



Payment Card  
Industry Data Security  
Standard (PCI-DSS)  
Implementation Guide



**XERA® POS Payment Card Industry Data Security Standard (PCI-DSS) Implementation Guide**

**XERA® POS Version 2.0**

**PUBLISHED BY**

Aldelo, LP  
6800 Koll Center Parkway, Suite 310  
Pleasanton, CA 94566

Copyright © 1997-2016 by Aldelo, LP

All rights reserved. No part of the contents of this manual may be reproduced or transmitted in any form or by any means whatsoever without the written permission of the publisher.

This manual is available through Aldelo, LP and resellers worldwide. For further information, please contact Aldelo, LP or visit our website at [www.aldelo.com](http://www.aldelo.com). Send comments about this manual to [contact@aldelo.com](mailto:contact@aldelo.com).

Aldelo is the registered trademark of Aldelo, LP. Other products or company names mentioned herein are the trademarks of their respective owners.

The example companies, organizations, products, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, logo, person, place, or event is intended or should be inferred.

For the sake of simplicity, all gender references are written only in the masculine. Any references to the masculine gender should be interpreted to include the feminine gender as well and vice versa, wherever applicable.



| Reviewed by:              | Date       | Time     |
|---------------------------|------------|----------|
| Jeff Moore / Dave Ventura | 03/28/2013 | 02:11 PM |
| Jeff Moore / Dave Ventura | 04/04/2013 | 11:50 AM |
| Jeff Moore / Dave Ventura | 06/10/2013 | 09:20 AM |
| Jeff Moore / Dave Ventura | 02/13/2014 | 04:21 PM |
| Dave Ventura              | 08/06/2015 | 08:45 AM |
| Jeff Moore / Dave Ventura | 02/29/2016 | 04:13 PM |
| Jeff Moore / Dave Ventura | 07/01/2016 | 04:05 PM |
|                           |            |          |
|                           |            |          |
|                           |            |          |



# Table of Contents

|  |           |
|--|-----------|
| <b>Chapter 1: Introduction to PCI-DSS Compliance .....</b>                   | <b>9</b>  |
| <b>Chapter 2: PCI-DSS Payment Application Environment Requirements .....</b> | <b>11</b> |
| Remote Access .....  | 11        |
| Non-Console Administration .....   | 11        |
| Transport Encryption .....   | 12        |
| Cardholder Data Retention.....   | 12        |
| Manager Access .....   | 12        |
| Network Segmentation.....  | 13        |
| Windows Restore Points .....   | 13        |
| Information Security Policy / Program .....                                  | 15        |
| <b>Chapter 3: XERA® POS Configuration .....</b>                              | <b>17</b> |
| Baseline System Configuration .....  | 17        |
| Application Configuration .....  | 17        |
| Installing XERA® POS .....   | 17        |
| Application Requirements.....  | 18        |
| <b>Chapter 4: Updates and References .....</b>                               | <b>19</b> |
| Updates to XERA® POS .....   | 19        |
| Technical Support .....  | 19        |
| More Information .....   | 19        |
| Application Versioning Methodology.....                                      | 20        |
| <b>Chapter 5: PA-DSS v 3.2 Requirements .....</b>                            | <b>21</b> |





# Chapter 1:

# Introduction to PCI-DSS

# Compliance

Systems that process payment transactions necessarily handle sensitive cardholder account information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the Payment Card Industry Data Security Standard (PCI-DSS). The security requirements defined in the PCI-DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI-DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application, included in or connected to, a network segment where cardholder data is stored, processed, or transmitted.

The following 12 Requirements comprise the core of the PCI-DSS:

## **Build and Maintain a Secure Network**

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

## **Protect Cardholder Data**

3. Protect Stored Data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.

## **Maintain a Vulnerability Management Program**

5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

## **Implement Strong Access Control Measures**

7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

## **Regularly Monitor and Test Networks**

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

## **Maintain an Information Security Policy**

12. Maintain a policy that addresses information security.

The remainder of this document describes the essential guidance for implementing XERA<sup>®</sup> POS in a PCI-DSS compliant environment.



