



CARD PAYMENT SECURITY

Payment Card Industry (PCI) Data Security Standard & Visa U.S.A. Cardholder Information Security Program (CISP)

In this age of heightened security concerns, Radiant is committed to providing our clients with solutions that assist them in avoiding financial and reputational losses as well as safeguard their customers' information. In a proactive effort to uphold consumer confidence in the security of the Aloha product, Radiant has successfully received validation with Visa U.S.A.'s payment application best practices for the Aloha POS Software version 5.3.15 and version 6.1 through Visa's Cardholder Information Security Program (CISP).

CISP defines a standard for securing Visa cardholder data wherever it is located. CISP compliance is required of all entities that store, process or transmit Visa cardholder data. CISP compliance reduces the risk of fraud and provides a safer, more secure processing environment for you and your credit and debit card customers. Merchants who are not compliant with CISP requirements pose a greater risk of credit card fraud and could be subjected to sanctions from Visa.

▶ **WHAT ALOHA PRODUCT IS VALIDATED?**

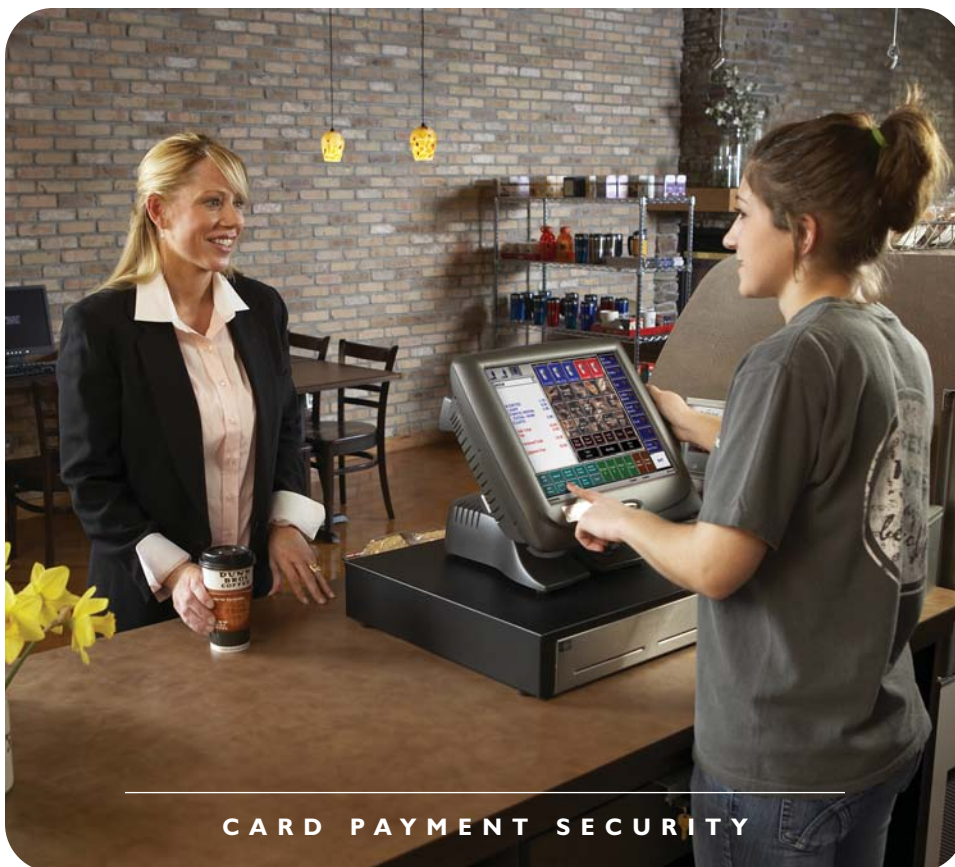
Aloha POS version 5.3.15 and version 6.1 has been verified against the PCI Data Security Standards and Visa CISP Best Practices by an independent third party.

▶ **WHO DOES CISP APPLY TO?**

CISP compliance is required of all entities that store, process or transmit Visa cardholder data.

▶ **HOW IS THE ALOHA PRODUCT ALIGNED WITH PCI STANDARDS?**

Visa U.S.A. has accepted Radiant Systems' CISP Payment Application Validation for Aloha POS version 5.3.15 and version 6.1 applications, based on the assessment and opinion of Ambiron, LLC.



CARD PAYMENT SECURITY

The Payment Card Industry (PCI) Data Security Standards is a result of collaboration between the various credit card associations and the federal government to create common industry security requirements. Each card association still maintains their own program identity name, for internal purposes within their operating rules and regulations, such as Visa CISP, Mastercard SDP (Site Data Protection), etc. However, they are generally referred to in a common language as the requirements of "The PCI Standards."

PCI DATA SECURITY STANDARD

Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard consists of 12 basic requirements supported by more detailed sub-requirements:

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

ATLANTA • DALLAS • LONDON • LOS ANGELES • MELBOURNE • MEMPHIS • PRAGUE • SINGAPORE

A-CISP-0707

© 2007 Radiant Systems, Inc. All rights reserved. Radiant Systems and design is a registered trademark of Radiant Systems, Inc. All other trademarks are the property of their respective owners.

