



L-POS

PCI implementation guide for L-POS

Copyright © 2008 Logivision

Logivision has attempted to make this document accurate. Logivision is not responsible for any direct, incidental, or consequential damages resulting from this documentation or inaccuracies within. Specifications are subject to change.

Printed in Canada

Contents

Introduction 5

- Document revision 5

What is PCI? 5

- What does PCI mean to me? 6

Secure Network Requirements 6

- L-POS Windows User Account 8
- L-POS Directories and Access 8
- WAN Setup / External Connections 9
- Wireless network settings 9

Remote access security 10

- Use SSL for secure data transmission 13
- Email encryption 13
- SSH, VPN, or SSL/TLS for encryption of administrative access 13

Credit Card Data handling 13

- Removing historical data and cryptographic key material 13
 - Removing historical log file data 14
 - Removing historical electronic journal sensitive card data 14
- Encryption and non-compliant historical data 15
- Never store cardholder data on internet-accessible systems. 15

Log settings 15

Access control 17

- Recommended setup of the SQL Server user account 17
 - Database User access 17
- L-POS Operators: Roles and Rights 18
 - Operator Passwords 19
 - Passwords Never Expire 19
 - Password encryption 19
- Modifying default application operator 19

Reporting Security Breaches 20

Maintaining Secure Systems 20

Notification of New Patches 20

Delivery of updates 21

Clearing Out After Testing 21

Introduction

Logivision provides this implementation guide to assist resellers and end-users in meeting the PABP recommendations related to securing the point of sale system environment and application data. You must follow the recommendations of this guide to minimize the risks associated with card processing and other sensitive data handling. It is up to the dealer/integrator and the end-user to ensure that the requirements outlined in this guide are implemented at the store. Failure to do so will result in the loss of PCS-DSS compliance.

You can reasonably expect your reseller to implement the software and other components of your system to ensure PCI compliancy. Notwithstanding the above, it is the ultimate responsibility of the end-user to verify that the requirements and recommendations of this guide have been followed.

Failure to maintain a PCI compliant environment may result in fines, penalties, restrictions, and financial responsibility for misused cardholder information.

For the latest information on PCI/DSS requirements contact Visa, or visit their web site at www.visa.com.

This document outlines requirements for creating a PCI compliant environment for the L-POS, EzScan or Symphony software only; the user is responsible for knowing and adhering to all additional PCI requirements beyond those addressed within this document.

Document revision

This guide will be reviewed with each new release, whenever PCI DSS requirements change or at least once a year and may be modified to ensure the recommendations remain current with the requirements of the PCI data security standards. Please check the Logivision website documentation area to obtain the latest version of the document. End-users must obtain the documents from the reseller who installed the system. This document will also be distributed with the application and can be found in the C:\LBOSS folder of L-BOSS server and workstations.

What is PCI?

PCI DSS stands for Payment Card Industry (PCI) Data Security Standard (DSS). Adherence to the PCI standards is a requirement to become CISP compliant. The Cardholder Information Security Program (CISP) was initiated by the Visa card company to create a set of standards for securing cardholder information. To perform Visa transactions, all merchants, products and processing environments must be CISP certified.

What does PCI mean to me?

To meet PCI requirements, the environment in which L-POS is deployed must be properly configured. L-POS and its supporting applications have been made compliant with PCI standards, but for the entire system to properly maintain the required security for cardholder information, specific further setup is required.

This document is designed to define the methods of deployment for the L-POS product and its supporting applications that uphold PCI requirements and best practices. The information contained in this document defines the responsibilities of the user to create and maintain a PCI compliant environment for the L-POS software.

Failure to maintain a PCI compliant environment may result in fines, penalties, restrictions, and financial responsibility for misused cardholder information. For the latest information on PCI/CISP requirements contact Visa, or visit their web site at www.visa.com.

This document outlines requirements for creating a PCI compliant environment for the L-POS software only; the user is responsible for knowing and adhering to all additional PCI requirements beyond those addressed within this document.

