

# PA DSS Implementation Guide

Sierra Software

Version 1.24B

Nov 3, 2010

### Document Revision History

<b>Version</b>	<b>Date</b>	<b>Summary of Changes</b>
1.00	14-Apr-2009	Initial release
1.24	19-Apr-2010	Document was completely rewritten and released for software version 1.24.
1.24A	30-July-2010	Revised sections 4.3, 4.4, 4.6 and 4.7 with minor clarifications
1.24B	3-Nov-2010	Revised sections 1.0 and 4.1 through 4.11 with minor clarifications. Added new requirement (“Note: Should customers....systems”) at the end of section 4.2.

## Table of Contents

Table of Contents .....	i
1 Introduction .....	1
2 PCI Standards .....	1
3 Roles and Responsibilities .....	2
4 Payment Application Implementation.....	4
4.1 Storage of Sensitive Data .....	4
4.1.1 Delete Historical Data .....	4
4.1.2 Data Collected for Troubleshooting .....	5
4.2 Protect Stored Cardholder Data .....	6
4.3 Delete Cryptographic Material.....	7
4.4 Secure Administrative and Cardholder Data Access.....	7
4.5 PCI DSS Secure Access to PCs, Servers and Databases.....	8
4.6 Audit Trails .....	8
4.7 Wireless Networks .....	9
4.8 Secure Software Updates .....	10
4.9 Secure Remote Access.....	11
4.10 Secure Data Transmission.....	11
4.11 Non Console Administrative Access .....	12

**This page is intentionally left blank**

## 1 Introduction

This document provides guidance to Unitec distributors (or resellers) and merchants (customers that purchase Unitec products) on implementing the Sierra software application in accordance with the requirements of the PCI Data Security Standard (DSS). It identifies requirements specific to compliant payment application implementation. The Sierra PA-DSS Implementation Guide is disseminated to all Sierra resellers and customers at the time of payment application shipment and via customer portal or reseller bulletin as needed to address payment application updates. The Sierra PA-DSS Implementation Guide is further reviewed and updated on an annual basis, as needed to document major and minor changes to the payment application, and in accordance with changes to the PA-DSS requirements.

## 2 PCI Standards

The PCI Security Standards Council was founded by the major credit card brands and consists of representatives from the brands along with participants from industry. Their publications include the Data Security Standard (or PCI DSS) and the Payment Application Data Security Standard (or PCI-PA-DSS). Although these standards share common principals and requirements, they serve different purposes.

The **PCI DSS** is the standard that's applied in assessing compliance of a Merchant's credit processing environment. The core of this specification is a group of principles and (12) accompanying requirements, as listed below.

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

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

### **Protect Cardholder Data**

3. Protect cardholder data
4. Encrypt transmission of cardholder data across open, public networks

### **Maintain a Vulnerability Management Program**

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

### **Implement Strong Access Control Measures**

7. Restrict access to cardholder 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 **PCI-PA-DSS** applies to a software vendor's payment application. Its requirements were derived from the DSS and its purpose is to ensure that payment software applications facilitate – and do not prevent – a customer's compliance with the requirements of the PCI DSS.

For more detailed information on PCI standards refer to the PCI security standards council's WEB site at <https://www.pcisecuritystandards.org>.

## **3 Roles and Responsibilities**

Although the Merchant is ultimately responsible for compliance with the PCI DSS, Unitec and their distributors (or resellers) have certain responsibilities towards ensuring the payment application implementation facilitates the merchant's compliance. The responsibilities of each party are summarized below.

### **Software Vendor (Unitec) Responsibilities**

- Create payment applications that comply with the PCI Payment Application Data Security Standard (or PA-DSS) and that facilitate and do not prevent their customers' PCI DSS compliance. (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement.);
- Follow PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting);
- Create a PA-DSS Implementation Guide, specific to each payment application, according to the requirements defined in the PA-DSS;
- Educate customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS-compliant manner;
- Ensure payment applications meet PA-DSS by successfully passing a PA-DSS review

### **Reseller (Unitec 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* provided by the vendor;

- 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

**Customer (Merchant) 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

## 4 Payment Application Implementation

While the use of a validated payment application facilitates a merchant's compliance with the PCI DSS, their compliance relies in part on proper implementation of the application. Payment applications contain certain security features, which could cause non-compliance with the PCI DSS if configured or used incorrectly.

This section lists the requirements of the PA-DSS that apply to the implementation of a payment application. Included is an explanation of how Sierra facilitates compliance with each along with instruction for any related actions that customers and resellers must take to securely implement Sierra.

