



## Risk

- Although it is just one part of the overall PCI requirements, if your system is not PA-DSS validated, your business is at **extreme financial risk**. Get, and keep, your CounterPoint system PA-DSS compliant with the [CounterPoint Subscription Service](#)..

- **PCI-Compliant Software and Services**
- In today's world of heightened security concerns, Radiant is committed to providing you with solutions that protect your customers' information. All of our latest software versions go through an extensive audit process to ensure that they are validated with the Payment Application Data Security Standards (PA-DSS).

- CounterPoint V7 and CounterPoint SQL are approved by Visa as PA-DSS Validated Payment Applications. In addition, CPGateway and CPOne are approved by the PCI Security Standards Council (PCI-SSC) as PCI-Compliant Service Providers. As PA-DSS-Validated Payment Applications, CounterPoint V7 and CounterPoint SQL adhere to all PA-DSS requirements through the security features below:

- Password security settings support PCI-compliant password policies.
- All passwords and credit card numbers are encrypted.
- Full credit card numbers are not displayed or printed; all card numbers are masked to display only the first 6 and the last 4 digits.
- Magnetic stripe track data is not retained in the CounterPoint database.
- CVV2/CVC2/CID data (i.e., verification numbers printed on each card) is not retained.
- Retention of full credit card numbers in history is optional; full card numbers retained in history are encrypted.
- **Keeping Your Software Compliant**
- PA-DSS requirements will continue to change. To meet the PCI-SSC's current and future PA-DSS requirements, you must keep your CounterPoint software up to date. CounterPoint Subscription Service (CSS) will keep your CounterPoint system compliant with the PCI-SSC's ever-changing requirements. With CSS, you automatically receive new CounterPoint features and enhancements as they are added to the software.
- If your CSS is expired, you can [renew online today](#).

## Security Practice #1 - Implementing Secure Remote Access Processes

- Breaking into a system through insecure remote connections is one of the most common tactics criminals use to steal sensitive consumer data. It is extremely important that you are using secure practices when remotely supporting your customers' sites.
- While there are many tools available with a wide range of functionality, one requirement applies to all of them. You must make sure you are implementing them in a secure manner. If you are unable to implement a tool according to the guidelines below, it is not suitable for securely supporting your customers. In addition to your support needs, the guidelines below should also be followed by your customers when using tools to access their sites remotely.

- **What to do when selecting/configuring a remote access tool:**
  - Ensure all default passwords are removed from the remote access software and use unique and complex passwords for each customer.
    - Passwords should be at least 7 characters long and include both alphabetic and numeric characters.
  - Ensure there is a mechanism in place for rotating passwords every ninety days.
  - Ensure encrypted data transmission of at least 128 bits is enabled on the remote access software.
  - Ensure account lockout after a maximum of 6 failed login attempts is enabled.
  - Ensure there is a mechanism for forcing automatic logoff after 30 minutes of inactivity.
  - Ensure the logging function on the remote access software is enabled.

- **What NOT to do when selecting/configuring a remote access tool:** Do not use "free" versions of remote access tools. These versions are for personal use only and are not approved for business use.
- Do not use Windows Remote Desktop without:
  - Running it over a secure protocol such as a Virtual Private Network (VPN) connection through a firewall.
  - Using two-factor authentication to sign in to the Terminal Servers.
  - Using a dedicated SQL Server on a separate logical network.
- Telnet should never be enabled at your customer sites due to significant security concerns.

## Security Practice #2 - Implement adequate password controls

- **PCI-DSS Password Requirements**  
One of the requirements for your customers to be PCI-DSS compliant is that they implement a password security policy that meets the requirements outlined in the guidelines. These security requirements apply to both Windows passwords and CounterPoint passwords.
- PCI-DSS compliant password security mandates that:
  - All user IDs and passwords are unique.
  - Passwords are complex (i.e., they contain both numbers and letters)
  - Passwords are at least seven characters long
  - Passwords are valid for a maximum of 90 days
  - A maximum of six unsuccessful login attempts is allowed
  - Each user creates at least four different, unique passwords before re-using a particular password
  - Each user that has access to CounterPoint terminals must have their own account. In addition, any user that has access to the back office server must have their own Windows user account. For both account types, users must be automatically locked out after a period of inactivity.

## Security Practice #2 - Implement adequate password controls

- **Password Management**  
With the implementation of these more stringent requirements, password management has become a more complicated task. The recommendations below are not comprehensive in scope, but will help both you and your customers define a password management policy that works best with your policies and infrastructure:
  - Never use default accounts for implementation and/or support.
  - Resellers should not maintain a password list on behalf of any customer.
  - End users should avoid using their own name, store name, or other obvious words as the primary component of their password.
  - End users should not write down passwords and post in plain sight as memory aids.
  - End users should treat passwords for any business application that handles sensitive data as securely as they treat passwords for their personal finance applications.

## Security Practice #2 - Implement adequate password controls

- **CounterPoint Passwords**  
CounterPoint allows you to easily establish complex passwords that meet the requirements outlined in the PCI-DSS guidelines. If your password settings do not meet the minimum PCI requirements, the message **Password settings not PCI DSS compliant - Click here to fix** appears on the Main tab in the Company window.

