CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

QuickSale mPOS
Version 2.2.*.*

Secure Payment Solution
Client Implementation Guide
2.0

Last Revision: 02/27/2020

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

Revision #	Date	Name	Description
1	11/08/07	CP	Added sections 13 and 14
2	11/12/07	CP	Updated section 12 to include recommendations for browser security.
3	11/15/07	CP	Reviewed all sections
4	11/20/07	CP	Updated section 12 and added section 15
5	11/30/07	CP	Updated section 12 to include Storage card information
6	1/15/08	CP	Added section regarding key rotation and troubleshooting procedures
7	3/17/08	CP	Removed sections that are no longer relevant
8	5/02/08	CP	Modified the section related to WiFi configuration
9	6/04/08	CP	Added wording regarding upgrades.
10	11/24/08	CP	Updated uninstall section for J2ME device
11	3/18/09	CP	Added the User Management section
12	1/29/10	TS	Added Uninstall procedure for Blackberry and Android
13	5/11/10	AL	Added Uninstall procedure for Brew, extra requirements for PA-DSS
14	9/07/10	CP	Added uninstall procedures for iPhone
15	9/30/10	CP	Added screen lock procedures for iPhone
16	10/15/10	TS	Added User Management for QuickBooks.
17	09/30/13	TS	Review and Edit for PA-DDSS 2.0
18	11/18/13	CP	Edits for PA-DSS 2.0
19	12/31/13	CP	Additional Edits for PA-DSS 2.0
20	01/03/14	CP	Additional Edits for PA-DSS 2.0
21	4/1/14	CP	Added Customer Database Section
22	6/11/14	CP	Added Card Protection Steps for QB
23	6/12/14	CP	Accepted PA-DSS changes
24	7/12/18	JO	Updated Title Page and name change to “QuickSale mPOS”
25	2/27/20	JO	Added PIN Transactions Security and PIN Block Updated TLS 1.2, removed Blackberry

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

WARNING: If all recommendations in this guide are not followed the application will not be PA-DSS compliant.

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

1. How to Create Passwords

The following guidelines pertain to PA-DSS requirement 3.1.

When the application is first installed, the user must provide the password for the default user admin. This is the highest level user, and its session will expire after 15 minutes. It is strongly recommended that a low level user is immediately created. If a function requires admin level, the low level user should see his manager for a password override, if applicable. Passwords expire every **90** days and the user is required to change them.
User can not reuse any one of the last 4 passwords.

Application uses strong password policy described below.

Password Policy:
- Password has to be at least 8 alphanumeric characters
- Password must have digits
- Password must have both upper and lower case letters
- Symbols are recommended but not required

The application contains the means to recover password by integrating a security phrase that is created by the user.

Every time user restarts the device and enters the application, the application will inform the user if he is using default/expired passwords. It is the responsibly of the user to immediately change the default passwords, and to changes the expired passwords.

Please note that when you are entering the password, you will be able to see what you are entering however, when you are entering the password on any other screen, your password will be masked (you will see asterisks).

Also, when you enter a screen to change a password, you will see your password since you have just entered it, so it is no secret at this point.

A user can be given permissions from **Security/Transaction Security.** these permissions can limit his access thus reducing the risk, and when necessary, a manger override will be required.

After 3 failed password attempts, the application will lock out for 30 minutes before allowing another 3 attempts. For users with admin level permission, if application is idle for 15 minutes, the application will lock out and require password for re-entry. A user can unlock his app by using the password recovery functionality. If successful, he will be required to change his password immediately.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

3. User Management (CHARGE Anywhere for Windows)

When starting the application for the first time, you will be presented with a screen to set the password on the "Owner" account, this password should follow the guidelines of Section 1. This account is required and has access to all the functionality available within the application.

User accounts should be created by logging in with the "Owner" account or an account with the User Management privileges. The following steps should be followed to create a new user:

NOTE: If creating a user that is only going to run transactions, it is recommended to extend the Idle Timeout.

