



# Lucas POS V4 Embedded

Version 4.02

---

## Secure Implementation Guide

---

Document Revision: 5

Lucas Systems provides this publication as is without warranty of any kind, either expressed or implied. This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lucas Systems may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time.

*Copyright © 2010 National Computer Corporation, Inc. All Rights Reserved.*

# Revision History

Rev	Author	Date	Description
1	DCH	Mar-2008	Created
2	DCH	Dec-2009	Modified for R4 and R4/ServiceMgr
3	DCH	May-2010	Modified for RTPOS
4	DCH	Aug-2010	Split document from WinPOS Updated for Windows 7 Modified Back Office PC Security to include enabling Automatic Updates Added Default Encryption Keys to Wireless Access Control Modified Wireless Access Control to only permit WPA2 Added IM and Txt Messaging to Transport Encryption Added Journal Lines to System Setup in RTPOS configuration Added information regarding DataCap products using SSL to send CHD over public networks Restrict VPN access to known IP/MAC addresses
5	MDH	Mar-2011	Updated for Lucas POS V4 Embedded

# Review History

Rev	Reviewed By	Date	Description
1	DCH	Feb-2009	No changes required

# Table of Contents

<b>Introduction .....</b>	<b>1</b>
Purpose .....	1
PCI DSS .....	1
Maintenance .....	1
<b>PCI DSS Payment Application Requirements .....</b>	<b>2</b>
Access Control.....	2
Remote Access.....	2
Non-Console Administration .....	2
Wireless Access Control .....	3
Transport Encryption.....	3
Network Segmentation.....	3
Application Updates .....	3
Cardholder Data.....	3
Cardholder Data Transmission .....	3
Information Security Policy/Program.....	4
<b>Payment Application Configuration .....</b>	<b>6</b>
Baseline System Configuration .....	6
Windows® XP/Vista/7 Back Office PC Security.....	6
Automatic Updates.....	6
Back Office PC User Accounts .....	6
Local Security Policy.....	6
Addressing Legacy Issues .....	7
Procedure for Removing Sensitive Historical Data .....	7
RTPOS Configuration .....	7
LogMeIn.....	9
End-User Messaging .....	9
DataCap® Products and Applications .....	9
Anti-Virus .....	9
Service Manager.....	9
Event Logging.....	10
RTPOS .....	10
PC Service Manager.....	10
Internet Applications .....	10
<b>Application Updates .....</b>	<b>12</b>
<b>Best Practices for Support.....</b>	<b>13</b>
<b>Additional Resources .....</b>	<b>14</b>

# Introduction

## Purpose

Lucas POS V4 Embedded version 4.02 (RTPOS) is a point of sale application designed specifically for the hospitality market. When integrated with a DataCap® DataTran/TwinTran or with PC ServiceMgr version 4.02 and DataCap® DSIClient/NETePay/DIALePay, RTPoS can process payment transactions and therefore is required to handle sensitive cardholder information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (PCI DSS). The security requirements defined in the PCI DSS apply to all members, merchants, and the 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.

## PCI DSS

The following 12 high level 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 RTPoS and ServiceMgr in a PCI compliant environment.

## Maintenance

This document meets all of the current PCI DSS requirements published in the *PCI Payment Application Data Security Standard 1.2*. This and future revisions of the *Lucas POS V4 Embedded Secure Implementation Guide* are available for download at <http://www.lucaspos.com>. This document will be reviewed and updated annually, whenever the application is updated, or whenever the PA-DSS is updated to ensure it stays current with the changing card payment industry.

# **PCI DSS Payment Application Requirements**

## **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 cannot 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/TLS at 128 bit, and/or WPA2
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values, encryption keys) 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, instant messaging or text messaging 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.

A simplified high-level diagram of an expected network configuration for a web based payment application environment is included below:

## Application Updates

The PCI DSS requires that Software vendors must establish a process for timely development and deployment of security patches and upgrades, which includes delivery of updates and patches in a secure manner with a known chain-of-trust, and maintenance of the integrity of patch and update code during delivery and deployment.

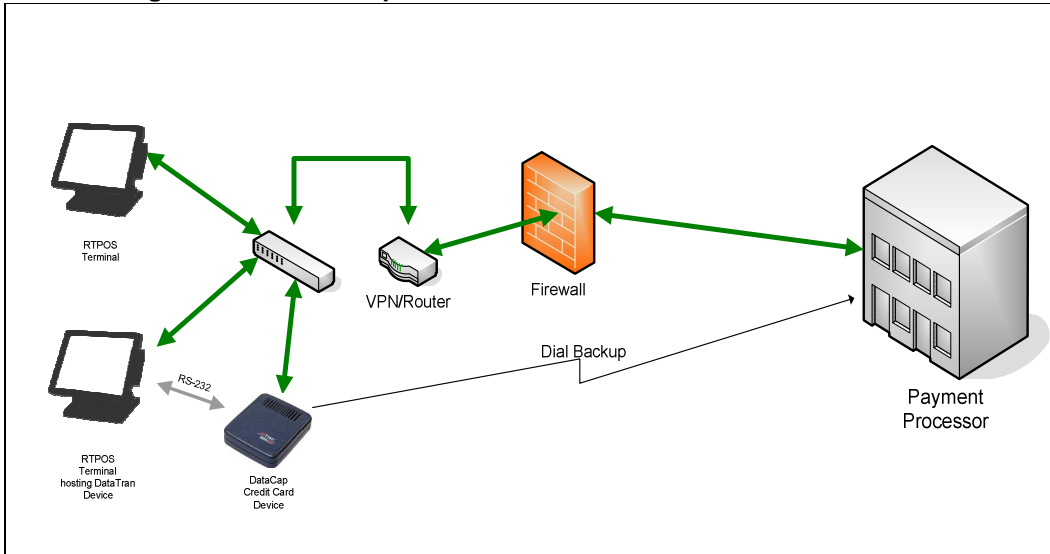
## Cardholder Data

The current version of the Lucas POS V4 Embedded system does not store cardholder data.

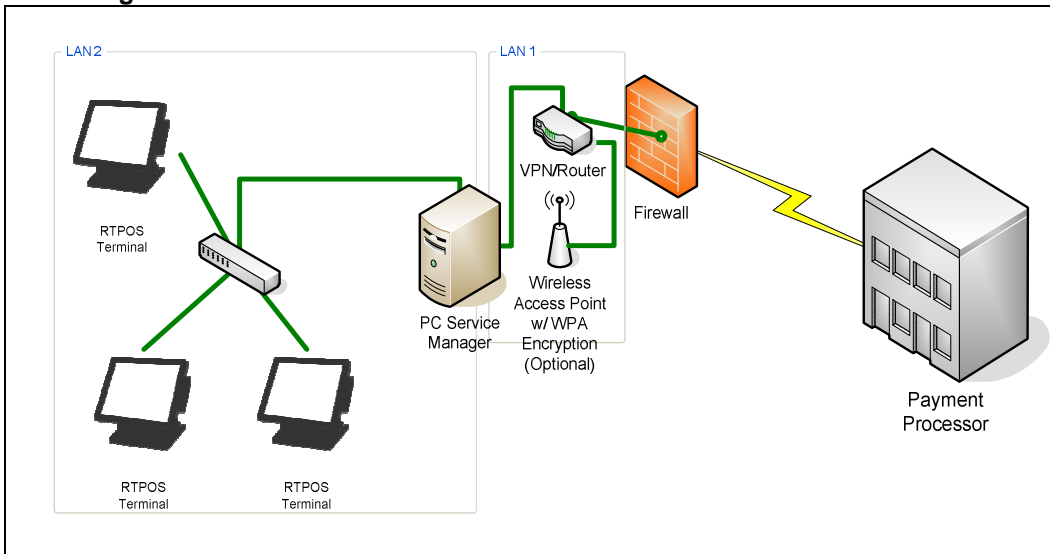
## Cardholder Data Transmission

The Lucas POS V4 for Windows system uses secure encryption transmission technology for data transmission of cardholder data over public networks via Datacap hardware / software devices which utilize non-configurable RSA key negotiation and RC4 symmetric payload encryption.

**RTPOS Integrated with DataCap® DataTran/TwinTran**



**ServiceMgr on Back Office PC**



**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

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance:

### Back Office PC (Optional)

- Microsoft Windows® XP Professional or Microsoft Windows® Vista or Microsoft Windows® 7. All latest updates and hot-fixes should be tested and applied.
- 1GHz Processor minimum
- 512 MB of RAM minimum, 1 GB or higher recommended
- 200 MB of available hard-disk space
- 100 Mb Ethernet LAN card

### Network Peripherals

- VPN Router for remote access

## Windows® XP/Vista/7 Back Office PC Security

### Automatic Updates

To ensure that the operating system is always kept up to date with the latest security patches, ensure that Automatic Updates is enabled on the Windows Back Office PC. It is recommended that the Automatic option be enabled which will automatically download and install the updates as they come available.

### Back Office PC User Accounts

Name	Group	Purpose
Administrator	Administrators	Full access for owner
Support	Administrators	Full access for dealer
Manager	Standard Users	Limited access
Assistant1	Standard Users	Limited access
Assistant2	Standard Users	Limited access
Assistant3	Standard Users	Limited access

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 **Local Security Policy** for more information on strong passwords.

### Local Security Policy

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

#### Password Policy:

Enforce Password History - Set to remember the last 4 passwords.  
 Maximum Password Age - 90 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

## 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 and therefore must be deleted. If prior data is not securely removed from the system during a PCI-compliant upgrade, the system will not be considered compliant.

Legacy versions of RTPOS and Service Manager do not store any key material and therefore do not require removal during migration.

## 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.

## RTPOS Configuration

This section describes the settings necessary to ensure that the RTOS application is configured properly in a PCI compliant environment. A properly configured (compliant) system must adhere to the following user authentication rules for administrative accounts:

- Do not use default administrative accounts for payment application logins
- Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts.
- Use secure authentication for the payment application and system whenever possible.
- Users must have a unique username
- Users must authenticate with a password
- Users must not authenticate with group, shared, or generic passwords
- Passwords must contain at least 7 characters
- Passwords must contain both numeric and alphabetic characters
- Passwords must expire after no more than 90 days
- Passwords must not be the same as any of the last 4 used
- Accounts must lock out after no more than 6 failed attempts
- Accounts must remain locked out for no less than 30 minutes or until an administrator enables the user ID
- Accounts must timeout and require password re-entry after no less than 15 minutes

*Not requiring unique usernames and secure authentication will result in non-compliance with PCI DSS.*

The Lucas POS V4 for Windows application handles incorporates the above user authentication rules as follows:

- 1.) Default administrative accounts are never used by the system.
- 2.) Secure authentication is used by default by sensitive functions. These settings can be changed by the end-user but should always remain enabled for proper compliance. See the Function Setup section below for details.
- 3.) The system is configured to use password authentication for administrative access by default (also known as Access Control). Access Control can be changed by the end-user but should always remain enabled for proper compliance. See the System Setup section below for details.
- 4.) The system automatically requires a unique user name for each user, a minimum of 7 characters in the password, both numeric and alphabetic characters, and different passwords from the last four used. These settings cannot be changed by the user.
- 5.) Thresholds for expiration of access codes, number of failed logins, locked out time, and idle timeout can be changed by the end-user but should always stay set to the default settings for proper compliance. See the System Setup and Job Code Setup sections below for details.

The following WinPOS settings are configurable by the end-user and must be set to the specified value in order to be compliant:

**System Setup**

Field	Value	Description
Access Control	Yes	Enables access control throughout the POS application
Access Code Age	90	Number of days that an access code is valid
Failed Logins	6	Number of consecutive failed logins before the account is disabled
Disable Time	30	Number of minutes that an account is disabled following an excessive number of failed login attempts
Journal Lines	5,000	Number of lines in stored in the electronic journal

**Jobcode Setup**

Field	Value	Description
POS Auto Logout	900	Idle time logout Set to 900 seconds (15 minutes)
PGM Auto Logout	900	Idle time logout Set to 900 seconds (15 minutes)

**Function Setup**

The following functions should have the Access Control flag enabled in Function Setup. This will force an Access Code to be entered by the operator prior to accessing these functions. Anyone who does not possess an access code will be denied access to these programming modules.

Function
Function Setup
Employee Setup
Jobcode Setup
System Setup
Network Setup
Enable VNC

<b>Function</b>
Enable SMB

### **Employee Setup**

Anyone with access to sensitive areas of program mode will be required to have an Access Code password in his employee record. Initially, an employee's access code must be entered through the Employee Setup module. Once an employee has an access code programmed in his employee record, the system will prompt for a new password when the current password expires.

### **Virtual Network Computing Setup**

To prevent unauthorized remote access, Virtual Network Computing (VNC) must be activated by an authorized person at the merchant location. This is performed by executing an RTPOS function that activates VNC. A second function is available to disable VNC. When these functions are executed, an event is written to the Electronic Journal or Application Event Log. During a VPN/VNC session, the customer should monitor activity and disable VNC as soon as the session terminates.

