



CARD PAYMENT SECURITY

Payment Card Industry (PCI) Data Security Standard & Payment Application Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards, developed by payment companies, Visa, American Express, MasterCard, Discover and JCB International, to establish common processes and precautions for handling, processing, storing and transmitting payment card data. The PCI DSS states that it is the responsibility of every business who processes, transmits, or stores credit and debit card information to make sure that their system is in compliance with data security requirements.

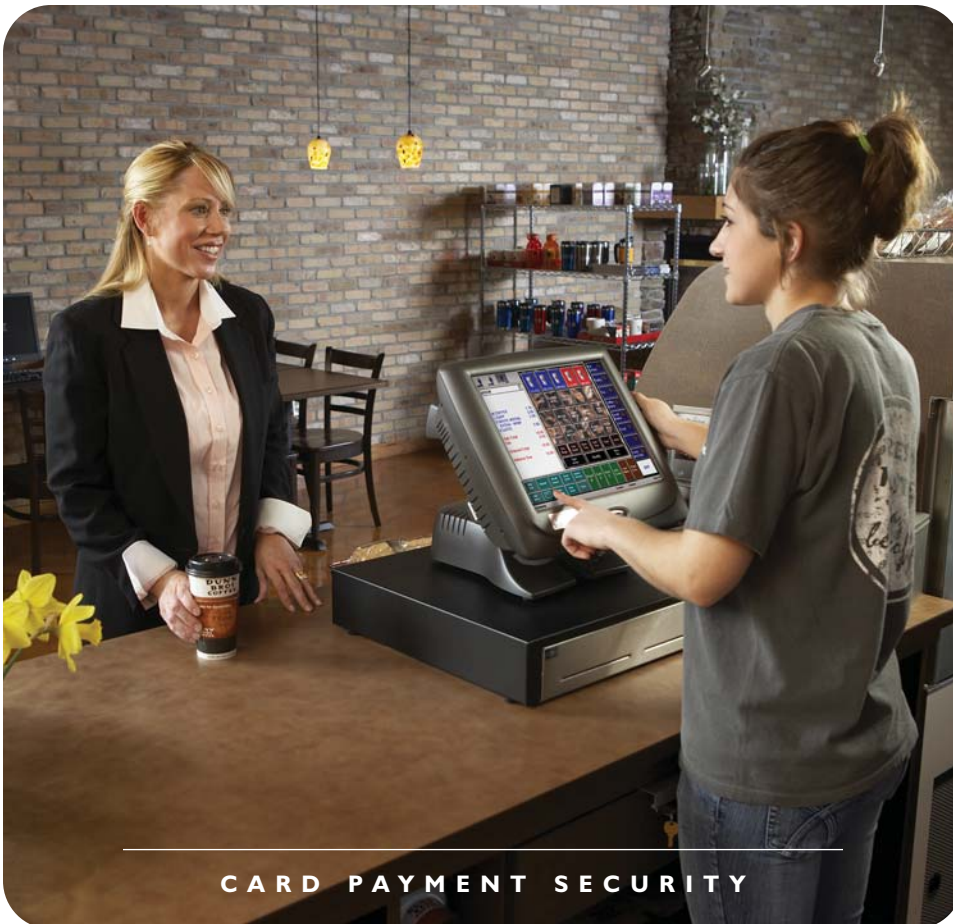
Radiant Systems' Aloha POS was one of the first POS technologies to be validated against VISA's initial set of data security requirements in 2005 and we have maintained payment industry validation when releasing new versions of our software (now called Payment Application Data Security Standard or PA DSS). With each new release of our software, we include features to proactively meet or exceed the PA DSS. These enhancements will continue to strengthen the security of our applications, but are just a small piece of the numerous requirements included in the PCI DSS.

▶ **WHAT IS THE PAYMENT APPLICATION DATA SECURITY STANDARD (PA DSS)?**

The PA DSS assists software vendors in developing secure payment applications that do not store sensitive cardholder data, ensuring that their products support compliance with the PCI DSS. Radiant Systems is listed as a vendor whose payment applications have been validated against the PA DSS.

▶ **HOW DOES YOUR ALOHA POS HELP SUPPORT YOUR PCI DSS COMPLIANCE?**

One of the most critical aspects of the 12 PCI DSS requirements is to ensure that full credit card track and CVV data is not stored in any form after authorization is complete. Best practices have been developed to address security and the risks associated with all payment applications. Radiant Systems continuously develops and releases payment applications that are validated against PA DSS requirements.



CARD PAYMENT SECURITY

LIST OF VALIDATED PAYMENT APPLICATIONS – ALOHA POS VERSIONS

PCI Data Security Standards state that it is your responsibility, as a merchant, to ensure your system is in compliance with data security requirements. Radiant Systems, the manufacturer of the Aloha suite of products, is constantly working on software improvements that will meet or exceed the evolving PCI and payment application data security standards. These improvements will continue to strengthen the security of our applications in every enhancement release. Below is a list of versions of Aloha POS that have been validated against the Payment Application Data Security Standards. We strongly encourage our customers to adopt the most recent Aloha releases as they become available.

POS version number:	Validated against PABP/PA DSS version:	Current validation expires on:
Aloha v5.3.15	Pre-PABP v1.3	December 2, 2009
Aloha v6.1	PABP v1.3	June 2, 2010
Aloha v6.2	PABP v1.4	December 2, 2010
Aloha v6.4	PA DSS v1.1	October 2, 2013
Aloha v6.5	PA DSS v1.2	October 2, 2013

PCI DATA SECURITY STANDARD

While upgrading Aloha assists companies with some of the items directly related to the Payment Application Data Security Standard, it is the responsibility of the merchant to ensure that all PCI standards are met. PCI security requirements apply to all “system components” which is defined as every network component, server, or application included in the cardholder data environment. This can include, but is not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

PCI DATA SECURITY STANDARD	
Build and Maintain a Secure Network	<ul style="list-style-type: none"> ➤ Install and maintain a firewall configuration to protect data ➤ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ul style="list-style-type: none"> ➤ Protect stored data ➤ Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> ➤ Use and regularly update anti-virus software ➤ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ul style="list-style-type: none"> ➤ Restrict access to data by business need-to-know ➤ Assign a unique ID to each person with computer access ➤ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> ➤ Track and monitor all access to network resources and cardholder data ➤ Regularly test security systems and processes
Maintain an Information Security Policy	<ul style="list-style-type: none"> ➤ Maintain a policy that addresses information security

Source: <http://usa.visa.com>



FOR MORE INFORMATION, PLEASE VISIT US AT
WWW.RADIANTSYSTEMS.COM OR CONTACT US AT 877.794.RADS (7237)

NORTH AMERICA • SOUTH AMERICA • EUROPE • AFRICA • ASIA • AUSTRALIA