

Lucas POS System

Point of Sale Software for Restaurants

CISP / PCI DSS Security Implementation Guide

Version 1.00.00

Release 1
Part Number 9000-001

Lucas Systems, Inc.

123 Grace Drive
Easley, SC 29640
(864) 288-9122
(864) 288-9097 Fax
www.lucaspos.com

Copyright © 2000-2007 Lucas Systems, Inc.

No part of this manual may be reproduced in any way without the express written consent of Lucas Systems, Inc.

Lucas Systems reserves the right to make changes to the functionality of this system without prior notice and this manual only reflects the functionality of the program at the time of printing.

Document Information

Author: Mark D. Hupman
File Name: lsi-cisp_pci-implementation-guide.doc
Last Save Date: 12/21/2007 5:10 PM
Last Print Date: 12/23/2007 12:49 AM
File Size: 91,648 bytes
Pages: 14

Table of Contents

- INTRODUCTION..... 5**
- ACCESS CONTROL..... 6**
- REMOTE ACCESS 6**
- NON-CONSOLE ADMINISTRATION 6**
- WIRELESS ACCESS CONTROL 7**
- TRANSPORT ENCRYPTION..... 7**
- NETWORK SEGMENTATION..... 7**
- INFORMATION SECURITY POLICY/PROGRAM..... 8**
- PAYMENT APPLICATION CONFIGURATION 8**
- Baseline System Configuration.....8**
- Addressing Legacy Issues9**
 - Procedure for Removing Sensitive Historical Data9
- Application Configuration.....9**
 - Windows XP Security.....9
 - pcAnywhere Configuration10
 - Email.....11
 - Datacap Applications.....11
 - Anti-Virus12
 - Credit Card Server12
 - Hardware Firewall12
 - Event Logging12
 - Internet Applications13
- Best Practices for Support and Troubleshooting.....13**
- MORE INFORMATION 14**

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.

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

The remainder of this document describes the essential guidance for implementing Lucas POS in a PCI compliant environment.

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 as possible, or at least should have PCI DSS compliant complex passwords and should not be used. Examples of default administrator accounts include “administrator” (Windows systems), “sa” (SQL/MSDE), and “root” (UNIX/Linux).

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

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.

Non-Console Administration

Users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, pcAnywhere, etc. to access other hosts within the payment processing environment. However, to be compliant, every such

session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for pcAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

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)

Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard sensitive cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

Additionally, PCI requires that cardholder information is never sent via email without strong encryption of the data.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

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.

Payment Application Configuration

Baseline System Configuration

- Microsoft Windows XP Professional with Service Pack 2. All latest updates and hot-fixes should be tested and applied.
- 256 MB of RAM minimum, 512 MB or higher recommended
- 200 MB of available hard-disk space for programs
- Minimum of 10GB free space for data
- TCP/IP and IPX network connectivity.

Addressing Legacy Issues

Depending on their configuration, prior versions of the POS application may have temporarily stored small amounts of credit card data on the PC. While this data is encrypted, it does not meet the requirements of PCI compliance and must be handled in an appropriate manner when upgrading to a PCI-compliant version of the software. If prior data is not securely removed from the system during a PCI-compliant upgrade, the system will not be considered compliant.

Procedure for Removing Sensitive Historical Data

In order to meet the requirements for PCI compliance all cryptographic material must be securely removed from the system. The following steps outline the procedure for removing cryptographic material from the system:

1. Use the TFS4v0.exe tool provided by Lucas Systems to delete any historical DAT files.
2. Run TFS4v0 and use the File => Select File function to select the following files:
 - C:\Program Files\CCServer\Logs\cctrans.dat
 - C:\Program Files\CCServer\Logs\forcedtrans.dat
3. Click the check next to both files in the File Path Window
4. Click the Delete All button
5. Click Yes at the warning prompt.

Application Configuration

Windows XP Security

1. Setting up Windows XP User Accounts on the host system

Each individual with access to the computer should have their own login. There should be two Permanent Windows User Accounts configured with Administrator access, and as many Standard User accounts as necessary for the management staff. The following is an example of a typical user Account setup:

Name	Group	Password	Purpose
Administrator	Administrators	Yes	Full Access for owner
Lucas	Administrators	Yes	Full Access for Lucas Systems
Manager	Standard Users	Yes	Limited Access
Assistant	Standard Users	Yes	Limited Access
Assistant	Standard Users	Yes	Limited Access
Supervisor	Standard Users	Yes	Limited Access

Notes on User Settings:

1. Administrative accounts should not be used for routine application logins.
2. Strong passwords must be assigned to these default accounts, and any that are not required should be disabled or removed from the system.
3. Always assign strong application and system passwords whenever possible. See Section 2 - **Local Security Settings** for more information on strong passwords.

2. Local Security Settings

In order to maintain the required level of password security on the system, the following settings must be configured in the Windows XP Local Security Settings module:

Password Policy:

Enforce Password History - Set to remember the last 5 passwords.
 Maximum Password Age - 21 Days
 Minimum Password Age - 0 Days
 Minimum Password Length - 7 Characters

Account Lockout Policy:

Account Lockout Threshold - 6 Attempts
 Account Lockout Duration - 30 Minutes
 Reset Account Lockout Counter After - 30 Minutes

3. Disabling Unnecessary Services

All unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, FTP server, HTTP server, etc.) should be disabled on the PC running the Lucas POS System. The POS PC should never be used to host a public FTP or HTTP (Web) server.

