# Security Guide for New Clients

December 2019

# Security Guide for New Clients

## Table of Contents

# Security Guide for New Clients

## Introduction

This document explains the basic, security PCI PA-DSS compliance information for 365 Retail Markets Kiosks. Contact Robert Hering at **888-365-6282 ext. 160** or Robert.Hering@365smartshop.com with any questions related to this document.

## About the PCI PA-DSS Security Standards

The PA-DSS Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PA-DSS Security Standards. This includes:

- The Data Security Standard (DSS),
- Payment Application Data Security Standard (PA-DSS),
- PIN-Entry Device (PED) Requirements.

All of the five founding credit card brands have agreed to incorporate the PA-DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs and ASVs certified by the PA-DSS Security Standards Council as being qualified to validate compliance to the PA-DSS.

The PA-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. All businesses handling credit and debit cards are required by the card brands to maintain PA-DSS compliance.

The PA-DSS is a security standard designed to help software vendors develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PA-DSS Data Security Standard. All payment applications handling credit and debit cards are required by the card brands to maintain PA-DSS compliance.

## 365 Retail Markets is PCI PA-DSS Validated

The 365 Retail Markets Kiosk is a validated Payment Application approved by the PCI SSC. PCI PA-DSS validation is an ongoing process that requires annual audits of 365 Retail Markets:

- Development Environment and Release Process
- Handling of Card Holder Data and Proper Encryption
- Corporate Network and the Access Levels of Essential Personnel
- Security of Kiosk Hardware and Physical Access
- Proper Disposal of Card Holder Data Upon Deletion

365 Retail Markets can provide the Attestation of Validation upon request or you may view our validated Payment Application on the PCI website at the following link: https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true

Additionally, the screenshot below shows an online listing of our validation:

| COMPANY | VALIDATION NOTES | DEPLOYMENT NOTES | REVALIDATION DATE | EXPIRY DATE | VALIDATED BY PA-QSA |
|---|---|---|---|---|---|
| 365 Retail Markets, LLC | | | | | |
| SmartHub Kiosk | | | | | |
| **Version #:** 2.0.6.3<br>**App Type:** POS Kiosk<br>**Target Market:** Major, local, US-based merchants that range in size from single owners to large-sized organizations<br>**Reference #:** 16-07.00817.002.aaa<br>**Tested Platforms/Operating Systems:** Windows 7, Windows POSReady 7<br>**Service Pack/Build/Version:** SP1, Embedded SP1 | Validated According to PA-DSS *(PA-DSS v3.2)* | Acceptable for New Deployments | 13 Oct 2020 | 28 Oct 2022 | Sikich LLP |

| PA-DSS APPLICATION DEPENDENCIES | REVALIDATION DATE | EXPIRY DATE |
|---|---|---|
| CreditLine, 4.1.3 SPxx | 28 Oct 2019 | 28 Oct 2019 |

| OTHER DEPENDENCIES |
|---|
| Cisco RV110W Firmware 1.2.1.7 |
| 365 Retail Markets Gen3 kiosk |
| LogMeIn Central Premier Enterprise |
| Microsoft .NET Framework 4.6.1 |
| Microsoft SQL Server 2008 SP4 10.0.6547.0 Express Edition |

**Description Provided by Vendor:** 365 Retail Markets designed SmartHub Kiosk to be a turnkey, unattended, and highly automated kiosk. Customers scan and pay for items selected at MicroMarkets using the SmartHub Kiosk payment center.

## Storing Sensitive Card Data

ATTENTION: 365 relies on 911 CreditLine to encrypt, transmit and process all credit card data and transactions. The 911 CreditLine application is PA-DSS certified. Current and previous versions of 365 SmartHub and 911 CreditLine payment applications do not store Sensitive Authentication Data (SAD), such as card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks.

## 365 Payment Application and Storing Sensitive Card Data

The 365 SmartHub payment application does not support the storage of any sensitive credit card authentication data. Use of a highly restricted Windows user account to auto-login the PC prevents a software compromise that could result in the collection of sensitive data. The 365 SmartHub payment application, through 911 CreditLine, encrypts and sends sensitive card data via a PA-DSS certified gateway that securely stores (specifically, cardholder name, first two and last four digits of primary account number (Truncated PAN)) indefinitely to allow a merchant time to verify that deposits have been received.