1. Sign in with an account that has the appropriate privileges
2. Right click on the CHARGE Anywhere icon in the system tray
3. Select **User Management**
4. Select **Add User**
5. Fill in the **Username**
6. Assign a **Password**
7. Assign a **Clerk Number**
8. Revise the **Idle Timeout** is required
9. Select a **Permission Template** or check the desired permissions
10. Press **Create**

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

4. User Management (QuickBooks)

QuickBooks has a built-in user called **Admin**, and QuickBooks by default does not assign it a password. However, when using CHARGE Anywhere QB Plug-in, it **required** that **Admin** user get a password in compliance to the "**Password Policy**" included in this document. Admin can subsequently create more users and give them passwords in compliance to the "**Password Policy**" included in this document.

Give Admin a Password:

1. From the "**Company"** Menu, choose **Users**
2. Choose "**Set Up Users and Roles…**"
3. **Admin** user will be highlighted. Click "**Edit**" button the right side of the window.
4. Give **Admin** user a password in compliance to the "**Password Policy**" included in this document.

Create More Users:

1. From the "**Company"** Menu, choose **Users**
2. Choose "**Set Up Users and Roles…**"
3. Click "**New**" button the right side of the window.
4. Enter Required Info and choose Roles, then click Ok. Password must be given in compliance to the "**Password Policy**" included in this document.

Enable Customer Credit Card Protection:

1. From the "**Company"** Menu, choose **"Customer Credit Card Protection…"**
2. Choose "**Enable Protection**"
3. Follow the prompts to setup the Admin password if not already configured

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

5. Secure Transmission of Data

Data must be sent using TLS version 1.1 or better using 128-bit keys to meet PA-DSS requirement 11.1. This is the default used by the application.

Please note that unencrypted card numbers should **NEVER** be sent over messaging systems like email or SMS.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

6. PIN Transaction Security ***(PCI-PIN req. 2-1)***

Merchant, clerk, and/or teller will not request or accept the PIN from the cardholder for PIN entry transactions. The Cardholder must always enter the card PIN themselves.

7. PIN Block Security ***(PCI-PIN req. 4-1)***

The QuickSale App ensures that the encrypted magnetic stripe, CVV2, and PIN block data are deleted from memory after processing and also during failed transaction transmissions.

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

Secure Access to systems with cardholder data

Use unique username and complex passwords to access machines with payment applications and/or cardholder data per PA-DSS **requirement 3.1. Also use unique usernames and PCI DSS compliant secure authentication for databases containing cardholder data.**

All devices that hold card data must be accessed with a complex password. Please follow the same guidelines as in section 1: “How to create passwords”.

Default passwords must be changed immediately upon the user’s next login.

Keep passwords secure. Authorized users are responsible for the security of their passwords and accounts. These passwords must be changed every 90 days.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

8. Secure Network Configuration for Systems with Card Holder Data

Systems that store cardholder data should **NEVER** be connected directly to the Internet. No direct inbound access to systems storing cardholder data should be allowed. There is no reason to allow inbound Internet access to any systems running CHARGE Anywhere software. There should be a firewall placed between the Internet and the cardholder data system that only allows legitimate outbound traffic through from systems to the Internet. The only outbound ports required for CHARGE Anywhere are 80 (HTTP) and 443 (HTTPS).

Remote Access

If this system is to be accessed remotely, then two-factor authentication **MUST** be used, and the connection needs to use strong encryption; a clear text protocol (e.g. telnet) should **NEVER** be used. This can be accomplished by providing each required user with a unique certificate and login/password for their account access, while using SSH as the connection medium.

In addition, the following security features should be set for remote access, if applicable:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each user).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins
- Enable account lockout after a certain number of failed login attempts
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Enable the logging function.
- Establish user passwords settings according to PCI guidelines

Non-Console Access

Non-console administrative access requires strong transport encryption. This is for local non-console administrative access using tools such as SSH, RDP, etc. Never use clear text transmission protocols such as telnet.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

9. Secure Wireless(WiFi) Setup

CISP-compliant wireless settings for deployment of a payment application in a customer environment per PA-DSS 6.1.

