PCI Compliance Training

Updated July 2019

This document is intended for Unitec Authorized Distributors

PCI Standards

PCI Standards

The PCI Security Standards Council (SSC) has issued (2) applicable standards:

- Data Security Standard (PCI-DSS) - Defines requirements for merchant's environment
- Payment Application Data Security Standard (PCI-PA-DSS)

These standards are available from PCI at www.pcisecuritystandards.org

Compliance Requirements

Merchant Requirements

- Determined by the card brands (Visa, AMEX etc.)
- May require quarterly network scans and audits depending on transaction volume. Merchants should contact their acquirer for guidance.
- Merchants are also required to use payment applications that comply with the requirements of the PA-DSS

Unitec Product Compliance

Wash Select II® & Enterlink®

- Use PA-DSS Validated (as compliant) payment application devices (from Datacap Systems, Chalfont PA)
- Dial Tran SL for dial credit processing or IP Tran for Internet processing

Portal ®, WashPay ®, Sentinel ® and C-Start ®

- Use Sierra as the payment application software
- Sierra has been PA-DSS validated by a Qualified Security Assessor (QSA)

Revision History

Date	Description of Changes
3-Nov-2010	Initial release (software version 1.24)
10-Apr-2012	Add recommendation for deleting hot file records in Sierra version 1.43 (under DSS Requirement 2.1)
10-Jun-2013	Major changes for Sierra version 1.63 and for compliance with PA-DSS version 2.0
18-Sep-2014	Operating system changes for Sierra version 1.73 (for compliance with PA-DSS version 2.0)
1-Jul-2017	Review and update for Sierra 1.76 under PA-DSS Version 3.2

Reseller (Unitec Distributor) Responsibilities

Reseller Roles and Responsibilities Under the PA-DSS

- Implement a PA-DSS-compliant payment application into a PCI DSS-compliant environment (or instruct the merchant to do so)
- Configure the payment application (where configuration options are provided) according to the PA-DSS Implementation Guide
- Configure the payment application (or instructing the merchant to do so) in a PCI DSS-compliant manner
- Service the payment applications (for example, troubleshooting, delivering updates, and providing remote support) according to the PA-DSS Implementation Guide and PCI DSS

Implementation Documentation

PA-DSS Implementation Guide

- Provides instructions to resellers (Unitec distributors) and customers for properly installing, configuring and using payment software applications
- Is shipped with Unitec products and is also available for download from the Unitec website at www.startwithunitec.com/PCI-Compliance

Implementation Requirements

The following slides outline the PA-DSS requirements that are covered in the Implementation Guide. The number after each (e.g. 1.1.4) identifies the specific requirement of the PA-DSS. Related requirements for implementing Sierra products are highlighted in green.

The information provided is an overview. Resellers and customers are to refer to the Implementation Guide for specific instructions.

Delete Historic Data (1.1.4)

- Customers and resellers must delete sensitive authentication data that was stored by previous versions of the payment application.
- No actions are required when using Sierra versions later than 1.12. Deployments with version 1.12 must be updated following the procedures described in the PA-DSS Implementation Guide.

Delete Cardholder Data Used for Troubleshooting (1.1.5)

- Customers and resellers are to follow procedures described in the Implementation Guide when troubleshooting customer problems. Sensitive data collected for troubleshooting must be kept to a minimum, protected while stored and securely deleted in accordance with the requirements described in the Implementation Guide.
- Sierra does not accommodate storage of cardholder data, so requirements related to the storage and deletion of such data are inapplicable. Customers and resellers however should follow the instructions in the guide when gathering data for troubleshooting customer problems.

Purge Cardholder Data (2.1)

- Customers and resellers must purge cardholder data after it exceeds the customer's defined retention period, according to the customer's data retention policy (as described in PCI-DSS requirement 3.1).
- No actions are required to comply with this requirements as Sierra only stores elements of cardholder data as allowed by the PCI DSS. It should be noted however that Sierra version 1.34 added a “Hot File” feature to block use of previously denied cards in self serve equipment. While this file only stores data allowed by PCI-DSS, file records should be deleted when no longer needed by the business. Instructions for deleting records are provided in the Sierra Manual.

Protect Cryptographic Keys (2.5)

- Customers and resellers must store keys to secure cardholder data in the fewest possible locations and restrict access to keys to the fewest possible custodians.
- No actions are required to comply with this requirements as Sierra only stores elements of cardholder data as allowed by the PCI-DSS and does not require the use of cryptographic keys.

Implement Key Management Processes (2.6)

- Customers and resellers must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.
- No actions are required to comply with this requirements as Sierra only stores elements of cardholder data as allowed by the PCI DSS and does not require the use of cryptographic keys.