**Note:** The 365 SmartHub payment application only displays the truncated PAN where needed on printed receipts and on credit reports generated by the operator. The truncated PAN is stored with only the first two and last four digits and only the truncated PAN is displayed, as the 365 SmartHub payments application does not store in-scope credit card data. By default any place the PAN would be displayed, it would be truncated to only the first two and last four digits.

There is any debugging or troubleshooting settings that permit sensitive information, such as magnetic stripe data, to be electronically stored in an unencrypted fashion. 365 does not collect or store magnetic stripe data for troubleshooting. To ensure end-user PA-DSS compliance, credit card numbers and track data cannot be retrieved from any portion of the 365 payment application. 911 CreditLine Software version 4.1 has been certified by PCI Security Council Quality Assurance Program.

## 911 CreditLine Server – Security Setup

911 CreditLine Server setup is pre-installed by 365 and does not require any operator intervention. This section is informational for operators and clients.

This section describes the security features of the 911 CreditLine application. These features were implemented as part of participation in industry wide credit card security programs. CreditLine version 4.1.3 SPxx and higher have been certified by VISA to be secure and follows the PA-DSS, as well as CISP PABP, guidelines based on the PA-DSS Data Security Standard.

The 911 CreditLine application ensures compliance with the PA-DSS Data Security Standard through the use of multiple security methods, including:

- Use of a secure token interface using a PCI certified gateway for all communication to and from credit card processors.
- Encryption keys that are automatically replaced before every encryption request, with previous keys made irretrievable.
- CreditLine logs provide a complete and secure audit trail of logins and all action performed on data with access provided only to those who job functions require it, and through secure level of passwords mandated by the CreditLine software.
- CreditLine account encryption and use of unique user names.

To ensure you are accessing the latest version of the Security Guide, you should review the document online at http://docs.911software.com.

## Troubleshooting and Storing Sensitive Card Data

The 365 payment application uses 911 CreditLine to accept and process credit cards. On the surface, it appears that the 365 payment application is accepting CHD, however this is all being handled by 911 CreditLine through a custom UI.

For that reason, the 365 payment application never transmits, stores, nor processes a sensitive CHD. 365 Coding Standard Collection of Sensitive Data explicitly states that CHD should only be handled by 911 CreditLine software, and any deviation is a violation of 365 Retail Market's Secure Coding Policies.

In collaboration with 365 Retail Market's Security Policies, 365 Support representatives will never collect, store, or communicate CHD. This data includes:

| | |
|---|---|
| Primary Account Number | Magnetic Stripe Data |
| Cardholder Name | Card Numbers |
| Expiration Date | CAV2/CVC2/CVV2/CID |
| Service Code | PINs/PIN blocks |

If an operator or 365 employees is asked to refund or void a credit card transaction originating from the 365 payment application, they are instructed to:

- Communicate to the client that the 365 payment application does not store credit card data and therefore cannot perform refunds.
- If the consumer requesting the refund has a MicroMarket user account, 365 or the operator can adjust their account balance without generating another credit card transaction on SmartHQ (this process is a manual customer service adjustment andis NOT associated with the 365 payment application and 911 CreditLine).
- If the consumer or client insists on a refund to their credit card, the operator can contact their credit card processor, who may provide a refund. This refund is NOT associated with the 365 payment application and 911 CreditLine.

## Encrypt Sensitive Traffic over an Internet Connection

365 relies on the 911 CreditLine application to accept, encrypt, transmit, and process all credit card data and transactions. The 911 CreditLine application is PA-DSS certified. The 365 SmartHub payment application does not store in scope credit card data.

The 365 SmartHub payment application, through 911 CreditLine, allows operators to choose from a variety of payment processors. Supported processors can be reviewed on 911 CreditLine's website at the following link: http://www.911software.com/processors/

All transmissions to and from the 911 CreditLine application and the chosen payment card processing service are encrypted using TLS and an approved strong encryption protocol transmitted via a PA-DSS certified credit card gateway. Attempting to send sensitive card data through alternate means is not supported by the 365 payment application or 911 CreditLine. 365's support and implementation personnel do not provide credit cards refunds. If the operator needs to complete a refund to a consumer's account, the operator must work through the relevant credit card payment processor.

## Remote Access

Remote access into the SmartHub Kiosk is restricted to select 365 Retail Markets employees for support and troubleshooting purposes only. Operators and clients will not be granted remote access, or administrative access to the SmartHub kiosk at any time for any reason.

365 Retail Markets employs LogMeIn Central with the Professional client package. It is configured with two-factor authentication, to access an operator's payment application for client support and troubleshooting purposes. All communications to and from LogMeIn use industry-standard algorithms using the TLS v1.0/v1.1/v1.2 protocols. Although older versions of the TLS protocol are supported, LogMeIn provides information on protections from known attacks at the following link: https://blog.logmein.com/products/poodle-logmein.

In addition, LogMeIn offers the following security whitepaper covering security measures that protect endpoints using the LogMeIn client: https://secure.logmein.com/welcome/documentation/EN/pdf/common/LogMeIn_SecurityWhitepaper.pdf?_ga=1.139209211.954905911.1438558445.

Finally, 365 Retail Markets configures all systems to only support the TLS v1.1/1.2 protocol at all our workstations/endpoints.

Both LogMeIn and the host operator's computer running the 365 payment application employ a lockout mechanism that will only allow a limited number of remote incorrect login attempts before locking the 365 user's account or offending IP address.

Additional LogMeIn security access features include:

- Use of strong authentication and implementation of accounts that are unique and specific to the 365 user accessing the operator's 365 SmartHub payment system.
- Auditing capabilities accessible under a 365 SmartHub user's account security settings that notify user by email when a change (e.g., adding a new computer) or suspicious event (incorrect login) occurs.
- Creation of detailed event logs that write major events (e.g., starting and ending a remote login session) into the operator's operating system event log.

LogMeIn remote access sessions contain three key components:

- Client
- Host
- LogMeIn gateway

The LogMeIn Host maintains a constant TLS secured connection with one of the LogMeIn gateway servers which are all held in a physically secure datacenter. When a client logs into a browser, LogMeIn uses TLS (Transport Layer Protocol) certificates to verify server identity. If the server passes verification, the client browser generates a "Pre-Mater Secret" or PMS, encrypts it with the server's public key contained within its certificate, and sends it on to the LogMeIn server. With the use of public key cryptography, only the LogMeIn server that holds the corresponding private key can decrypt the PMS. The PMS is then used to derive session keys for the duration of the secure session.

LogMeIn users are authenticated by both the gateway and the host. The gateway must prove its identity to the host before it is trusted with access code. The host checks its TLS certificate to assure it is connecting to a LogMeIn gateway server. The host's identity to the gateway is verified when it accepts an incoming connection using a long unique identifier string only communicated over an TLS-secured channel. Data encryption between client and host is accomplished through the strongest cipher possible. This is done by the client sending the host a list of ciphers it is willing to use, and the host choosing the one it prefers from the following list:

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

# Networks

## Wireless Networks

Third party wireless or Wi-Fi (802.11x) wireless devices are not supported and cannot be connected to the SmartHub Card Data Environment.

## Corporate Versus Dedicated Networks

The 365 SmartHub kiosk requires network connectivity for credit card processing and receiving updates. Operators have two primary options for establishing network connectivity at most client locations, corporate and dedicated networks.

Many corporate environments (offices, hospitals, etc.) contain existing networks to provide Internet connectivity throughout a building. These corporate networks often restrict the types of information that can be transmitted on them. Corporate networks are typically managed by a dedicated team member(s) who can advise on the feasibility of allowing your kiosk to operate on their existing Internet connection.

