



## What is PCI and why should you care?

The Payment Card Industry Security Standards Council (PCI SSC) facilitates the broad adoption of the PCI security standards in an effort to enhance payment account data security. This council was organized and founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. You are responsible for handling sensitive payment card data according to the PCI DSS standards. You could experience any, or all, of the following, in the event of a data security breach, depending on the circumstances and whether you have taken the necessary steps to comply with PCI:

- ⇒ Heavy financial damages due to fines that range from \$50,000 to \$500,000.
- ⇒ A loss of reputation; therefore, a decline in the number of guests visiting your restaurant.
- ⇒ A temporary or permanent loss of your ability to accept credit cards as a form of payment at your restaurant.

Failure to comply with the PCI DSS standards could be very costly, and possibly even result in the loss of your business.

## How can you protect your business?

- ⇒ Use a POS system that has been validated against the Payment Application Data Security Standards (PA DSS), formerly supervised by Visa and known as Payment Application Best Practices (PABP). The PA DSS assists software vendors in developing payment applications that do not store sensitive cardholder data, thus ensuring their products are validated against the PCI DSS. Radiant Systems is pleased to say we are already listed as a vendor whose payment application has been validated. This list is available at [www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](http://www.pcisecuritystandards.org/security_standards/pa_dss.shtml).

More information about the PA DSS is available at [www.pcisecuritystandards.org/tech/pa-dss.htm](http://www.pcisecuritystandards.org/tech/pa-dss.htm).

- ⇒ Ensure your system is set up to comply with the Payment Card Industry Data Security Standards (PCI DSS). These standards are intended to help merchants proactively protect customer account data by helping you:
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

More information about the PCI DSS is available at [www.pcisecuritystandards.org/tech/index.htm](http://www.pcisecuritystandards.org/tech/index.htm).

We recommend you obtain the Aloha POS Data Security Handbook that applies to the version of Aloha<sup>®</sup> you are using, and use it as a starting point for configuring your sites for maximum security. We also recommend you take advantage of the ever improving security features by upgrading to the latest version of Aloha available.

- ⇒ Undergo an onsite data security assessment by a Qualified Security Assessor (QSA) or complete a Self Assessment Questionnaire (SAQ D), to identify any vulnerabilities within your system. The PCI DSS requires merchants to do this on an annual basis, to assist you with PCI DSS compliance. Merchants using Aloha must perform this self-evaluation using SAQ D, as this is the questionnaire that best applies to the Aloha POS. The PCI DSS also provides a set of frequently asked questions, to help you better understand the purpose of the council, and the PCI DSS.

The SAQ D, and all other materials, are available at [www.pcisecuritystandards.org/tech/saq.htm](http://www.pcisecuritystandards.org/tech/saq.htm).

- ⇒ Undergo a network scan through a PCI DSS Approved Scanning Vendor (ASV). This is required on a quarterly basis, to ensure network security.

More information is available at [www.pcicomplianceguide.org/pcicompliance-vendors.html](http://www.pcicomplianceguide.org/pcicompliance-vendors.html).

# PCI DSS Configuration Checklist

## Aloha POS v6.4 Configuration:

Install Aloha® version 6.4, the latest PA DSS validated version of Aloha available. Versions later than 6.4 inherit the security enhancements of this version.

Configure printer output to mask the card number and omit the expiration date.

In Maintenance > Store Settings > Credit Card group > Voucher Printing 2 tab:

- Select **Only show last 4 digits on all vouchers** from the 'Credit Card Number Mask' drop-down list.
- Select **Suppress Expiration dates**.

Create secure payment card tenders. In Maintenance > Payments > Tenders > Type tab:

- Select **Use Magnetic Card ONLY**.
- Clear **Print Expiration**.

**Note:** Requiring manager approval for manual card entry is not a PCI requirement; however, it does provide a means for making payment card data even more secure. You may want to allow your managers to enter a card number manually without encountering the Manager Approval screen by selecting 'Manual Card #' on the Financial tab for the manager access level.

On the Identification tab:

- Clear **Print on Check**.

Require each employee to use passwords for accessing the Front-of-House terminals and set them to expire regularly:

In Maintenance > Store Settings > Security group > POS Password Settings tab:

- Select **Required**.
- Type a number in **Min Password Digits**. We recommend at least 3 digits.

In Maintenance > Labor > Job Codes > Job Code tab:

- Select **Uses Password**.
- Select **Password Expires**.
- Type at least '30' in **Renew after \_\_\_\_ Days**.

Configure alternate security devices for use on the FOH terminals, such as fingerprint scanners, when installed. Activate fingerprint scanners in Maintenance > Hardware > Terminals > Readers tab.

**Note:** Using alternate security devices is not a PCI requirement; however, it does provide a means for making payment card data even more secure.

Configure back office security levels that provide no more access than required for each employee type, in Maintenance > Labor > Back Office Security Levels.

You must use a unique user name and complex, expiring password to access Aloha Manager, unless a 'super-key' is available. For Aloha v6.4, the Alt-X login method is no longer available. For Aloha versions earlier than v6.4, you must manually disable the 'Alt-X' login method. (Refer to RKS ID 6298.)

Add the DelTrack command line to Winhook to remove sensitive card data.

Run DelTrack, preferably within Winhook as part of the End-of-Day (EOD) process, to ensure you are not storing sensitive card data for longer than the recom-

Stop EDC activity logging, in Maintenance > Store Settings > System group > Troubleshooting tab.

- Clear **Debug Touch**.
- Clear **Debug EDC Services**.

## Network Configuration:

Verify Windows® is configured to purge the paging file each time you restart the BOH file server. Information about how to do this is available in the Microsoft® Knowledge Base.

Disable the 'Guest' user in Control Panel. Procedures for doing this vary slightly from one operating system to another.

Reconfigure all Aloha data and program directories relevant to remove the 'Everyone' user from them. Verify their configuration permits access only by the system administrator or other authorized accounts.

Install antivirus software, and obtain updates for it routinely and often. Daily is not too often.

Change all default passwords in routers, remote administrative software, or other third-party hardware or software, as appropriate.

Install Aloha(QS) in a secondary directory beneath the root, as in C:\Bootdrv\Aloha(QS).

Configure Aloha EDC to use an alternate path, outside the BootDrv share, to prevent network access to the EDC files. Accomplish this by creating a new environment variable (EDCProcPath) and moving the contents of the current EDC folder to the new location. (Refer to RKS ID 8755.)

Ensure procedures are in place to prevent opening a direct Internet connection from any computer on the Aloha network.

Configure CtlSvr, EDCSvr, RFSSvr, and any other Aloha related services or devices to use a network user account created specifically for this purpose.

Create a Windows user account specifically for use in the Aloha network, independent of any other network requirements. Use local security policy settings to restrict this Windows user account from logging on to the network. Select Start > Settings > Control Panel > Administrative Tools > Local Security Policy. Select Security Settings > Local Policies > User Rights Assignment in the left panel, then locate and double-click 'Deny logon locally' in the policy list. Use the resulting dialog box to add the Aloha Windows user account to the list of denied users.

Delete any default Windows user accounts provided by Radiant Systems or affiliated companies for use in initial configuration.

Disable Remote Desktop on routers, BOH servers, and POS terminals, if this remote access tool is not used to support the site. Radiant Systems strongly recommends using Command Center as the single means of remote access for Aloha POS systems, to ensure the highest level of site security.

Disable the System Restore feature in Windows.

