RETAIL BUSINESS MANAGEMENT SYSTEMS

New York, NY • East Rutherford, NJ • Philadelphia, PA

White Oak Corporate Center • 105 White Oak Lane • Suite 101 • Old Bridge, NJ 08857 • Toll Free (800) 506-4321 • Fax (732) 607-7755 • http://www.rbms.com

DATA SECURITY

Security Practice #3 – Implementing only PCI/DSS compliant Hardware
Big or small, credit card companies require every merchant to comply with Payment Card Industry Data Security Standards (PCI-DSS). The only exception is those that do *NOT* take credit cards. For more information, please see www.pcisecuritystandards.org. If they are not already doing so, all merchants must:

- Use only PCI/DSS compliant POS Hardware
  - POS Magnetic Strip Reader (MSR) must encrypt data at the time of the swipe.
  - MSR may not utilize a hardware keyboard wedge or equivalent device.
  - MSR may not utilize a software keyboard wedge or equivalent.

As a general rule of thumb, Radiant POS Terminals with integrated MSR **are** PCI/DSS Compliant. External keyboards with integrated MSR or external MSR devices **are not** PCI/DSS Compliant.

If you are not sure if your current hardware is PCI/DSS compliant please contact your POS Hardware vendor or manufacturer for more information.

a table providing more detail on selected topics to help merchants meet PCI requirements:

PCI Data Security Requirement	How you can meet this requirement...
Maintain a vulnerability Management Program	
Use and regularly update antivirus and antispyware software.	Install a reputable antivirus program that is also capable of detecting and removing spyware and adware. Update it immediately upon installation, and continue to update it regularly. Configure the antivirus program to run continuously, and ensure that it is generating audit logs. You can use separate antivirus and antispyware programs, if you wish, as long as both fulfill the requirements.
Develop and maintain secure systems and applications.	Obtain and install all POS and operating system security patches and updates at least monthly.
Regularly Test and Monitor Networks	
Regularly test security systems and processes.	Perform regular security tests to expose vulnerabilities in systems and processes. Establish a schedule of physically examining and verifying that all security-related settings are set correctly in the CounterPoint system, and in any third-party programs that could impact security.
Maintain a policy that addresses information security for employees and contractors.	Create and maintain a process for explaining the security policy to all employees. In this process, discuss all requirements, authentication procedures, and more. Do not permit employee or customer memory cards, laptops, or PDAs in sensitive areas, and do not permit any e-mail or Internet access within the cardholder environment.

These guidelines can help secure your 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.org.