PA_DSS Implementation Guide

PA-DSS Doc 3.0

Applicable Application Version

This document supports the following application version: 1.5

Introduction

Systems which process payment transactions necessarily handle sensitive cardholder account information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data. The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

INSOMNIAC Kiosk is a Point-of-Sale (POS) solution for small retailers and is not intended to be used by issuers or organizations performing issuing services. The application supports an application/database model for deployment, with the application operating on the Windows 7 32-Bit SP1 or 64-Bit SP1 system, running Microsoft Access for data storage. Distribution of the software includes the INSOMNIAC Kiosk software and the Microsoft Access database.

The application supports the following PinPad/MSR device types:

Magtek PermaSeal Insert Reader

Transmitting CardHolder Data

The INSOMNIAC Kiosk application transmits cardholder data over the Internet using 128-Bit SSLv3.0 for encryption to your property Management System Vendor. This is done by default and cannot be disabled. This secure, encrypted transmission is required for you to maintain PCI DSS compliance. This is the only means of transmitting cardholder data supported by the INSOMNIAC Kiosk software; the application does not support and/or facilitate sending of PANs by end-user messaging technologies.

Note: Understand that the transfer of cardholder data across public networks must be encrypted in order for you to maintain your PCI DSS compliance.

INSTALLED Files

The INSOMNIAC Kiosk application comes pre-installed on your kiosk. The installation directory is c:\insomniac.

These files are critical to the application and should be monitored for unauthorized access and modification attempts.

Logging

A key feature of the INSOMNIAC Kiosk to enable you to meet PCI DSS compliance is logging. INSOMNIAC Kiosk enables extensive logging for all user types. This logging is required for you to maintain your PCI DSS compliance and, as such, logging is enabled by default per PCI DSS and PA DSS requirements and may not be disabled or configured. For all log files, only the last four (4) digits of the PAN are recorded.

Log File Location and Names

All log files are located within the c:\insomniac\logs directory. Within this directory you will find the following log files:

- YYYYMMDD.log - This log file contains information for troubleshooting the main INSOMNIAC Kiosk application
- YYYYMMDDnet.log – This log file contains information for troubleshooting the .net components of the INSOMNIAC Kiosk application
- ccYYYYMMDD.log – This log contains information for troubleshooting the credit card reader. Note that no card holder data is logged
- imYYYYMMDD.log - This log contains information for troubleshooting the INSOMNIAC Monitor application which is responsible for automatic updates of the INSOMNIAC Kiosk software as well as reporting the health of the kiosk
- kbYYYYMMDD.log – This log contains information for troubleshooting the on-screen keyboard.

Support

Customers may contact OpenTech for support in troubleshooting the INSOMNIAC Kiosk or for the reporting of issues with the application. Support consists of phone and email support and, when needed, remote access support. Support may be contact at:

Phone: 602.749.9370 Option 2

Email: support@opentechalliance.com

Note: OpenTech will not collect sensitive authentication data (magnetic stripe data, card validation codes or values, and PINs or PIN block data) or Primary Account Numbers (PAN) for any reason, even upon customer request. To do so may compromise PA DSS validation and, in return, your PCI DSS compliance.

If you, as a customer, decide to collect sensitive authentication data as part of your own troubleshooting process, you must adhere to the following guidelines or risk compromising your PCI DSS compliance:

- You must only perform the collection of sensitive authentication data when needed to solve a specific problem;

- You store such data in a specific, known location with limited access;
- You must perform collection of only the limited amount of data needed to solve a specific problem;
- You must provide for the encryption of sensitive authentication data as required upon storage; and
- You must perform secure deletion of such data immediately after use, using tools which utilize the DoD 5220.22-M military grade secure deletion process.

The following high level 12 Requirements comprise the core of the PCI DSS:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect Stored Data

4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to 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

PCI DSS Payment Application Environment Requirements

Firewall Protection

Each site is required to protect the INSOMNIAC kiosk with an appropriate firewall. Most consumer routers and ISP provided modems offer firewall support and these should be enabled.

Default Passwords

The default passwords for the INSOMNIAC application should be changed during setup.

Access Control

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed, or at least should have PCI DSS compliant complex passwords and should not be used.

Contact our STC department to create a new user to administer the settings of your INSOMNIAC kiosk.

Remote Access

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate). In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

In the case of Company customer support, Company utilizes the application LogmeinRescue for remote access. This access is only enabled during the time of support and must be disabled after support is concluded.

To use the LogmeinRescue, Company engineer will direct you to the Logmein website to download and run the client. Once troubleshooting is complete, you will exit the Logmein session, terminating any remote access. Company will never have access to your computers without you initiating connectivity first.

If purchased, OpenTech's call center agents will also have access to remote control your kiosk in order to assist your customers with transactions. Please note that call center agents are unable to exit the INSOMNIAC software or make any modifications to your kiosk.

Sites wishing to remotely access the INSOMNIAC Control Panel should setup a VPN system on their network with 2 part authentication. Additionally a secure certificate should be setup so that the INSOMNIAC Control Panel is only accessible via https.

Automatic Updates

Your INSOMNIAC kiosk should be set to automatically download Windows Updates. The setting is necessary for PCI compliance.

Software Upgrades

Your INSOMNIAC kiosk will be automatically upgraded when new software is available. You can request that this feature be turned off by contacting our tech support.

Virus Scanning

Each site should install and maintain anti-virus software on their INSOMNIAC kiosk. Please note that OpenTech does not supply anti-virus software. Contact OpenTech Technical Services for help in choosing an anti-virus application

Wireless Access Control

The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment application environment with rules restricting access
- Use of appropriate encryption mechanisms such as VPN, SSL/TPS at 128 bit,WEP at 128 bit, and/or WPA
- If WEP is used the following additional requirements must be met:
    - Another encryption methodology must be used to protect cardholder data
    - If automated WEP key rotation is implemented key change should occur every ten to thirty minutes
    - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC Address filtering)

Information Security Policy/Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data. The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed. Visa has published a Qualified Security Assessor List of companies that can conduct on-site CISP compliance audits for Level 1 Merchants, and Level 1 and 2 Service Providers. MasterCard has published a Compliant Security Vendor List of SDP-approved scanning vendors as well.

Sensitive Credit Card Data Requires Special Handling

- Only collect sensitive authentication only when needed to solve a specific problem
- Store data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Delete such data immediately after use