Wireless POS solutions are permitted to be deployed at a customer's facility. The wireless POS communicates directly with the customer's access point and data is then routed to CHARGE Anywhere's data center via the internet in a VISA/Master card approved encrypted methodology.

The following configuration steps **MUST** be used as the basis for all Wireless Access Point (WAP) system deployments:

- Change the default SSID (Service Set ID or network name)
- Change the default password for the WAP's Administrator account
- Enable MAC Address Filtering
- Limit the number of allowed connections to the minimum needed
- Disable DHCP
- Enable the highest encryption possible:
    - WPA2 with TKIP or AES (802.11g) or better
- Enable the WAP's firewall
- Disable the 'DMZ' feature
- Disable the Remote Management feature
- Disable Universal Plug 'n' Play (UPnP) feature
- Place the WAP near the center of buildings and avoid placing near exterior walls
- Change the SNMP community string or disable SNMP
- Periodically update WAP firmware

There should be a firewall configured between the wireless network and the network that contains card holder data so that only known traffic is being allowed access to the card holder data.

Under no circumstances should the encryption strength be configured to be less than 128 bits. Wireless encryption keys will be changed periodically, or whenever an administrator with knowledge of the keys is terminated.

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

10. Application of Security Updates

All CHARGE Anywhere customers, Resellers, System integrators must apply security updates to their systems as available. In the event that there is a security related update that is required of the application an email will be sent to the effected parties. There will also be an announcement posted on the main site.

The communications will contain instructions on what actions need to be taken to update the effected pieces of software.

If the application was downloaded from the application store, the user will receive a notification that there is an update that he needs to install. If he configured the device for automatic update, then the application will be automatically downloaded and updated.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

11. Key Maintenance

There are no physical keys for these app, all keys are dynamic. Generation and destruction is a function of the application. The user has the ability to rotate the keys at will.
It is required that the merchant perform a key rotation from the maintenance menu at the end of the defined cryptoperiod for the key. The recommendation is that the key rotation be performed every two years (or more frequently) or any time a compromise is suspected. The steps required to rotate keys follows:

- Launch the application
- Enter the required password
- Select Maintenance from the Main Screen
- Enter the required password
- Select Rotate KEK
- Select Rotate Keys

12. Suggested Key Rotation Period

Keys should be rotated periodically. CHARGE Anywhere suggests the following cryptoperiod for encryption keys.

Key	Rotation Schedule
Key Encryption Key(KEK)	Every 2 years
Data Encryption Key(DEK)	Every 2 years

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

13. Compromised Key Procedures

In the event that the merchant suspects or knows that their key has been compromised, a key rotation must be performed immediately to prevent the disclosure of sensitive data. To rotate the keys, follow the steps that are detailed in the section labeled Key Maintenance.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

14. Implementing Mobile Phone Security

Instruct customers on how to harden a mobile phone being used as a credit card processing device. The instructions should also include instructions/information pertaining to external devices, such as a Bluetooth card reader.

Sleep Settings:
It is required that the sleep timer on the mobile phone be set to no longer than 15 minutes.

Android:

NOTE: The application will NOT launch from the Storage card.

It is advised that all customers follow these procedures to harden their mobile device to prevent unauthorized access. The following steps should be taken:

1. Go to Start Menu →Settings →Connections Tab
2. Tap Bluetooth
3. Check the box labeled "Turn on Bluetooth"
4. Uncheck the box labeled "Make this device discoverable to other devices"
5. Tap the Security Tab
6. Check the box labeled "Authentication(Passkey) required"
7. Tap OK

It is recommended that the device should have a password set to prevent unauthorized use. In this section if the option is available on the device, select the option to enable strong alphanumeric passwords. This feature can be accessed from the following screen:
Start Menu→Settings→Personal Tab→Password

After the password is set, set the device inactivity timer. This feature can be accessed from the following screen: Start Menu → Settings → System Tab → Power → Advanced Tab
Set the two options listed there to be checked and that the time is set to 15 minutes or less.

It is also recommended that the user make the following changes to the Internet Explorer web browser on the mobile device:

1. Open Internet Explorer
2. Tap Menu
3. Go to Tools… → Options
4. Tap the Security Tab
5. Uncheck "Allow Cookies"
6. Check "Warn when changing to a page that is not secure"
7. Tap OK

These changes are recommended to prevent any accidental disclosure of personal data due to browsing to a malicious site. Please read all warnings presented carefully before continuing to make sure that the page that was arrived at is indeed the page that you intended to visit.

Special Notes Regarding the P25M Card Reader:

The P25M has a security feature that once it is paired to a mobile device, it is no longer discoverable by any other mobile device. This prevents the data from being transmitted to multiple devices. Each P25M has an eight digit passkey that is unique to each device and is required to pair to a mobile device.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

15. Security Guidelines for 3rd Party Mobile Phone Applications

Special Note regarding installing 3rd party applications onto your mobile phone

It is advised that the user restrict the 3rd applications that are installed onto the mobile phone to those that are trusted. It is recommended if a 3rd party application must be loaded, that the user verifies that it is a signed application from a reliable source. If these guidelines are not followed, a trojan or other form of malware may be inadvertently installed and compromise the security of the device.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

16. Secure Storage of Sensitive Data

All transaction attempts, successful or not, must be logged.

All authorized transactions must be rotated daily, sequentially from Current Day Logs to Archives 1, 2, and 3. All logs rotated out of Archive 3 are purged, so that no authorized transactions shall remain for longer than 4 days. Auth Only and Offline Transaction logs will be purged after 7 days.

Special Notes on receipt truncation options

When the application is configured to not truncate the merchant copy of the receipt, this receipt must be stored in a secure manner. For example, in a safe that only the manager has access to. This procedure is imperative as failing to do so could lead to the compromise of cardholder data.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

17. Secure Deletion of Sensitive Data

All sensitive data is deleted upon either during upload and authorization, or uninstall of the application.

- If there is a transaction stored on the local device because authorization could not be performed online, then once it is possible to authorize, the local sensitive data is overwritten by some random string other than the sensitive data. There are two separate implementations:
    1. Implementation 1 updates the record with the sensitive data and does not delete it. In this case, the update destroys data on disk and thus sensitive data is destroyed.
    2. Implementation 2 deletes the record with the sensitive data. The app first overwrites the record with some data other than sensitive data, and then deletes the record.

Secure Deletion on Windows (prior to uninstall)

Download sdelete from Microsoft's website here: http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

1. From a command prompt, navigate to the QuickSale for Windows install directory, typically C:\QuickSale For Windows\
2. Run the command: sdelete –p 3 userInformation.dat
3. Run the command: sdelete –p 3 comstarpos.mdb
4. To ensure that free space on drive c: is wiped clean, run the command: sdelete –c c:

18. Uninstall procedures

It is a requirement of PCI that sensitive data is removed securely when an application is uninstalled from a device. Please follow the process below for your specific device. The process performed from within the app securely removes all sensitive, cryptographic keys, cryptograms, log files, debugging files, and any data that pertains to the application that is of sensitive nature.

Android:

Uninstall procedure:

From app

1. Login to the app
2. Go to Config
3. Go to Maintenance
4. Go to Unregister

From Device

1. Click Menu to go to System Settings
2. Select Applications
3. Select Manage Applications
4. Select the CHARGE Anywhere application
5. Select Uninstall
6. Follow any further instructions that are presented by phone

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

iPhone:

Uninstall procedure:

From app

1. Login to the app
2. Go to Config
3. Go to Maintenance
4. Go to Unregister

From Device

1. Long press on the CHARGE Anywhere application's icon until an 'X' appears
2. Press the 'X'
3. Press Delete in the pop up that displays

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

19. Upgrade Procedures

The standard procedure for an upgrade is to uninstall the old software version, thereby removing all historic data and cryptographic material as per PA-DSS requirements, before installing the latest version. It is also recommended that if the merchant no longer has need of the application that they delete the app to remove all historical data from the device.

Mobile Applications(Android, ios, ….)