N.B. Throughout this document the use of the trademark L-POS refers to the entire suite of Logivision software applications delivered to the store. They include L-POS, L-BOSS, EzScan, Symphony and Symphony PRO.

The L-POS software version 3.0.1.4 and greater has been updated to be PCI compliant, but the environment into which it is installed has an impact on the safety and security of cardholder information that L-POS utilizes to process transactions. Although L-POS V. 3.0.0.0 and greater does not allow users to record, display or store any sensitive cardholder data your installation must meet the PCI-DSS requirements. Data and physical security are the responsibility of the end user; for the production environment to be fully PCI compliant the following requirements must be met.

Secure Network Requirements

L-POS should not be installed on servers that provide a different network function than payment processing; this means that L-POS can be installed on the same system that runs the POS back office, or other payment applications, but should never be installed on systems that perform network functions such as DHCP, DNS, routing, web services etc.

Make sure that virus scanning software is present within the payments environment. PCI requirements state that virus scanners be up to date, active, and be capable of writing log files.

PCI implementation guide for L-POS

PCI requirements state that all software in the payments environment must have the latest security updates and that all security related updates be installed within a month of their release.

The PCI standard 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 and/or devices should be removed/disabled/renamed if possible, or at least should have complex passwords and should not be used.

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and at least one upper case and one lower case alphabetic character
- Passwords must be changed at least every 90 days
- New passwords cannot be the same as the last 4 passwords

Below are the other PCI account requirements beyond uniqueness and password complexity:

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

The Local Area Network requires both physical and electronic security. It is the responsibility of the Merchant to provide appropriate physical and electronic security to protect customer card information. This section covers some specific suggestions for LAN network security relating to L-POS.

Merchants should prevent unauthorized access to the Poswin directory on the POS lane, and to the LBOSS directory on the L-POS server. Only the L-POS Windows User Account (see next section) and valid administrators require access to the LBOSS directory. Allowing unauthorized access could endanger system information; the merchant is responsible for locking down access to the LBOSS directory and Poswin directory to prevent unauthorized or malicious changes to the program or direct manipulation of configuration files. Similarly, the Poswin directory on the POS lane should only be accessible by valid administrators.

To ensure maximum cardholder data security it is not recommended to install L-POS into a wireless networking environment. If you do install L-POS into an environment that includes wireless networking, additional requirements must be met. PCI requirements include specific instructions on the use of wireless networking within the production environment. PCI requirements section 1 (specifically 1.3.9) should be reviewed for complete information on wireless setup. The following information is provided to assist in wireless setup:

- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Wireless encryption must be in use, such as: VPN, SSL/TLS at 128 bit, WEP (Wired Equivalency Protocol) at 128 bits, and/or WPA.
- If WEP keys are changed manually, they must be rotated at least quarterly and whenever key personnel leave. For automated key rotation, keys must be rotated at least every 30 minutes.
- Do not depend entirely on WEP to secure card information; traffic across wireless networks should utilize a second method of encryption as well.
- Wireless connection points should be secured with the appropriate use of firewalls.
- Firewall/port filtering services should be placed between wireless access points and the payment processing environment with rules restricting access
- Access point should restrict access to known authorized devices (using MAC address filtering)

L-POS Windows User Account

When installing L-POS and L-BOSS, the user must log on as a Windows administrator. This allows the install process to perform actions like writing to the registry. The Windows user account must have the ability to access LBOSS and POSWIN folders:

- The Windows user requires the rights to read and write to the POSWIN and LBOSS directories and all sub directories.
- Unless the account is an administrative account, the Windows user account used to log in to perform configuration changes should not have access to any other directory that those required.
- Before installing L-POS and L-BOSS, define a separate Windows user account. This account should be a Power User, not an administrator. Do not use already existing accounts, or accounts that are installed in the operating system by default, like the Administrator account.
- L-POS Windows User Account should have a unique and recognizable name, as well as a unique and complex password.