Delete Cryptographic Material (2.7)

- Customers and resellers must delete any historic cryptographic material stored by previous version of the payment application.
- No actions are required when using Sierra versions later than 1.12. Version 1.12 did use encryption materials and deployments with this version should be updated following the procedures described in the PA-DSS Implementation Guide.

Secure User Access to Payment Application (3.1)

- Customers and resellers must establish and maintain unique user IDs and secure authentication for administrative access and access to cardholder data. Secure authentication requirements are defined in PCI-DSS requirements 8.5.8 through 8.5.15.
- Sierra includes several factory default accounts and password. The default password must be changed, or the default account deleted during product installation. Furthermore, all users are to be provided with unique User IDs and passwords.

Secure User Access to PCs and Databases (3.2)

- Customers and resellers must establish and maintain unique user IDs and secure authentication for access to PCs, servers or databases with payment applications and/or cardholder data.
- No actions are required to comply with this requirement as Sierra dose not store cardholder data or allow for any user access to the database. It should also be noted that Sierra can only operate on proprietary, Unitec supplied hardware and can not be installed to operate on a PC.

Implement Automated Audit Trails (4.1)

- Customers and resellers must establish and maintain PCI-DSS-compliant logs per the PA-DSS Requirements 4.2, 4.3 and 4.4.
- Sierra includes a PCI compliant logging function which is enabled and properly configured by default and can not be disabled or modified.

Facilitate Centralized Logging (4.4)

- Customers and resellers must establish and maintain centralized logging.
- To facilitate centralized logging, log files can be exported and saved as a .CSV file.

Use Necessary and Secure Services Only (5.4)

- Customers and resellers shall use the documented list from the Implementation Guide to ensure only necessary and secure protocols, services, etc., are used on the system.
- The implementation guide provides a list of services used by Sierra. It should be noted that Sierra does not provide access for a user to view active services or to enable or disable services.

Securely Implement Wireless Technology (6.1)

- When wireless communications are implemented into the payment environment, customers and resellers must change vendor defaults per PA-DSS Requirement 6.1 and install a firewall (per PCI DSS Requirement 2.1.1).
- Unitec does not supply any wireless communications devices or support their use with their products. Customers that incorporate wireless components are solely responsible for their implementation and must comply with the requirements described in Sierra's PA-DSS Implementation Guide.

Secure Wireless Transmissions (6.2)

- When a payment application is implemented into a wireless environment, customers and resellers must use secure encrypted transmissions.
- Unitec does not supply any wireless communications devices or support their use with their products. Customers that incorporate wireless components are solely responsible for their implementation and must comply with the requirements described in Sierra's PA-DSS Implementation Guide.

Do Not Store Cardholder Data on Internet Accessible Servers (9.1)

- Customers and resellers must establish and maintain payment applications so that cardholder data is not stored on internet-accessible systems.
- No actions are required to comply with this requirement as Sierra does not store cardholder data or require cardholder data to be stored on a separate PC or server at any time.

Implement Two-Factor Authentication for Remote Access (10.2)

- Customers and resellers must establish and maintain two-factor authentication for remote access to the payment application.
- Remote Desktop is disabled by default but can be temporarily enabled for troubleshooting. This requires two-factor authentication consisting of an administrative password and a unique activation code (or token) available from Unitec.

Securely Deliver Remote Updates (10.3.1)

- Customers and resellers must implement controls to securely receive remote payment application updates from vendors.
- No actions are necessary to comply with this requirement as Sierra does not allow for remote software updates.

Securely Implement Remote Access Software (10.3.2)

- Customers and resellers must use remote access security features if remote access to the payment application is to be allowed.
- If Remote Desktop is to be enabled for remote access, a VPN must be used to secure the remote connection.

Secure Transmission of Card Holder Data (11.1)

- Customers and resellers must establish and maintain strong cryptography and secure protocols for transmission of cardholder data.
- Sierra's transmission of cardholder data (to the processing network) are secured through the use of TLS and/or SSL. This is a built-in feature which is not configurable and can not be disabled. No actions are required by the customer or reseller to comply with this requirement.

Secure Data Sent by Messaging Technologies (11.2)

- Customers and resellers must encrypt cardholder data that's sent over end user messaging technologies (text message, e-mail).
- No actions are required to comply with this requirement as Sierra does not provide capabilities for sending cardholder data through end-user messaging technologies. Customers should be advised against manually recording cardholder data and transmitting this data in a text message, e-mail or any other form of communication.

Non-Console Administrative Access and Multi-Factor Authentication (12.2)

- Use multi-factor authentication for all personnel with non-console (across LAN/WAN) administrative access.
- Unitec utilizes an Internet-based SMS user authentication mechanism for non-console (remote) access to the web interface. This requires outbound Internet access be available from the Sierra host system, and users have the ability to receive a standard text message, containing a one-time use, expiring access code.