## Security Practice #3 - Regularly perform procedures to securely remove any sensitive data no longer needed and securely delete any unallocated space

- **What is Secure File Removal?**
- Many people do not realize that simply deleting a file does not mean it cannot be recovered. File deletion is different than secure file removal. When deleted, a file moves to the Recycle Bin but the link still points to the file retained on the hard drive. The space previously occupied in the hard drive is now freed as unallocated space. The retained file is only overwritten when the drive space is needed. On larger drives it will take years for this to happen. Secure file removal is a secure method of ensuring that data is irreversibly deleted and helps you avoid potential exposure associated with the support of sensitive data such as track data, account numbers, etc. An example of the exposure that can be associated with not securely removing files is highlighted in a 2003 research study from MIT. Two students purchased 158 used disk drives from readily available sources for used computer hardware. Of those 158, 81% were functional
  - 60% of the disks were formatted
  - 45% of the disks contained no files, yet data was still retrieved from them
  - 18% had little or no attempt to erase information
  - Less than 8% were properly sanitized
  - One came from an ATM and contained a year's worth of transactions
  - From those drives, over 5000 credit card numbers, personal and corporate financial records and medical records were found.

## Security Practice #3 - Regularly perform procedures to securely remove any sensitive data no longer needed and securely delete any unallocated space

- **When should I run a secure file removal process?**
- Secure file removal utilities can be used to wipe a file, folder contents or entire hard drive. If you are supporting sensitive data, you should perform a secure file removal on your hard drive. Any time sensitive data is written and no longer needed for business purposes
  - Sensitive data includes any data surrounding a credit card: account number, card verification number, PIN, or especially track data. It is also a good idea to treat personnel information such as Social Security numbers, etc as sensitive.
- After any update of CounterPoint or other payment application
  - Updates include major release changes as well as minor service pack installations
- During hardware return to service. Even if hardware is ghosted, this does not necessarily mean it was securely wiped. (Radiant uses secure file removal procedures on hardware returned to Shiloh office.)
- In addition, when you have completed work on log files or transaction files containing sensitive data, you should place them in a single repository. This repository should be wiped frequently, at least once weekly. Some file removal utilities allow you to set this up as a recurring task, but it can also be done manually.

## Security Practice #4 - Install a hardware firewall

- **Choosing The Right Firewall**
- One of the most important things customers can do to secure their data and work towards PCI compliance is install and maintain a commercial grade firewall. In fact, requirement #1 of PCI-Data Security Standard (PCI-DSS) requires customers to have and maintain a firewall to protect cardholder data. Additionally, to meet the details of the standards, customers must implement a more robust firewall than the home computer firewalls that are available off the shelf at a standard electronics store. At a high level, the PCI-DSS requires the firewall to include the following features not available on home computer firewalls:
  - Intrusion prevention system (IPS) with regular updates to IPS list of potential threats
  - Filtering incoming data traffic for malware
  - Network segmentation to keep cardholder data separate from email, internet, etc
- To help our customers better secure their sites and work toward PCI-DSS compliance, Radiant will begin offering the WatchGuard XTM firewall to CounterPoint customers in September 2010. The CounterPoint team is currently performing baseline testing for both v7 and v8 with the WatchGuard firewall to minimize any issues that may arise during implementation. When the WatchGuard firewall is released, we will provide you with installation documentation and a CounterPoint configuration template on the MySara portal. In addition, to coincide with the launch of this product, WatchGuard will provide training on basic installation and product information in the September data security webinar.

- For more information on the difference between commercial and a consumer grade firewalls and how the WatchGuard XTM meets the PCI-DSS requirements, please review the [WatchGuard XTM PCI-DSS Compliance Guide](#).
- Customers are not required to purchase a firewall from Radiant but they need to ensure they are implementing a commercial-grade firewall that is feature comparable to WatchGuard to meet PCI-DSS requirements. However, there are advantages to using a product aligned with Radiant including: AED warranty, joint testing, vendor coordination and CounterPoint customized documentation.
- If you have questions or concerns about a firewall other than WatchGuard that your customers are using today, first contact the technical support function for the firewall vendor. If you have additional questions, email us at [help@counterpointpos.com](mailto:help@counterpointpos.com).
- These guidelines can help secure your customers' business today. Please note, however, that there are more requirements than outlined here to be PCI compliant. More information about PCI requirements may be found at [www.pcisecuritystandards.com](http://www.pcisecuritystandards.com).

## Install anti-malware programs

- **Security Practice #6 - Ensure you are using version 7.5.12 CounterPoint or newer, or version 8.3.3 CounterPoint SQL or newer.**

## Security

- Ensure your operating system is up-to-date with security patches
- Prove compliance at specific points in time (SAQ/network scans)
- Implement operational security processes
- Consistently monitor your security infrastructure and procedures

## What can you expect from us? LPA and Radiant

- Ongoing security bulletins and webinars providing details on the PCI-DSS requirements and best practices related to each of the 10 areas of security focus identified above.
- A public website, [www.counterpointpos.com](http://www.counterpointpos.com), to educate existing customers and prospects across the retail industry with topics such as:
  - **PCI Compliance 101** - overview of the 12 PCI DSS requirements and what that means to retailers
  - **Data Security Milestones** - timeline of key dates regarding data security and compliance
  - **What you can do today** - key areas of concentration for protecting a site from risk (network configuration, remote access configuration, Windows/OS configuration, user management, POS configuration, auditing)
  - **Life Cycle of a Security Breach** - what happens to a retail merchant if they do get breached and the costs associated with this
- An enhanced data security section on [counterpointpos.com](http://counterpointpos.com) including all the information on the public website with additional information related to security and compliance related specifically to CounterPoint.
- Central contact point for questions related to PCI compliance and data security in general: [help@counterpointpos.com](mailto:help@counterpointpos.com).