# Chapter 2:

# PCI-DSS Payment Application Environment Requirements

## Remote Access

The PCI-DSS standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment, access should be authenticated using a multi-factor authentication mechanism (username/password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited. Remote access should be disabled when not in use.

If remote access is used, the following guidelines must be adhered to:

- Change default settings in the remote-access software (for example, change default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication and complex passwords for logins (See PA-DSS Requirements 3.1.1 through 3.1.11)
- Enable encrypted data transmission according to PA-DSS Requirement 12.1
- Enable account lockout after a certain number of failed login attempts (See PA-DSS Requirement 3.1.8)
- Establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed
- Enable the logging function
- Restrict access to your environments by vendors for support to authorized integrator/reseller personnel

## Non-Console Administration

The XERA® POS application itself does not support non-console access. All access is through an application-provided interface. However, you as a merchant may choose to access the underlying systems remotely.

Users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop Protocol (RDP)/Terminal Server, etc., to access other hosts within the

payment processing environment; however, to be compliant, every such session must be encrypted with at least 128-bit encryption, although 256-bit encryption is preferred (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). Implement and use strong cryptography (such as SSH, VPN, or TLS) for encryption of any non-console administrative access to payment application or servers in the cardholder data environment. In addition, any non-console access must support the multi-factor authentication.

## Transport Encryption

The PCI-DSS DSS requires the use of strong cryptography and encryption techniques with at least a 128-bit encryption strength (either at the transport layer with TLS or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard sensitive cardholder data during transmission over public networks (this includes the Internet and Internet accessible demilitarized zone [DMZ] network segments).

Additionally, PCI-DSS requires that cardholder information is never sent via e-mail without strong encryption of the data.

The XERA<sup>®</sup> POS application uses TLS 1.2 for transmission of cardholder data to the processor. The application does not support the use of end-user messaging technology for the transmission of cardholder data.

## Cardholder Data Retention

The application will automatically purge all cardholder data upon batching and sending the data to your merchant processor.

As you may decide to retain cardholder data outside of the application using third party means (Excel spreadsheet, written hardcopy, etc.), you must understand that any cardholder data collected by you exceeding the defined retention period must be purged based upon business, legal, and/or regulatory requirements in order for you to achieve and meet your own PCI-DSS compliance requirements.

## Manager Access

The XERA<sup>®</sup> POS passwords are administered by the Master (first or primary) Administrator. This Master Administrator therefore is responsible to perform periodic password changes.

Additionally, the Master Administrator should sign an official acknowledgement form created or issued by the merchant organization of those manager access responsibilities.

Examples of Manager Access Responsibilities:

- Change the administrator account password periodically in compliance with PCI-DSS requirements
- Periodically perform security audit and transactional log audits in compliance with PCI-DSS requirements

- Maintain System updates, patches, and security perimeter configurations in compliance with PCI-DSS requirements
- Manage user or process accounts in compliance with PCI-DSS requirements
- Customers are advised to assign secure authentication to any default accounts (even if they will not be used) and then disable and do not use any default accounts
- Only system administrators should have administrator-level access to the system; all other users should have user-level access only
- Do not use default user names and passwords, such as “Administrator” and “12345”
- Always use unique user names and passwords
- Passwords must be strong and include a minimum of seven (7) characters, including letters (both upper and lower case), numbers, and special characters
- Users should never create shared usernames and passwords, as each user must have a unique username and password that is appropriate to his system access level
- The payment application requires users to change their passwords at least every ninety (90) days
- New passwords must be unique and cannot repeat any of the previous four (4) passwords used for that account
- The payment application must limit repeated attempts to access the system by locking out any user who fails to login successfully after six (6) attempts, as per PCI-DSS requirements
- When a user is locked out as described above, the lockout period is a minimum of thirty (30) minutes or until the administrator enables the user’s ID
- If an application session has been idle for more than fifteen (15) minutes, the application will automatically require the user to login again