### 4.1 Storage of Sensitive Data

The PA-DSS prohibits the storage of sensitive data after authorization of a transaction. Examples of sensitive data include full contents of magnetic stripe tracks, card validation codes and customer PINs. The Sierra application does not store sensitive cardholder data.

#### 4.1.1 Delete Historical Data

Customers and resellers are required to delete historical data and data that is used for troubleshooting purposes to ensure compliance with PCI DSS. Customers and resellers must remove cardholder data stored by previous versions of the payment application. The removal process should include the use of a secure wipe tool provided by the vendor and used in accordance with the instructions provided in the *PA-DSS Implementation Guide*. Removal of this data is absolutely necessary for PCI Compliance.

*Sierra retains only cardholder data elements that are allowed per the PCI DSS. It should be noted however that versions prior to 1.24 did store full track 2 contents – in encrypted form – prior to authorization. This data was deleted from the database upon authorization but there are no tools available to securely wipe trace data from the storage device (the D-Drive flash card). To comply with this requirement, Sierra installations with versions prior to 1.24 should be updated as follows:*

1. *Acquire a software upgrade utility and new D-Drive from Unitec.*
2. *Apply the software upgrade in accordance with the instructions provided with the upgrade utility.*
3. *Save a database back up onto a thumbdrive by following the procedures described in the Operator's Manual.*
4. *Install the new D-drive that contains the compliant version of Sierra. Use the restore function to copy the database from the thumbdrive onto the new D-*

*Drive. Use of the restore function does not transfer either historic or cryptographic material including track data.*

*The replaced D Drive may house sensitive data and must be securely destroyed. Unitec uses a 3<sup>rd</sup> party service to handle the destruction of these drives. Upon completion of the update process described above, any replaced D Drive older than version 1.24 must be returned to Unitec Customer Service through a secure courier (e.g. Fed-ex, UPS) so it can be destroyed. Unitec ensures the secure handling and destruction of all received D Drives through contract with a media destruction service who incinerates the drives in a secured environment and provides Certificates of Destruction which are archived at Unitec.*

#### 4.1.2 Data Collected for Troubleshooting

Any data that's collected for troubleshooting purpose must be:

- Collected only when needed to solve a specific problem.
- Collected only in a limited amount as needed to solve a specific problem
- Stored only in specific, known locations with limited access
- Encrypted while stored and,
- Securely deleted immediately after use

Customers and resellers are to troubleshoot customer problems in accordance with the procedures described in the payment application vendor's PA-DSS Implementation Guide.

*Sierra does not allow for storage of any sensitive data for troubleshooting or any other purposes.*

*When troubleshooting customer problems, Unitec personnel will only request certain data elements that are allowed by the PCI- DSS. The data may vary by the nature of the problem but will always be limited to:*

- *Credit Card Type/Brand (Visa, AMEX, etc..),*
- *1<sup>st</sup> (4) digits of the Primary Account Number (or PAN),*
- *Last (4) digits of the PAN and,*
- *Card expiration date.*

*Merchants and resellers should ensure their personnel never manually record cardholder data beyond the elements listed above when troubleshooting a customer's problem.*

## 4.2 Protect Stored Cardholder Data

In accordance with PCI DSS requirement 3.1 customers must develop data retention policies to limit the amount of time cardholder data is stored. This data is to be purged in accordance with the instructions provided in the vendor's PA-DSS Implementation Guide after the customer's defined retention period is reached.

*Sierra does not store any cardholder data that is not allowed per PCI DSS. As data cannot be stored, procedures for purging stored data are non-applicable.*

*A transaction is initiated when a sales request is received from the client terminal. The sales request identifies the product(s) being purchased and the payment types and amounts being applied. When a credit card is one of the payment types, track 1 and 2 data will be included in the request (from the client). Sierra parses the track data and extracts the account number (PAN). The account number prefix is compared against 'acceptable' types which include, Visa, MC, Disc, AMEX, local account cards for the site (non-credit) and, gift cards that are accepted by the processor (Mercury Payment Systems). If the account prefix does not match any of these types, the sales request is rejected. If the account prefix matches one of the aforementioned credit cards, Sierra will create a transaction object which includes the full contents of track 2 which is required by the credit processor. The transaction object is held in dynamic memory until authorization is received from the processing network. A transaction record is added to the database and it includes the card type (or brand), expiration date, and last 4 digits of the account number that was extracted from Track 2.*

*Upon receipt of authorization from the network, the characters of track 2 data in memory are replaced with zeros and the transaction object is discarded (releasing the memory space). If the transaction is declined (by the processor), no response is received, or the transaction is cancelled the transaction object is discarded as described previously.*

Requirement 9.1 of the PA-DSS requires cardholder data to not be stored on Internet-accessible systems (for example, web server and database server must not be on same server). The customer and reseller must implement payment applications so that cardholder data is not stored on Internet-accessible systems in accordance with DSS Requirement 1.3.