L-POS Directories and Access

It is recommended that only administrative personnel be allowed to directly modify L-POS program files. L-POS is installed to the C:\POSWIN\ directory by default. L-BOSS is installed to the C:\LBOSS\ folder on the server by default. It is recommended to restrict access to the \POSWIN\ or \LBOSS\ folder and below to the Windows users created to run these applications. In addition it is highly recommended that the POSWIN and LBOSS directories be protected through the use of a File Integrity Monitoring System. The POSWIN and LBOSS directories contain configuration information that could potentially be altered with malicious intent. Specific vulnerable files are the INI configuration files, as these contain the IP addresses in use and could be manipulated potentially to attempt to redirect payment processing traffic. Users are responsible for monitoring file integrity with tools like the Tripwire Security Suite. File Integrity Monitoring Systems keep track

of changes to files or applications and can alert technical staff when changes are made; undesirable changes can be easily tracked and removed.

When using a File Integrity Monitoring System, be aware that certain files (typically log or database files) are constantly changing. It is often useful to either exclude these files from alerts completely, or configure the alerting software to allow the L-POS software to freely manipulate files within its directory structure, and to configure alerts for when files are directly manipulated by users or when manipulated by other software. The POSWIN and LBOSS directories and all sub-directories should be monitored by a File Integrity Monitoring System. Take care that each POS lane will have a POSWIN directory. If your daily routines include any type of system backup to other locations these locations must also be secured.

WAN Setup / External Connections

This section covers requirements for WAN setup and external connections, such as VPNs into the LAN, and connections from L-POS to the payments processing applications. L-POS and its components should never be deployed onto systems with direct internet access. L-POS software should be deployed on systems that reside behind firewalls, with communication to the processing application secured, and allowed through the firewall. The firewalls must be configured to protect information by limiting the incoming and outgoing connections to only those which are required. PCI section 1 covers firewall requirements. To successfully process payments, L-POS will require a network route to the payment processing application. It is the responsibility of the L-POS user to ensure that the connection from the payment processing application to the financial processor is properly encrypted and/or secured according to PCI requirements.

PCI Requirements state that it is necessary to use strong encryption technology such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), or Internet Protocol Security (IPSEC) to secure communications over any public network, such as the internet.

Wireless network settings.

Logivision recommends wired installations whenever possible. If you decide to implement the payment application into a wireless environment, you must respect the PCI Data Security Standards concerning wireless environments.

Install personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

L-POS, L-BOSS and its related applications do not transmit sensitive cardholder data. Notwithstanding this fact it's important that you implement the following

security in your wireless environment. For wireless networks encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology,
- VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to
- Keys
- Restrict access based on media access code (MAC) address.

Remote access security

It is recommended to advise customers that they must establish secure methods of confirming the identities of users who will be granted access to the local network. They should use an access request form that is filled out when any outside party, including Logivision personnel, need to remotely connect to a production environment system. This form should contain, at minimum, information on who is accessing the network, their contact information and the contact information of their immediate superior, the purpose of the access, and the expected duration of the access.

For remote access requests, the identity of the requesting individual should be firmly established. Establish contact with known personnel, such as the account manager or their designate that is assigned to your company. This may also entail contacting the requesting individual or company at a known telephone number or e-mail address.

Remote access accounts must be granted only to individuals; a single access account must not be given to a group of individuals for common use. Remote access should be logged in an auditable format.

Remote access is the ability to connect and interact with a remote network or computer as if you were directly connected of that remote network or computer. Full remote access implies that this access is available at will (on demand), and some level of network communication is allowed to or through a firewall.

In identifying and authorizing users for access, use of two of the three authentication methods (factors) below constitute valid two-factor authentication:

- Something you know, such as the User ID/Password combination
- Something you have, such as a Digital Certificate or RSA token
- Something you are, such as a Biometric ID mechanism.

Note that two different sets of a single method (e.g., two User ID/Password combinations) do not create a valid two-factor authentication scenario. It is also important to note that both methods of authentication must uniquely identify a specific person or user, not a group of people or users.