Mobile applications are downloaded from the market place, every time there is an update; the user receives a notification that an update is available and will download the new application. If the update process is set to automatic (recommended), then the update will be automatically installed.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

21. **Card Holder Data retention.**
    All our application rotates data daily. All cardholder data is moved automatically at day end to the next day archive log. There are 3 archive logs in the application, after day 4 the, archive 3 is purged. The merchant also has the ability to purge all this data from the application manually from the maintenance menu by choosing, rotate logs.

    In the situation where the Customer Database feature is available, the merchant has the option to delete any profiles that have not been used for a certain period of time. The typical workflow for deleting a customer profiles is as follows:
    1. Access the Customer Database Screen
    2. Select the filtering option for Last Used
    3. Choose the cutoff date for the Last Used value
    4. Perform Search
    5. Delete the desired profiles

Disabling System Restore Points in Windows 7/8

In order to prevent storing clear text cardholder data, or sensitive authentication data, systems running Windows and payment applications should have Windows System Restore Points disabled. This will prevent violation of PA-DSS requirement 2.1.

The following steps can be used to disable System Restore Points on Windows 7

- Click Start, right-click Computer, and then click Properties.
- In the left pane, click System Protection.
- Enter the administrator password
- Under Protection Settings, select the disk, and then click Configure.
- Choose the radio button labeled “Turn off system protection”
- Click OK, and then click OK again.

For Windows 8, follow these instructions:

- Move the cursor to the bottom right corner of the screen, select the charm bar and choose “Settings”
- Choose PC Info > System Protection
- Click on Configure
- Select “Disable System Protection”
- Click “Apply”

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

22. Logging

Access to several parts of the application is logged and trace including and not limited to the below:

- All individual accesses to cardholder data.
- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.

Each log entry contains at least:

- User identification.
- Date and time.
- Application that originated the event.
- Hardware Id (Mobile Devices) or IP Address
- Message describing the event.

Centralized Logging

For both mobile and desktop applications, these logs are downloaded to the server as they are generated and are stored for the merchant to review 24/7 for a period of one year. Merchants can access their application logs at:

https://www.chargeanywhere.com/transactionmanager/login.aspx

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

23. Training Sessions

Training sessions will be held periodically per PA-DSS requirement section 13. The session information will be sent out in an email two weeks prior to the scheduled date of the training. The training will cover the PA-DSS requirements to deploy the payment application in a secure manner.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

24. Troubleshooting Procedures

During the troubleshooting of a device, the data on the device will not be copied nor transmitted in any fashion. The troubleshooting process involves a customer support representative directing the merchant to take specific steps to remedy the issue. If the customer support representative cannot resolve the issue, they document the exact error and if possible, the steps required to recreate it. The issue is then posted to the development team. The development team tries to reproduce the issue, resolves it, and then publishes a new version for download.

The steps described above also apply to any reseller's or integrator's support staff. Under no circumstances should application data be copied from the device or transmitted in any fashion.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

25. Ports Used By All Applications

CHARGE Anywhere is a stand-alone application and does not require services or daemons to run. It also does not require any inbound traffic. The following outbound ports are needed for CHARGE Anywhere to operate.

Port Number	Service
80	HTTP
443	HTTPS

To further lock down outbound traffic, restrict outbound traffic for CHARGE Anywhere to the following domain:

*.chargeanywhere.com

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

About CHARGE Anywhere: CHARGE Anywhere is a leading provider of secure Point of Sale (POS) solutions and electronic payment services. Our proprietary Visa Payment Application Best Practices (PABP) Charge Anywhere® v2.2.x.x Mobile Payment and POS software solution designed for QuickBooks®, Smartphones and e-commerce environments, and the Web Terminal Payment Solution - ensures Payment Card Industry (PCI) Level 1 compliance via ComsGate® Payment Gateway. CHARGE Anywhere offers business partners and customers the most secure and robust selection of industry specific and customized POS solutions and services, including; IP/Wireless Payment Gateway, POS software, Encryption and Data Security Services, Custom Card Issuance, and Merchant Billing Services. For more information contact them at www.chargeanywhere.com , or (800) 211-1256.