## **LogMeIn**

A Lucas-managed LogMeIn service is used to provide a secure remote control connection between Lucas Systems and the merchant location. Log Me In works by establishing a SSL-secured connection between the client (Lucas) and the host (merchant) through a LogMeIn gateway server. The remote connection is always initiated by the host (merchant) from inside the firewall, and the firewall handles it as an outgoing connection. The LogMeIn service does not use a listener for incoming connections originating from outside the firewall.

## **End-User Messaging**

RTOS and Service Manager do not send cardholder data via end-user messaging technologies such as email, instant messaging, SMS text, etc.

## **DataCap<sup>®</sup> Products and Applications**

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

DataCap's DataTran<sup>™</sup> and TwinTran<sup>™</sup> send all cardholder data across public networks using SSL. DataCap's DSIClientX and NetEPay<sup>™</sup> send all cardholder data across public networks using RSA Key Negotiation and RC4 Symetric Encryption.

## **Anti-Virus**

In installations where a Back Office PC is present, anti-virus software must be installed on the 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.

## **Service Manager**

In order to access configuration mode in the Service Manager, the current user must be logged in with an account that has Administrative rights (See section Windows<sup>®</sup> XP/Vista/7 Back Office PC Security).

## Event Logging

The PCI DSS requires that payment applications make implement an automated audit trail to track and monitor access. RTPOS and PC Service Manager applications use event logs to record events that are related to

- Actions taken by all administrative users
- Successful and Failed Login attempts
- Payment processing settings
- Access to payment records
- System startup
- Changes to user account permissions
- Changes to Event Log settings
- Access to and Resetting of Event Logs

Information recorded in the individual event log entries should include when possible

- User identification
- Type of event
- Time stamp
- Success or Failure of the event
- Origin of the event
- Name of the affected resource

**NOTE:** Failure to properly configure event logging will result in Non-Compliance with the PCI DSS.

## RTPOS

RTPOS events are logged into the electronic journal. Ensure that the [Journal Lines] setting in System program mode is set to a value adequate to keep transactions for an entire day. The Sales Z process will back up the Electronic Journal. The electronic journal can be printed by

Utilities => Print Journal

*By default RTPOS events are always logged into the Electronic Journal, this functionality cannot be reconfigured or disabled.*

## PC Service Manager

Service Manager security events will be logged to the Windows® Event Log in the Application Log and are identified by the source "CCServer Admin". The event log can be accessed in

Control Panel => Administrative Tools => Event Viewer

*By default Service Manager events are always logged into the Windows Event Log, this functionality cannot be reconfigured or disabled.*

## 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 RTPOS and Service Manager applications do not provide internet services, and do not require that any internet service 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 Back Office PC running Service Manager.

## ***Application Updates***

Deployment of application updates for Lucas POS V4 for Windows is provided directly by Lucas Systems through a secure channel. The following process is used for application updates and patches:

- 1.) Update files will be stored on and transferred to / from a secure FTP (FTPS) server.
- 2.) A unique validation code that is keyed to the file contents will be generated for each update file at the time it is built.
- 3.) The unique validation code will be communicated in a separate Release Announcement document
- 4.) A Lucas Systems representative will transfer the update file to the target restaurant on the date scheduled with the merchant. At the appointed time, the update file will be transferred to each POS terminal in preparation for installation.
- 5.) Each time an update file is transferred to a POS terminal the validation code reported by the installation process will be checked against the validation code published in the Release Announcement. This comparison will be done manually by the person installing the update and if the validation codes do not match the update will be aborted.

## ***Best Practices for Support***

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

## ***Additional Resources***

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

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

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

[http://usa.visa.com/merchants/risk\\_management/cisp\\_tools\\_faq.html?it=12/merchants/risk\\_management/cisp\\_merchants.html|Tools and FAQ](http://usa.visa.com/merchants/risk_management/cisp_tools_faq.html?it=12/merchants/risk_management/cisp_merchants.html|Tools and FAQ)

A list of qualified security assessors from VISA is available at the following internet address:

[http://usa.visa.com/merchants/risk\\_management/cisp\\_assessors.html?it=12/merchants/risk\\_management/cisp\\_tools\\_faq.html|Assessors](http://usa.visa.com/merchants/risk_management/cisp_assessors.html?it=12/merchants/risk_management/cisp_tools_faq.html|Assessors)

Windows and Windows XP/Vista/7 are registered trademarks of Microsoft Corporation, Inc.