Traditional scenarios supported and expected for two-factor remote access include the use of User ID/Password at the network or computer level in combination with a Certificate or RSA SecureID used to authorize an encrypted VPN connection.

If you cannot justify the expense of implementing a two-factor authentication solution for remote access, there are other options available by providing connectivity needed to support customers without creating a “full” remote access solution. When considering these alternative solutions, the following principles must be addressed to ensure that the solution provides needed controls without enabling “full” remote access:

- Ensure that remote connectivity can be traced to a specific service request (this would allow identification the customer support representative and the user requesting support).
- Ensure that the solution does not allow “on demand” or “always on” access.
- Ensure the solution uses robust (at least 128 bit) encryption for all communications.
- Ensure that the solution does not allow for the exchange of credentials.
- Mandate that the customer environment must be monitored while access is enabled.
- Ensure that the connection is enabled by an outbound connection that does not require firewall port enablement.

Examples of the type of solution that can be implemented to meet these requirements include:

- **Go To Assist** (full usage tracking with unique session tokens created by customer support rep) <http://www.gotoassist.com/>
- **LogMeIn Rescue** (full usage tracking with unique session tokens created by customer support rep) <https://secure.logmeinrescue.com/HelpDesk/Home.aspx>
- **Techinline Remote Desktop** (full usage tracking with unique session tokens created by customer support rep) <http://www.techinline.com/>
- **iRemotePC Remote Support Service** (full usage tracking with unique session tokens created by customer support rep) <https://www.iremotepc.com/>
- **Go To Meeting** (tracking of meeting IDs used and persons involved need to be tracked in support tickets) <https://www.gotomeeting.com/>
- **LiveMeeting** (tracking of meeting IDs used and persons involved need to be tracked in support tickets) <http://office.microsoft.com/en-us/livemeeting/default.aspx>
- **UltraVNC** (configure to require customer to initiate access and to connect to a specific IP address or range for support connectivity, and persons involved need to be tracked in support tickets) <http://www.uvnc.com/>

Although the L-POS and L-BOSS applications do not store any sensitive cardholder data, it is still a PCI-DSS requirement that you follow these guidelines with regards to remote access. Before using any remote access software you must implement and use the remote access software security features. These are the specific requirements related to remote access to in-store systems.

- Change default settings in the remote access software and use unique passwords for each remote customer.
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication or complex Passwords for logins
- Enable encrypted data transmission
- 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
- Restrict access to customer Passwords to authorized personnel
- Establish customer Passwords according to PCI DSS requirements:
- Identify all users with a unique user name before allowing them to access system components or cardholder data.
- In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices (e.g., SecureID, certificates, or public key)
 - Biometrics.
- Encrypt all passwords during transmission and storage on all system components.
- Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
- Verify user identity before performing password resets
- Set first-time passwords to a unique value for each user and change immediately after the first use
- Immediately revoke access for any terminated users
- Remove inactive user accounts at least every 90 days
- Enable accounts used by vendors for remote maintenance only during the time period needed
- Communicate password procedures and policies to all users who have access to cardholder data
- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than six attempts
- Set the lockout duration to thirty minutes or until administrator enables the user ID

- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

Use SSL for secure data transmission

L-POS does not transmit sensitive cardholder data over the internet. Nonetheless, in accordance with PCI DSS requirement 4.1 all data transmission over the Internet should specify the use of SSL to secure the data transmission.

Email encryption

L-POS cannot send PANS by e-mail. This option is not part of L-POS, L-BOSS or its related applications. Nonetheless Logivision recommends that if any other applications allow or facilitate sending e-mail they should use the appropriate email encryption solution.

SSH, VPN, or SSL/TLS for encryption of administrative access

L-POS, L-BOSS and related Logivision application modules do not store sensitive cardholder data. Even though access to sensitive cardholder data is not possible in the L-POS, L-BOSS or related Logivision applications, Logivision still recommends the following considerations should be taken into account. For all non-console administration Logivision recommends the proper usage of SSH, VPN, or SSL/TLS for encryption of non-console administrative access.

Credit Card Data handling

According to the PABP standards several considerations should be made in regards to sensitive Credit Card data handling and storage considerations:

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

No sensitive card data is stored by Logivision's point of sale software versions 3.0.0.0 and greater. Although we have minimized the risk of data compromise, it is still necessary to follow the credit card data handling to ensure that the environment is compliant to PABP and PCI requirements.

Removing historical data and cryptographic key material

The PABP approved versions of L-POS, L-BOSS and related applications do not store any sensitive cardholder data. Versions previous to release 3.0.0.0 of L-POS may

have stored limited card data. This data may be present in the electronic journal transaction logs (EJ) and/or in the system debug log files (log files). It is the responsibility of the user/dealer/integrator to ensure that this sensitive card data and any cryptographic key material have been removed. L-POS did not use any cryptographic keys to mask or encrypt the data. Not cleaning this data compromises the compliance of your system to the PCI-PABP DSS requirements.

Removing historical log file data

All system debug logging files that contain sensitive card data must be deleted from each POS terminal in the store.

- It is not sufficient to simply delete the debug log files. For old versions where cardholder data may have been stored Logivision recommends using either SDelete or Eraser clean removal tools to ensure proper removal of all files and sub-folders under the C:\Poswin\Log folder of the POS terminal. Sdelete can be obtained from <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>. Eraser can be downloaded from <http://www.heidi.ie/node/14>.
- Refer to operation instructions to ensure that you have securely removed and wiped the disk space.

Removing historical electronic journal sensitive card data

It is possible that your system stored card numbers in the electronic journal if it was installed before 2006. In this case you will need to remove the card numbers from the files or securely delete the files from your system. Not cleaning this data compromises the compliance of your system to the PCI-PABP DSS requirements.

EJ files that contain sensitive card data must be processed to remove such sensitive data. Logivision provides an EJ conversion utility that will process the existing EJ files to mask any card sensitive data from the EJ files.

- Copy the RemoveInfoEj.exe program to the LBOSS folder of the terminal that contains the sensitive cardholder data.
- Copy the RemoveInfoEj.Ini file to the same LBOSS folder.
- Edit the RemoveInfoEj.Ini file using a text editor like Notepad.
- By default the program will search for credit card numbers by locating the title of the field as it was printed on the customer receipt. Normally the title was: "Card number:" The RemoveInfoEj.Ini is already programmed to search and clean card numbers per the default settings. Otherwise you will need to change the text of the INI file to match the title of this field in your journal files.
- Execute the RemoveInfoEJ.EXE.
- Press the Start button to process the electronic journal files.
- Review the transaction data that you have cleaned to make sure all sensitive card data has been purged.
- If any sensitive card data remains you must repeat this procedure until no sensitive card data can be found.

- It is your responsibility to execute this process in order to ensure a PABP compliant installation.
- You may also decide to simply remove all the old journal files from your system. If you prefer to remove the journal files rather than converting them we recommend that you use the Sdelete or Eraser application to securely clean all files and subfolders found under the LBOSS\Office\Journal folder of the L-BOSS server. Sdelete can be obtained from <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>. Eraser can be downloaded from <http://www.heidi.ie/node/14>
- Refer to operation instructions to ensure that you have securely removed and wiped the disk space.

Encryption and non-compliant historical data

L-POS, L-BOSS and related applications do not use encryption to store sensitive cardholder data. Previous versions of the software did not use encryption to store sensitive cardholder data. Although out of the scope of this document, Logivision nonetheless recommends that other software used in your store must be PCI compliant and PABP approved.

Never store cardholder data on internet-accessible systems.

L-POS, L-BOSS and its related applications do not store sensitive cardholder data. But if you could retain or store cardholder data on a server connected to the Internet, you must not store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

Log settings

L-POS, L-BOSS and related Logivision application log settings are not configurable by the user or dealer / integrator. No sensitive cardholder data can be found in the L-POS or L-BOSS log files.