A dedicated network, (which for the purposes of this document) constitutes a completely separate network that operators would install, circumvents many challenges that a corporate network may present. A dedicated network could consist of a DSL line, 3G/4G Wireless card, or other dedicated high-speed connection. As the kiosk owner, the operator would need to organize this new, dedicated service to be installed into the client's environment.

| **Corporate Network*** | **Dedicated Network**** |
|---|---|
| **Pros** | **Pros** |
| Internet service already in place. No additional cost to the operator. | Do not need to ask client IT staff to open access or run wiring to a new location. |
| Network is typically very fast compared to DSL or cellular Internet service. | The operator owns the network, and therefore requires less coordination to ensure PCI best practices are being followed. |
| Typically managed by dedicated personnel at the client location with knowledge of troubleshooting and secure networking protocols. | If cellular is chosen, you have the added mobility to move the kiosk and internet together as needed. |
| **Cons** | **Cons** |
| The operator may need to coordinate and implement the correct and secure settings with the client IT staff/network administrator. | The operator needs to organize, implement and pay for Internet service. |
| Wiring is typically run to a single location, making kiosk mobility challenging. | Network connectivity (especially cellular) may be slower than a corporate network. |
| The operator is responsible for ensuring the corporate network follows PCI standards which often requires more coordination with client IT staff. | When service is interrupted (power surge, modem needs reset) the operator is responsible for troubleshooting the outage. |

*If the operator chooses to use a corporate network, it is the operator's responsibility to ensure this guide is followed by the client network administrator. Be sure to supply them a copy of this guide early in the implementation process, paying special attention to the Networks section.

**If the operator chooses to use a dedicated network, it is their responsibility to ensure the best practices outlined in this guide are followed. May require an operator resource with IT and networking knowledge to ensure the best practices are outlined in this guide. (365 Retail staff is available to assist with secure network setup)

## Network Segmentation for Corporate Networks

For deploying on a corporate network, segmenting the kiosk into a secure card data business environment is required. Network segmentation is a strategy intended to simplify the PA-DSS compliance of your network and help you protect your business from hackers. At the most basic level, there are three zones representing three levels of risk.

- **High Risk – Untrusted Environment** – Network connections that anonymous people have access to be considered "untrusted." They should have no network access to your business computers and POS equipment. Business computers should never be connected directly to this zone. Common untrusted networks are the internet connection itself, customer wireless internet access, and visitor network connections. This is the highest risk zone because anybody can connect to it anonymously.
- **Medium Risk – Non Card Data Business Environment** – Systems that are not used for payment processing but are still business owned fit into this segment. These are systems that can be used for email, web browsing, and other higher risk activity that you would never want to perform on your payment processing systems. On occasion, these systems will almost certainly become infected with malware and viruses. When a computer in this zone is infected, the hacker or infection will spread to other systems if they are not protected by a firewall.

  **Note: I**f any systems in this zone handle credit card data, that data is being put at risk.

  This is a medium risk zone due to risk of occasional infection. By segmenting these systems into their own zones, a breach can be contained. The hacker, malware, or virus do not reach your payment processing zone that is protected by a firewall.
- **Low Risk – Card Data Business Environment** – Systems used for payment processing fit into this segment. These systems should only be used for POS activity and should NEVER be used for any other reason. If these computers become infected with malware or viruses, sophisticated hacking tools can potentially steal sensitive data such as credit cards. This is a low risk zone because it's protected from the other two zones and high risk activities such as web browsing, and email do not occur inside it. The chance that hackers, malware, or viruses spread to these systems is minimal.

In summary, to segment your network for security you should:

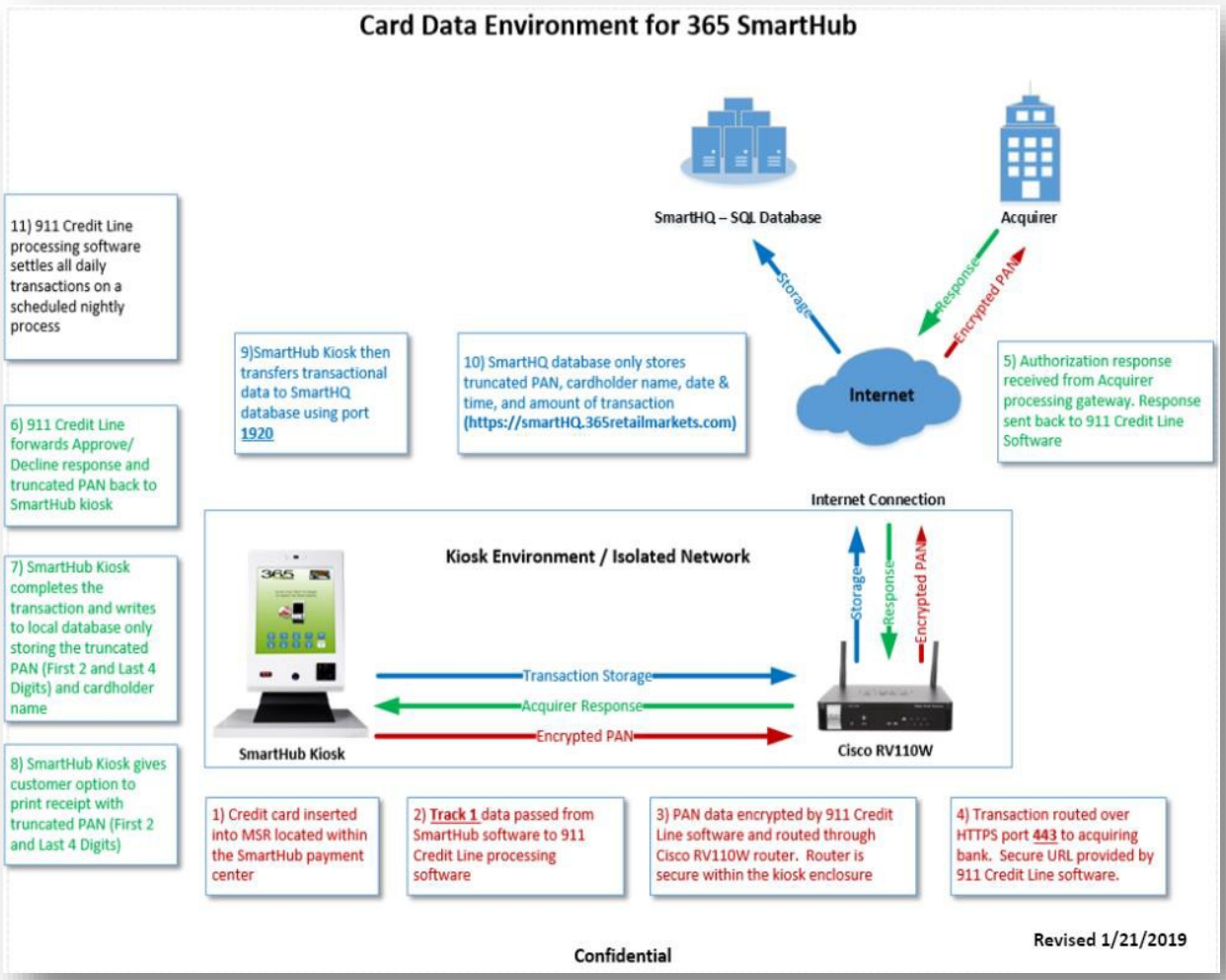
- Protect both the low risk and the medium risk business environments from the high risk untrusted environment.
- Protect your low risk Card Data Business Environment from the medium risk Non-Card Business Environment.

## Best Practices for Dedicated Networks

- Always change vendor supplied passwords on DSL or cellular modems. Do not leave default passwords on any of your network devices.
- Keep your network devices (modems, switches, routers) in a secure, locked area.

- Disable all WiFi broadcasts from modems.
- Upgrade the firmware on your devices regularly. Manufactures often deploy security patches to their devices. You are responsible to ensure that your device firmware stays up to date.
- A dedicated network is your Card Data Business Environment. Do not use it for any purposes other than those critical to your business. This includes only the services outlined in the Kiosk Technical Network Requirements document.

## Non-OTI Kiosks (PA-DSS and PC DSS)



## OTI Kiosks with E2EE at Swipe (PCI DSS)