New Zealand
Suite 2 Level 8,
100 Pacific Highway
North Sydney, NSW 2060
Australia
Phone: +61.2.9927.6200
Fax: +61.2.9927.6298