*Sierra does not store cardholder data or require that it be stored on a local computer server. Consequently, requirements related to the storage of cardholder data on internet-accessible systems are non-applicable. Further, Sierra facilitates a single transaction at a time and solely retains a truncated value inclusive of the last 4 digits of the PAN in addition to the expiration date*

*Note: Should customers or resellers choose to store cardholder data, cardholder data must at no time be stored on internet-accessible systems.*

### **4.3 Delete Cryptographic Material**

As cardholder data must be encrypted when stored, a payment application may contain cryptographic material or cryptograms. Cryptographic materials stored by previous versions of the payment application must be deleted in accordance with the instructions provided in the vendor's PA-DSS Implementation Guide. The PA-DSS Implementation guide must also provide instructions for re-encrypting historic data with new encryption keys. Removal of such cryptographic material is absolutely necessary for compliance with the PCI DSS.

*As Sierra version 1.24 does not store cardholder data, encryption and the associated cryptographic materials are not used. No actions are required by the customer or reseller to comply with this requirement when using version 1.24 or later.*

*However, Sierra versions prior to 1.24 did include encryption for storage of cardholder data pre-authorization. As there are no tools available for removing cryptographic materials, customers using versions older than 1.24 should upgrade their products following the procedure described in section 4.1.1.*

### **4.4 Secure Administrative and Cardholder Data Access**

The 'out of the box' installation of a payment application must facilitate use of unique user IDs and PCI DSS compliant authentication for all administrative access and for all access to cardholder data. More specifically:

- Assign a unique ID for access to system components or cardholder data

*Sierra does not provide user account access to system components or cardholder data. Sierra facilitates a single transaction at one time and neither provides access to cardholder data nor administrative access. Nevertheless, Unitec Electronics strongly advises that customer's employ unique IDs, not use default accounts, and ensure PCI DSS compliant authentication for all administrative access and for all access to any cardholder data which may be otherwise retained within customer cardholder data environments.*

- Do not use default administrative accounts for payment application logins.

*Sierra does not provide default administrative accounts for a user log-in. Sierra is factory installed onto Unitec proprietary hardware terminals and designed to automatically run upon equipment start-up. Sierra neither provides a user with*

*access to create an administrative account nor the ability to access administrative capabilities inclusive of direct database access. Additionally, Sierra facilitates a single transaction at a time and solely retains a truncated value inclusive of the last 4 digits of the PAN in addition to the expiration date.*

- Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts

*Sierra does not provide default administrative accounts.*

- Use secure authentication for the payment application and system whenever possible.

Sierra does not provide default administrative accounts nor does it provide for user access to cardholder data.

#### **4.5 PCI DSS Secure Access to PCs, Servers and Databases**

PA-DSS requires the use of unique user names and secure authentication to control access any PCs, servers, and databases with payment applications and/or cardholder data. Requirements for Secure Authentication are defined in PCI DSS Requirements 8.5.8 through 8.5.15 (and also listed in section 4.4 of this document).

*Sierra is factory installed on Unitec proprietary payment terminals. It can only operate on these terminals and as such, cannot be installed on a PC or Server in the customer's environment. Further, Sierra also does not store cardholder data or allow for any user access to the application's database.*

#### **4.6 Audit Trails**

PCI DSS requires that the merchant track and monitor all access to network resources and cardholder data. This includes the use of audit trails (or logs) that record actions of all users to the payment application or with access to cardholder data. While the customer is responsible for implementing audit trails, payment applications must accommodate the customer's use of PCI compliant logs. Logs must be enabled and disabling logs will result in a non-compliance with PCI DSS. The events to be logged in the audit trail are defined in PCI DSS requirement 10.2

*Sierra includes a logging function that is automatically enabled and cannot be disabled by the user. The logging function is intended to capture hardware events that may be helpful in troubleshooting equipment problems. Sierra facilitates a single transaction at a time and solely retains a truncated value inclusive of the last 4 digits of the PAN in addition to the expiration date.*

*The events to be logged (per PCI DSS Requirement 10.2) are listed below along with an explanation of Sierra's compliance with each.*

- *Individual access to cardholder data – The Sierra application does not store non-truncated cardholder data. However, all individual application access is logged.*
- *All actions taken by a user with root or administrative privileges – The Sierra application does not allow a user to access root or administrative functions. However, all system-level administrative privilege use is logged.*
- *Access to audit trails – Sierra event logging access is audited.*
- *Invalid logical access attempts – Unsuccessful log-in attempts are audited.*
- *Use of identification and authentication mechanisms – A valid user ID and password is required to access the event log..*
- *Initialization of audit logs – Log files are initialized upon equipment start up. All start-up events including the initialization of audit logs are logged.*
- *Creation and deletion of system level objects – Though the use of administrative privileges is not provided to Sierra users, the creation and deletion of system level objects is audited as a default system function.*

## **4.7 Wireless Networks**

*Unitec products do not include wireless components or support the use of wireless technology. Customers that elect to acquire and utilize wireless technology are solely responsible for ensuring that they are implemented in accordance with the following requirements:*

When wireless devices are used within the payment environment, perimeter firewalls must be installed between the wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment (Ref PCI DSS requirement 1.2.3).