Protocols and Ports can be disabled from the Windows Firewall and the Hardware Firewall.

Services can be disabled from Control Panel => Administrative Tools => Services.

pcAnywhere Configuration

pcAnywhere is used for remote access to the system, but it must be set up properly in order to meet the requirements for PCI DSS compliance. The following procedures must be followed when using pcAnywhere:

- The default settings created by pcAnywhere during installation are not secure. All default settings generated by pcAnywhere must be changed before the system goes live (for example, change default passwords and create unique passwords for each user)

- Access to logon information and passwords must be limited to authorized personnel. This includes both above-store personnel (Owner, Area Managers) and Lucas support personnel.
- Create passwords that meet the requirements of PCI DSS requirements. See sections 8.1, 8.2, 8.4, and 8.5.

In addition, the following pcAnywhere configuration is required when allowing Remote Desktop access to the host system:

1. pcAnywhere should not be configured to launch automatically when Windows starts. Instead, a button on the Lucas Site Manager menu should be configured to allow someone on-site to manually launch a host when a connection is needed.
2. The pcAnywhere host connection object should be set to Cancel the Host after any session ends. If a re-connection is needed, the host will need to be launched manually again by someone on-site.
3. There should be a dedicated pcAnywhere Caller for each person who has access to the host remotely. By default, there are two pcAnywhere callers set up on each host:

Name	Description	Password	Purpose
HQ	Owner's Access	Yes	Remote system access for owner
Lucas	Lucas Support	Yes	For Lucas remote support

4. Strong passwords and unique logins must always be used for remote access. See Section 2 - **Local Security Settings** for more information on strong passwords.
5. The host should be configured to use the Symmetric encryption level and the option to Deny Lower Encryption Level should be checked.
6. Under Log In Options, the option to limit the number of login attempts per call should be checked and the limit should be set at 3.
7. pcAnywhere logging should be enabled by going to Edit => Preferences => Event Logging and checking the box for Enable Event Logging and Record in Local NT Event Log. Under the Select Events button, choose Select All to record all types of events.

Email

The Lucas application does not send cardholder data via email.

Datacap Applications

Systems using Datacap NETePay or DIALePay as part of the Lucas POS system need to be running version 4.00 or higher in order to be compliant. Versions 3.xx and of the Datacap software earlier do not store cardholder data in a secure manner, and must be upgraded.

Anti-Virus

Anti-virus software must be installed on the Manager's PC, and must be configured to automatically receive and install updates. It is the owner's responsibility to make sure the anti-virus database is kept up to date and the software license is renewed as needed.

Credit Card Server

The Settings screen in Credit Card Server can only be accessed by an Administrator. Users must log into the system with one of the permanent Administrator accounts to make changes to the Credit Card Server configuration.

Hardware Firewall

An ICSA Labs Certified Firewall needs to be installed as part of the Lucas POS system in order to maintain the proper level of security. The firewall should be configured to allow incoming network connections for only those services required for proper restaurant operations. Examples are pcAnywhere, a Digital Video System, and VPN. Outbound connections should also be restricted to only those services required for proper restaurant operations. Examples are HTTP client, FTP client, POP3 client, SMTP client, Credit Card processing, and Gift Card processing.

Event Logging

Routine Functions: All routine activity will be logged to the Windows NT Event Log. The log can be accessed in Control Panel => Administrative Tools => Event Viewer. The routine security events are recorded in the Application Log and identified by the source "LucasSecurityModule".

Credit Card Server Functions: All Credit Card Server activity will be logged to the Windows NT Event Log. The log can be accessed in Control Panel => Administrative Tools => Event Viewer. The Credit Card Server security events are recorded in the Application Log and identified by the source "CCServer".

PcAnywhere Functions: All pcAnywhere activity will be logged to the Windows NT Event Log. The log can be accessed in Control Panel => Administrative Tools => Event Viewer. The pcAnywhere events are recorded in the Application Log and identified by the source "pcAnywhere".

Internet Applications

In order to meet the requirements of PCI DSS, sensitive cardholder data cannot be stored on a server connected to the internet. The Lucas application does not provide internet services, and does not require that any internet applications reside on the computer containing cardholder data. Software that provides internet services (such as a web server or FTP server) must never be run on the same computer as the Lucas application.

Best Practices for Support and Troubleshooting

The following guidelines must be followed by Resellers, Integrators, Support Technicians, and End-Users when dealing with sensitive information in order to meet the requirements of PCI compliance:

1. Personnel must collect sensitive authentication only when needed to solve a specific problem.
2. Personnel must store such data only in specific, known locations with limited access.
3. Personnel must collect only the limited amount of data needed to solve a specific problem.
4. Personnel must encrypt sensitive authentication data while stored.
5. Personnel must securely delete such data immediately after use.

More Information

A copy of the Payment Card Industry (PCI) Data Security Standard from VISA's security website is available at the following Internet address:

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

Additional information for merchants from VISA is available at the following Internet address:

http://usa.visa.com/merchants/risk_management/cisp_merchants.html

A listing of qualified security assessors from VISA is available at the following Internet address:

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf