

PCI Compliance Training

PCI Training Topics

- Applicable PCI Standards
- Compliance Requirements
- Compliance of Unitec products
- Requirements for compliant installation and use of products

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-PADSS)
 - Defines requirements for payment application software
- These standards are available from PCI at:
<https://www.pcisecuritystandards.org>

Compliance Requirements

Requirements for Merchant compliance:

- Determined by the card brands (Visa, Mastercard etc..)
- Vary depending on Merchant size (# of transactions/yr)
 - Most car wash operators are tier 4 merchants (<1,000,000 transactions/yr). Compliance actions for tier 4 merchants are left to the discretion of the merchant's (acquiring) bank and may include:
 - Annual Self-Assessment Questionnaire (SAQ) - A form the merchant completes to confirm their operation complies with PCI-DSS requirements
 - Quarterly network scan - A 3rd party software tool is used to scan the merchant's computer network and identify any security risks
- **Merchants are also required to use payment applications that comply with the requirements of the PA-DSS**

Unitec Product Compliance

- WashSelect II & Enterlink:
 - ◆ Use compliant (and validated) payment application devices (from Datacap Systems, Chalfont PA)
 - Datatran SL for dial credit processing or,
 - IP Tran for Internet processing
- Portal, Washpay and Sentinel
 - ◆ Use “Sierra” software as a common application
 - ◆ Sierra was validated as compliant with the PA-DSS by a Qualified Security Assessor (QSA)

PADSS Compliance

- PADSS Requirements affect Merchants (end users), resellers (Unitec distributors) and Software Vendors (Unitec)
- The roles and responsibilities for each of these parties as defined in the PADSS are listed on the following pages.

PADSS Roles & Responsibilities

- Vendor (Unitec) Responsibilities:
 - ◆ Create payment applications that comply with the PCI -PADSS and that facilitate and do not prevent their customers' PCI DSS compliance.
 - ◆ Follow PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data
 - ◆ Create a PA-DSS Implementation Guide, specific to each payment application, according to the requirements defined in the PADSS;

PADSS Roles & Responsibilities

■ Vendor Responsibilities (Cont):

- ◆ Ensure payment applications meet PA-DSS by successfully passing a PA-DSS review.
- ◆ Educate customers and resellers on how to install and configure the payment applications in a PCI DSS-compliant manner.
 - ◆ Customer and reseller education is provided through the content of this presentation

PADSS Roles & Responsibilities

- Reseller (UE Distributor) responsibilities:
 - ◆ 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 remote updates, and providing remote support) according to the *PA-DSS Implementation Guide* and PCI DSS

PADSS Roles & Responsibilities

■ Merchant (Customer) Responsibilities:

- ◆ Implement a PA-DSS-compliant payment application into a PCI DSS-compliant environment;
- ◆ Configure the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor;
- ◆ Configure the payment application in a PCI DSS-compliant manner;
- ◆ Maintain the PCI DSS-compliant status for both the environment and the payment application configuration

Implementation Requirements

- PADSS Implementation Guide:

- ◆ Provides instructions to resellers (UE distributors) and customers for properly installing, configuring and using payment software applications
- ◆ Is shipped with Unitec products and available for download from the distributor section of Unitec's WEB site at:

<http://www.unitecelectronics.com/>

Implementation Requirements

The following slides list the PADSS requirements that are covered in the Implementation guide. The associated actions for implementing Sierra products are highlighted in **yellow**.

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

Implementation Requirements

■ Delete Historic Data

- ◆ Customers and resellers must delete sensitive authentication data that was stored by previous versions of the payment application. Removal of such data is absolutely necessary for PCI Compliance.
- ◆ No actions are required when using Sierra version 1.24 or later. Earlier versions should be updated following the procedures described in the PADSS Implementation Guide.

Implementation Requirements

- Delete Cardholder data used for troubleshooting
 - ◆ Customers & 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.**

Implementation Requirements

- Purge Cardholder Data
 - ◆ Customers & 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.

Implementation Requirements

- Delete Cryptographic Material
 - ◆ Customers & Resellers must delete any cryptographic material or cryptograms stored by previous version of the payment application. Removal of this material is absolutely necessary for PCI DSS compliance.
 - ◆ No actions are required when using Sierra version 1.24 or higher. Earlier versions did use encryption materials and these versions should be updated following the procedures described in the PADSS Implementation Guide.

Implementation Requirements

- **Secure User Access to payment application**
 - ◆ Customers & 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.
 - ◆ **No actions are required to comply with this requirement as Sierra does not allow Administrative Access for any user and does not store cardholder data at any time. Customers should be advised however to apply unique user IDs and secure authentication to all general users to control their access to functions that may be sensitive and/or disruptive to the business.**

Implementation Requirements

- Secure user access to PCs and Databases
 - ◆ Customers & 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 does not store cardholder data or allow for any user access to the database. It should also be noted that Sierra can only operate on Unitec supplied payment terminals and can not be installed to operate on a PC or server.

Implementation Requirements

- Implement Automated Audit Trails
 - ◆ Customers & Resellers must establish and maintain PCI DSS-compliant log settings. Logs must be enabled, and disabling the logs will result in non-compliance with PCI DSS.
 - ◆ No specific actions are required as Sierra does not allow for the events that must be logged in an audit trail (e.g. access to cardholder data and administrative accounts). Customers should be aware however that Sierra does include a logging function which is useful for troubleshooting hardware problems.

Implementation Requirements

- **Securely Implement Wireless Technology**
 - ◆ When wireless communications are implemented into the payment environment, customers and resellers must install a firewall (per PCI DSS Requirements 1.2.3 and 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 PADSS Implementation Guide.**

Implementation Requirements

- **Secure Wireless Transmissions**
 - ◆ When a payment application is implemented into a wireless environment, customers and resellers must use secure encrypted transmissions (per PCI DSS Requirement 4.1.1.)
 - ◆ **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 PADSS Implementation Guide.**

Implementation Requirements

- Do not store cardholder data on Internet accessible servers
 - ◆ Customers and resellers must establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems (per PCI DSS Requirement 1.3.4.)
 - ◆ No actions are required to comply with this requirement as Sierra does not store cardholder data or require that it be stored on a separate PC or Server at any time.

Implementation Requirements

- Securely deliver remote updates
 - ◆ Customers & Resellers must implement controls to securely receive remote payment application updates from vendors (per PCI DSS Requirements 1, 1.3.9, and 12.3.9)
 - ◆ No actions are required to comply with this requirement as Sierra does not allow for remote software updates.

Implementation Requirements

- Secure remote access with two-factor authentication
 - ◆ If a payment application can be accessed remotely, customers and resellers must establish and maintain two-factor authentication for remote access in accordance with PCI DSS Requirement 8.3.
 - ◆ No actions are required to comply with this requirement as remote access to the [payment application is not supported.

Implementation Requirements

- Secure Transmission of card holder data
 - ◆ The PCI-DSS requires the use of SSL to secure cardholder data that's transmitted over public networks. Customers and resellers must establish and maintain secure transmissions of cardholder data, in accordance with PCI DSS Requirement 4.1.
 - ◆ Sierra's transmission of cardholder data (to the processing network) are secured through the use of 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.

Implementation Requirements

- Secure data sent by messaging technologies
 - ◆ Customers and Resellers must establish and maintain secure transmissions of cardholder data that's sent over end user messaging technologies (text message, e-mail) in accordance with PCI DSS Requirement 4.2
 - ◆ 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.

Implementation Requirements

- **Encrypt Non-Console Access**
 - ◆ Customers and Resellers must encrypt all non-console administrative access through the use SSH, VPN, or SSL/TLS in accordance with PCI DSS Requirement 2.3.
 - ◆ **No actions are required to comply with this requirement as Sierra does not provide any capabilities for non-console Administrative access.**