For wireless environments connected to the cardholder data environment or transmitting cardholder data, wireless vendor defaults must be changed, including but not limited to, default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission (ref PCI DSS requirement 2.1.1).

Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission (Ref PCI DSS requirement 4.1.1).

**Note:** *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*

## **4.8 Secure Software Updates**

All system components and software have the latest vendor-supplied security patches installed. Furthermore, critical security patches must be installed within one month of release (per PCI-DSS requirement 6.1).

*Unitec Electronics subscribes to alert services that provide prompt notification on the release of any Operating System patches or upgrades that address potential vulnerabilities. Unitec Electronics will test the payment application for applicable vulnerabilities and promptly develop appropriate patches to address affected software. Unitec Electronics will further notify their equipment distributors and Merchants upon releases. The release notification identifies updates that include security patches and will highlight those that address a critical issue requiring prompt attention. Software updates are deployed through authorized Unitec Electronics equipment distributors.*

*Unitec Electronics advises merchants to ensure their systems have the latest security updates in their payment applications and requires that critical security updates be installed within 30 days of their release. When notified of software releases that address security issues, the merchant should contact their equipment distributor to arrange for in-person update of their system so as to ensure a known chain-of-trust..*

*As required by the PA-DSS the Sierra upgrade program includes a mechanism to validate authenticity of the files that are being applied. The purpose for this validation is to prevent unauthorized files from being applied to the Sierra application. A description of this mechanism follows:*

*The update program calculates a SHA 512-bit hash of all binaries included in the update package before the installation actually occurs. If the hash matches the "key" value stored in a separate (ie, not part of the hash calculation) file, then the update is allowed to proceed. If the hash does not match, the update program will terminate and an error message ("Software Verification Failed") will be displayed to the operator.*

*The fact that the key value is accessible/visible is not an issue because the hash is also "salted" so that the key value cannot be recreated given the contents of all files in the update. The salt value is a large random number that is included in all hash calculations. An individual would need to know this number plus where it is inserted into the*

*calculation plus how many times it is used in the calculation in order to compromise the security.*

Remote updates to payment application software must be delivered in a secure manner. Remote access technologies should be activated only when needed for downloads from the vendor and deactivated immediately after the download completes (per DSS requirement 12.3.9). Alternatively, if updates are delivered via VPN or other high-speed connection, a firewall or a personal firewall product should be configured to secure “always-on” connections (per DSS requirement 1).

*Sierra does not provide remote access to system administrative functions (whether from on-site or through a remote connection) and must be performed on site.*

#### **4.9 Secure Remote Access**

The PCI DSS requires the use of two-factor authentication (user ID and password and an additional authentication item such as a token) for remote access to the network by employees, administrators, and third parties. Remote access to a payment application should also be secured by use of two-factor authentication in accordance with PCI DSS requirement 8.3.

When remote access software is used to remotely access the payment application or payment environment, its security features must be used. This requirement applies to all users of the remote access software including (but not limited to) the payment application vendor, reseller and customer.

*Sierra does not support remote access to administrative functions or to retained cardholder data. Furthermore, neither Sierra nor the Unitec terminals on which the application runs allow for remote access through any 3<sup>rd</sup> party remote access software products.*

#### **4.10 Secure Data Transmission**

*Sierra uses a 3rd party (software) product for processing credit card sales. The product is a PCI validated application that employs strong SSL-based encryption and secure protocols to ensure the security of cardholder data communications. Sierra will only transmit cardholder data when authorizing a credit card sale.*

Sierra further does not support the use of end user messaging technology for transmitting cardholder data. If customers elect to manually collect and transmit cardholder data through such methods, , all cardholder data must be encrypted in accordance with PCI DSS requirement 4.2.

## **4.11 Non Console Administrative Access**

PCI DSS requirement 2.3 requires non-console administrative access to the payment application or to servers in the cardholder data environment to be encrypted with SSH, VPN or SSL/TLS.

Sierra does not support or facilitate non-console administrative access.