Nonetheless, PCI recommends that a review of log files occur daily. If a security breach of another nature is discovered it may be important to know who was accessing the L-POS and L-BOSS applications, even though these applications do not store any sensitive cardholder data. It is therefore recommended that the log files be reviewed for unauthorized user activity. This review can be accomplished by searching for specific text relating to unauthorized activity. The system tracks access to the L-BOSS application through the LBOSS.Log file located in the install directory of the L-BOSS application.

Example Log line:

2008-04-08 11:38:32.359 Cashier login: Programmeur

The log file can be searched for all User Access Logging by performing a text search on 'Cashier login:' and then each access can be individually evaluated. No access to sensitive cardholder data is provided in the L-BOSS log files.

The system tracks access to the L-POS application in the Poswin\Log\YYMM\POS.log file of each point of sale device. Each day a new log is created for that day's activities on each POS terminal. No administrative access can be performed inside the POS application. No access to sensitive cardholder data can be gained through the L-POS application or in its log files. Critical POS activity is captured in the POS.log file, but this does not include any sensitive cardholder data. All application access is tracked in this file.

Example log line:

```
08-06-13 10:07:58.777 CON: MailSlot sending:  
192.168.0.255,003001,998,29,9031,M,,MB,'Login cashier','Programmer'
```

The log file can be searched for all User Access Logging by performing a text search on 'Login cashier' and then each access can be individually evaluated.

Log File Vulnerability

These files are vulnerable to direct manipulation by L-POS users that have the permission to enter the LBOSS or POSWIN directories and make changes. This could allow the deletion of the logs that detail unauthorized access. However since no access to card information is available the vulnerability of the log files will not result in any cardholder data security breach.

Nonetheless, due to the vulnerability of the log files, it is highly recommended that access to the LBOSS and POSWIN directories be severely limited to only those users that have a business need to directly access L-POS and L-BOSS configuration, log, and program files. Additionally, it is recommended that additional software be run that will log access to specific files.

Log File Vulnerability

These files are vulnerable to direct manipulation by L-POS users that have the permission to enter the LBOSS or POSWIN directories and make changes. This could allow the deletion of the logs that detail unauthorized access. However since no access to card information is available the vulnerability of the log files will not result in any cardholder data security breach.

Nonetheless, due to the vulnerability of the log files, it is highly recommended that access to the LBOSS and POSWIN directories be severely limited to only those users that have a business need to directly access L-POS and L-BOSS configuration, log, and program files. Additionally, it is recommended that additional software be run that will log access to specific files.

It is your responsibility and that of your customer to secure data on the system as described. Not doing so could result in data compromise and loss of PCI-DSS compliance.

Access control

L-POS, L-BOSS and related applications do not store any sensitive cardholder data. Nonetheless administrative access to data must be restricted by unique usernames and complex passwords. This access restriction does not apply to cashiers operating the POS application who may need to enter card information in the course of a normal point of sale transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application. No parameter settings available within Logivision's applications permit either storage or printing of sensitive card data from Logivision's applications. Even though L-POS and its related applications do not store any sensitive cardholder data we have enforced the use of complex passwords for backend administrative access to the L-BOSS software according to PCI DSS requirements.

PABP requires controlled access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data. Logivision software versions 3.0.0.0 and greater do not store any sensitive cardholder data. Nonetheless Logivision recommends that you take care to secure access to administrative functions and databases used for all applications.

Recommended setup of the SQL Server user account

PCI requirements specify that database programs such as SQL Server cannot run under the default administrator account supplied in the program. A new user must be created who does not have administrator rights. PCI requirements state that you must assign a complex password to the login account you create.

The program supplied with L-POS to install SQL Express (a royalty-free version of Microsoft's SQL Server) assigns a user automatically to the L-Boss database. The default database name is LogiDB. If you installed a different SQL Server version you will need to ensure that you do not use the default SA account to run the application. In following PCI guidelines, Logivision recommends that you create a new login account. Under the login properties of this new account the Database role membership must be set to db_owner for the LogiDB database.

It is also required that you assign a complex password to the default "SA" account, or that the default account should be replaced by another administrator account with a complex password. In no case should you connect to the database server using the default SA account.

Database User access

Here are considerations to make in respect to database user settings:
Do not use the default database "sa" user for database access rights.

You should delete the default "sa" user or to rename and assign a complex password.

You must assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts.

You must assign strong application and system passwords whenever possible.

- 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

You must control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

L-POS Operators: Roles and Rights

Operators are user accounts for the L-POS and L-BOSS software. Some accounts will allow the configuration of L-POS and L-BOSS settings. The examples below indicate typical user configurations of rights. These examples limit the available rights of each user account to only those rights required to fulfill their function. Only the Administrative user illustrated below is expected to need to configure L-POS and L-BOSS settings.

L-POS User Types:

User level 7: Programmer (Administrative User)

User level 6: Owner.

User level 5: Manager

User level 4: Assistant manager

User level 3: Clerk

User level 2: Cashier

User level 1: store specific

User level 0: No user.

Level 7 Programmer - Administrative User – User with full access to all L-POS and L-BOSS features and functions. At least one administrative account must exist in each L-POS and L-BOSS installation. Administrative Operators must possess all rights to be able to create other accounts with those rights, as well as perform L-POS and L-BOSS configuration setup. Since an Administrative Operator possesses all rights, access to an administrative operator should be restricted to only those personnel who require the ability set up L-POS and L-BOSS and to make configuration changes.

All other user levels are configurable as required in the store specific environment.

Owner –Typically will have access to all system functions, but will not have access to system settings such as peripherals management, configuration menus, etc.

Manager – Normally will be restricted from some reporting, or system control functions.

Assistant Manage - Normally will be restricted from some reporting, system and register control functions.

Clerk – Typically store personnel with limited access.

Cashier – Will be restricted in control functions on the till with no backend system rights.

New user - Will be restricted in control functions on the till with no backend system rights.

No user - Will be restricted in control functions on the till with no backend system rights.

There must be no 'universal' accounts. This means that no account name and password combination should be defined on multiple L-POS or L-BOSS systems with the intention that the account information be available to more than one person. Do not create an account at multiple locations with the intention to make it a 'default' account that all administrators can log onto, for example.

It is permissible to create the same account on multiple systems, so long as that account's information (username and password) is maintained by a single individual and is not available to anyone else.

Limit L-POS and L-BOSS operators to only those personnel necessary. The fewer personnel with access, the more secure the system can be. If a user must be given access, grant only those operator rights necessary to fulfill their assigned role. If a user that is assigned an Operator account is terminated, immediately remove the assigned Operator account. If the user has accounts on multiple L-POS installations, their Operator account information must be removed at each location.

Operator Passwords

The L-BOSS application enforces PCI required operator password requirements for user levels 4 and greater (8 character password minimum, 1 capital letter, 1 number). Additionally, the maximum number of days that the password may remain unchanged is 90 days; any login after the set duration will prompt for new password. A password may not be the same as any of the previous four passwords used for that Operator.

Passwords Never Expire

Users of previous versions of L-BOSS are familiar with the fact that Operator account passwords never expired automatically. PCI requirements state that passwords must be changed at least every 90 days.

Password encryption

L-BOSS uses Blowfish with SHA-512 to encrypt user passwords.

Modifying default application operator

On a fresh installation of L-BOSS, the default operator's login name is 7, with an original password of Password1. While during the first login the password must be changed from the default, it is also recommended that the login name be changed to something other than 7.

Follow the steps below to change the default Operator's Name.

1. After logging in to L-BOSS, go to Maintenance | Register | Operators.

2. Select the 7 Account; change the User Name, and Full Name and save the changes.

Reporting Security Breaches

If it is known or suspected that L-POS or its components are breached, contact Logivision immediately.

Maintaining Secure Systems

It is up to you the reseller to advise your customers of the need to maintain the systems they are operating up to date. You must ensure that critical updates for the operating system, database engine, anti-virus and other store applications are obtained and installed regularly, in no case more than one month after release of the updates. We recommend that you subscribe to a service that can help you identify and remedy vulnerabilities. One such source of information are weekly newsletters from the SANS Institute who free distribution to subscribers. Please go to www.sans.org for more information. Logivision also recommends that you conduct tests regularly to validate the end to end functionality of the operating system, or other applications running in the store. You should obtain software designed to test this functionality. One source that you can try is with Sophos who provide many tools with free 30 day evaluation licenses for this type of end to end testing. Go to www.sophos.com for more information.

Notification of New Patches

Software updates and patches are made available to all L-POS users. Logivision cannot individually contact all software users. Logivision's software patches are distributed via the reseller network. If a software patch is released, Logivision will post the patch to its secure reseller website. It is therefore recommended that all resellers of the L-POS software periodically check the web site to determine if any new security related patches are available. It is highly recommended that all resellers keep their customers' L-POS system up to date by acquiring the latest L-POS patches. It is recommended that L-POS Users receive patches through a known and trusted chain of personnel. This will ensure authenticity and that the received patch is the most recent.

Logivision delivers security related patches within 30 business days after notification of the security breach. The patch will be made available to all Logivision users; Logivision will post a notice on its public web site (www.logivision.com) about such a patch, but cannot individually contact all software users. It is therefore recommended that all users of the L-POS, Symphony or EzScan software periodically check the web site to determine if any new security related patches are available. Logivision can also be contacted directly to request current patch information.

Delivery of updates

If you perform or deliver updates via remote access to customer networks:

- ◆ You must use 2-factor authentication for remote access.
- ◆ As per PCI Data Security Standard 12.3, you must secure the use of modem and wireless style communication devices as follows:
- ◆ You are required to develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. You must ensure these usage policies require the following:
 - ◆ Explicit management approval must be obtained prior to connecting to remote networks.
 - ◆ You must set the proper authentication required for use of the technology
 - ◆ You must create a list of all such devices and personnel with access
 - ◆ You are required to label devices with owner, contact information, and purpose
 - ◆ You must implement update delivery only with acceptable uses of the technologies.
 - ◆ You must define acceptable network locations for the technologies
 - ◆ You must include a list of company-approved products
 - ◆ Automatic disconnect of modem sessions after a specific period of inactivity
 - ◆ Activation of modems for vendors only when needed by vendors, with immediate deactivation after use
 - ◆ L-POS and its related applications do not store any sensitive cardholder data. Nonetheless, if you access cardholder data remotely via modem, your remote connection policies must prohibit storage of cardholder data onto local hard drives, floppy disks, or other external media. The policy must prohibit cut-and-paste and print functions during remote access.

Logivision recommends that all customers and resellers/integrators should use a personal firewall product if a computer is connected via VPN or other high-speed connection, to secure these “always-on” connections, per PCI Data Security Standard 1.3.10.

Clearing Out After Testing

Given the nature of our business and our role, Logivision does not use production systems in-house. But a reseller may use a production system to validate functionality both before and after delivery to the customer. In this case it is important that all test data be cleared out of the production system.

To avoid problems Logivision recommends using the “training mode”. In training mode no data is stored for the transactions entered. Training mode does not allow credit or debit transactions.

PCI implementation guide for L-POS

If you have entered live transactions (other than training mode) into the production system they need to be removed before going live. Logivision recommends that you use a clean wipe tool like SDelete to remove the data accumulated during the testing. Sdelete can be obtained from <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>. Refer to operation instructions to ensure that you have securely removed and wiped the disk space. The following folders need to be securely cleaned:

Clean each POS terminal that contains test data:

Use SDelete to remove all transaction files under C:\Poswin\Journal.

Use SDelete to remove all report files under C:\Poswin\Silback.

Use SDelete to remove all log files under C:\Poswin\Log.

Clean data from L-BOSS server:

Use SDelete to remove all transaction files under C:\LBOSS\Office\Journal.

Use SDelete to remove all report files under C:\LBOSS\Office\Processed\Sales.