## Network Segmentation

The PCI-DSS requires that firewall services be used (with NAT [Network Address Translation] or PAT [Port Address Translation]) to segment the network into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

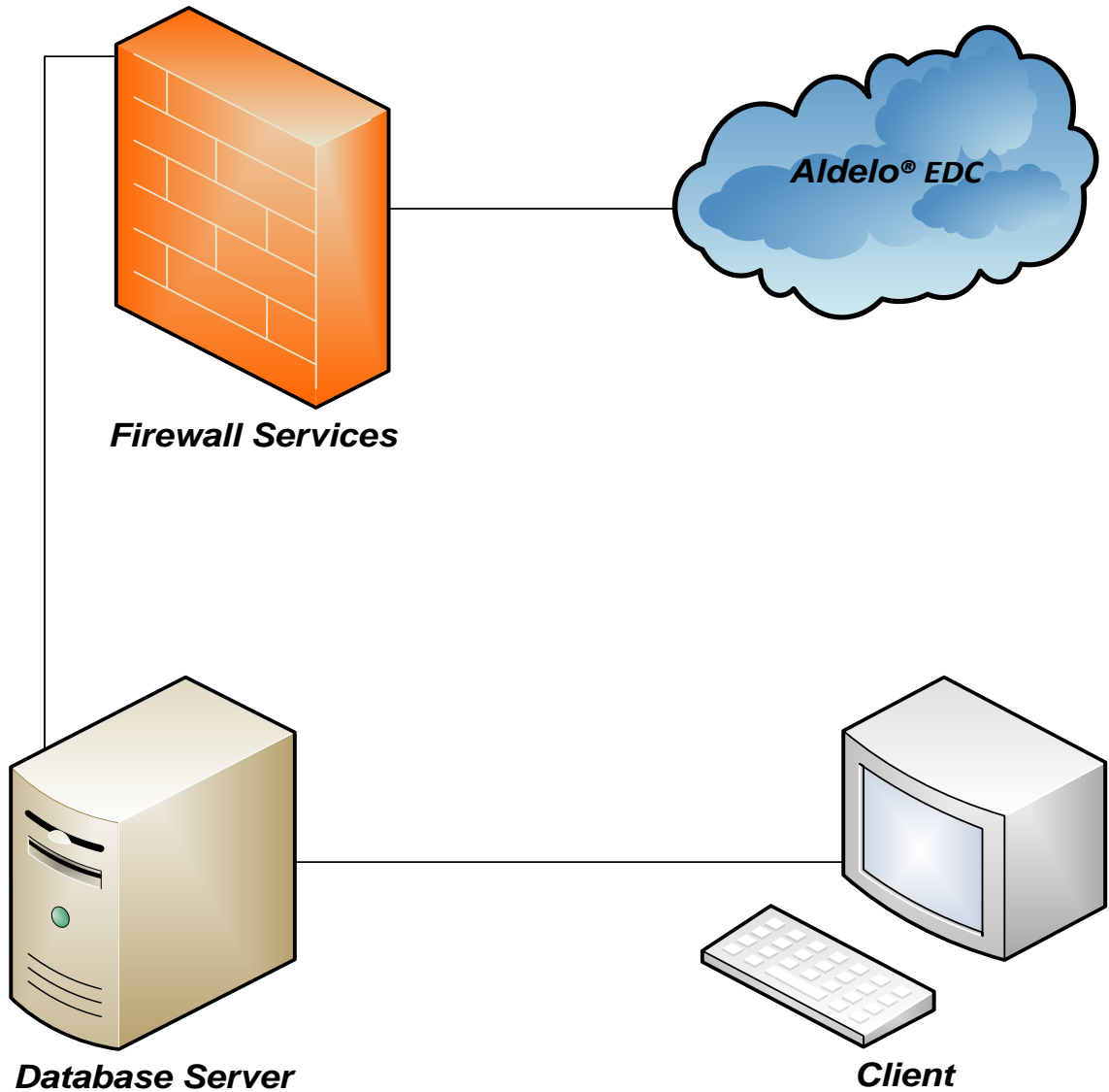
## Windows Restore Points

Please note that Windows Restore Points must be disabled. Restore points may be disabled by following the instructions for your operating system as follows:

- Windows 7 – <http://windows.microsoft.com/en-us/windows7/turn-system-restore-on-or-off>
- POS Ready 7 – <http://support.microsoft.com/kb/310405>
- Windows 10 – Windows Restore Points are disabled by default in Windows 10.
- Windows Server 2014 – The Windows Restore Points feature is not available in Windows Server 2014 and therefore does not have to be disabled.

A simplified high-level diagram of an expected network configuration for a web based payment application environment is included:

## Data Flow Diagram



## Information Security Policy / Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI-DSS in full and perform a security gap analysis to identify any gaps between existing practices in your organization and those outlined by the PCI-DSS requirements
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls or increasing the logging and archiving procedures associated with transaction data
- Create an action plan for on-going compliance and assessment
- Implement, monitor, and maintain the action plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI-DSS Self Assessment Questionnaire. The questionnaire is available at the following Internet address: [https://www.pcisecuritystandards.org/merchants/self\\_assessment\\_form.php](https://www.pcisecuritystandards.org/merchants/self_assessment_form.php)
- Call in outside experts as needed. The PCI Council has published a Qualified Security Assessor List of companies that can conduct on-site PCI-DSS compliance audits for Level 1 Merchants, and Level 1 and Level 2 Service Providers. The PCI Council has also published a list of PCI-approved scanning vendors. This list is available at the following Internet address: [https://www.pcisecuritystandards.org/approved\\_companies\\_providers/approved\\_scanning\\_vendors.php](https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php)





# Chapter 3:

# XERA® POS Configuration

## Baseline System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI-DSS compliance:

- Windows POSReady 7
- Windows 7 Professional
- Windows 10
- Windows Server 2014
- All latest updates and hot-fixes should be tested and applied
- CPU 2GHz
- 2GB of RAM minimum
- 2 GB of available hard-disk space
- TCP/IP network connectivity
- A firewall, configured and installed
- An active anti-virus program installed and updated

## Application Configuration

XERA® POS requires certain Windows Operating System features to be installed prior to deploying. There are some prerequisites that must be met before XERA® POS may be installed on a system.

The following list describes the hierarchical order of deployment:

- **Step 1:** Ensure that the system to which XERA® POS will be deployed meets the Baseline System Configuration requirements
- **Step 2:** Install XERA® POS based on intended deployment strategy (Server or Client)

The following sections describe key concepts for deployment to a system running Windows 7 Professional. Installation in Windows POSReady 7, Windows 10, and Windows Server 2014 should be comparable.

## Installing XERA® POS

When the above considerations have been met, you are ready to install and setup XERA® POS. The first action is to install XERA® POS onto the system that will be hosting the application. Install this application just like you would any other program. For instructions on installing the XERA® POS software, please see the section

titled “Installation of XERA® POS” in the Software Setup Chapter of the XERA® POS Manager Manual. Once installed, the software may be configured.

## Application Requirements

The XERA® POS application may operate on the following Microsoft Windows operating systems:

- Windows POSReady 7
- Windows 7 Professional
- Windows 10
- Windows Server 2014

The XERA® POS application requires the following ports and services to function:

- TLS 1.2 over 443/TCP outbound to the processor
- For internal communication, the port number is dynamically selected, using the lowest port number available.

The XERA® POS application supports the following POI devices for MSR card and Chip acceptance:

- All pinpad devices are semi-integrated systems and are supported by your acquirer’s bank.

# Chapter 4:

## Updates and References

### Updates to XERA® POS

Updates to XERA® POS are made available from time to time and should be installed immediately if the update addresses a security issue. Aldelo, LP will have security related issues resolved within 10 business days of the development department confirming such issues. Updates will be posted to the <https://downloads.aldelo.com/Default.aspx> website upon release and may be downloaded at any time with the proper credentials for the website. To obtain the proper credentials, contact your Aldelo authorized reseller. All downloaded files are digitally signed for your protection. The user must maintain system updates, patches, and security perimeter configurations in compliance with PCI-DSS requirements.

### Technical Support

Aldelo Technical Support is available 24/7 to assist customers with software related questions and provides remote support for advanced troubleshooting using LogMeIn Rescue. LogMeIn Rescue requires fully attended operations by the end user and does not allow for unattended support operations.

During application and support processes, the following criteria must be adhered to by you, the customer, and our resellers/integrators regarding to the collection of sensitive authentication data:

- Sensitive authentication data (pre-authorization.) must only be collected when needed to solve a specific problem.
- Such data must be stored only in specific, known locations with limited access
- Collect only the minimum amount of such data that is needed to solve the specific issue
- Sensitive authentication data must be encrypted while stored
- Such data must be securely deleted immediately after use

Note: Aldelo support staff will never ask for nor collect sensitive authentication data for troubleshooting purposes.

### More Information

A copy of the Payment Card Industry Data Security Standard (PCI-DSS) from the PCI Council's security website is available at the following Internet address:

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml).

A listing of qualified security assessors from the PCI Council is available at the following Internet address:  
[https://www.pcisecuritystandards.org/approved\\_companies\\_providers/payment\\_application\\_qsas.php](https://www.pcisecuritystandards.org/approved_companies_providers/payment_application_qsas.php).

For information on Security Best Practices when installing Internet Information Services, please refer to the Microsoft website:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.mspx?mfr=true>.


## **Application Versioning Methodology**

The application versioning methodology for XERA<sup>®</sup> POS is as follows: MAJOR.MINOR.BUILD

- A change in the first portion of the version number indicates a major change to the software
- A change in the second portion of the version number indicates a minor change to the software that may include security changes that affect PA-DSS
- A change in the third portion of the version number represents the internal build that does not include security changes that affect PA-DSS
- Wildcard elements are never used to represent security-impacting changes to the software

# Chapter 5:

## PA-DSS v 3.2 Requirements

| PA-DSS v 3.2 Requirement  | Requirement Fulfillment  |
|---|--|
| <p><b>1.1.4</b> Securely delete any magnetic stripe data, card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.</p>  | <p>Magnetic stripe data is never stored within XERA<sup>®</sup> POS. Previous versions of the XERA<sup>®</sup> POS application did not and could not be configured to store sensitive authentication data; therefore, a tool for removal of such data is not provided.</p>   |
| <p><b>1.1.5</b> Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other sources received from customers, to ensure that magnetic stripe data card verification codes or values, and PINS or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.</p> | <p>Sensitive data is never stored within XERA<sup>®</sup> POS. Aldelo agents will never collect sensitive data from customers for troubleshooting or debugging purposes.</p>   |
| <p><b>4.1</b> At the completion of the installation process, the “out of the box” default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users.</p>   | <p>All activities of all users are logged to the audit trail within Aldelo<sup>®</sup> EDC.</p>  |
| <p><b>4.4</b> Payment application must facilitate centralized logging.</p>  | <p>All activities of all users are logged to the audit trail within Aldelo<sup>®</sup> EDC. To export this log file, from the main screen of Aldelo<sup>®</sup> EDC, navigate to File Tab\Import &amp; Export to display the Import &amp; Export screen. Choose the data and settings you wish to export from the Select Transform Options group box (making sure Audit Logs is selected), and click the navigation button . Navigate to your desired location for the export file, create a name for the file, and click the “Open” button to return to the Import &amp; Export screen. Click the “Export” button to complete the creation and exportation of the file. For a detailed explanation of this procedure, see the chapter titled Administrative Tasks in the Aldelo<sup>®</sup> EDC User Manual.</p> |

| PA-DSS v 3.2 Requirement  | Requirement Fulfillment   |
|---|---|
| <p><b>10.3.1</b> If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes.</p> | <p>Payment application updates are not automatically sent to customers. Customers must obtain these from Aldelo's secure website.</p> |

