SPOT Business Systems, LLC

PCI – DSS IMPLEMENTATION GUIDE

11/11/2010

Table of Contents

Introduction

As a business entity that processes credit cards, in terms of both getting authorizations as well as processing sales, you are required to be compliant with the 'Payment Card Industry Data Security Standard' (PCI DSS). There are several levels of PCI DSS compliance. One criterion is the number of credit card transactions processed in a year. You need to review the compliance documentation at https://www.pcisecuritystandards.org and take the necessary steps to obtain and maintain your appropriate PCI DSS compliant status.

By SPOT Business Systems, LLC being PCI-DSS compliant, we support your PCI DSS compliance. Our being PCI-DSS compliant does NOT make you PCI-DSS compliant.

The PCI DSS consists of 12 Requirements that cover the handling, processing and storage of credit card data:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

This Implementation Guide explains your company and SPOT Business Systems' role in the security of your customers' credit card data; instructs you and your network administrator how to enable security settings in regards to both your network and hardware; instructs you on secure SPOT product implementation; and defines some of your responsibilities for meeting PCI DSS requirements.

Following these guidelines does NOT make you PCI DSS compliant, nor does it guarantee your network's security. It is your responsibility, along with your network administrator, to ensure that your hardware and network systems are secure from internal as well as external intrusions.

SPOT makes no claims on the security of your network, nor of your level of being PCI DSS compliant.

One of the most vulnerable areas for credit card data is within what is referred to as 'legacy data'. Legacy data includes, but is not limited to SPOT installations on computers no longer in use, backups on old computers, backups on old zip disks, and backups on other storage devices. In addition, any stored paper records that contain credit card data, including but not limited to paper based customer information sheets, credit card on file agreements, register receipts and reports. Legacy SPOT data may be found on existing SPOT installations, not running the PCI-DSS compliant version.

Appendix A to this Implementation Guide details what EVERY existing company MUST do to securely delete this legacy data from their systems. Once the data has been securely deleted, you must then have your network administrator use a wipe tool to scrub the unused space to make it unreadable and unrecoverable.

Anytime SPOT has been installed at your company, you were required to follow SPOT's system specifications (see Appendix B). You must review the current specs and have your network administrator verify that your SPOT network meets them. Changes the network administrator will need to make include adding in unique user names and complex Windows passwords for ALL the employees as well as other password restrictions. There are probably other changes which need to be made to bring your system to SPOT's current specs. Following SPOT's specs does NOT make you PCI DSS compliant; however, it contributes to your PCI DSS compliance as it includes sections on security issues such as user passwords and setting up a secure network. SPOT's System Specifications can be found at http://www.SPOTpos.com and are also attached as Appendix B to this document.

This Implementation Guide is organized by the PCI-DSS requirements which SPOT must meet to be PCI-DSS certified. In many cases, the measures you need to take have already been discussed and detailed either by the Data Security Letter(s) and/or the SPOT System Specifications. It also references the PCI DSS (Version 1.2 Release: November 2008) and the Appendixes.

Keep this Guide in a safe location for future reference. This Guide will also be posted on http://www.SPOTpos.com . SPOT will issue updated pages and/or sections as required.

Once you have read through this Guide; have had your network administrator make all necessary changes on your computers, network, and SPOT data; and you have taken the additional necessary steps such as formulating, maintaining and adhering to an in house security policy, you MUST sign and fax, mail or email back the signature page found at the end of this document. If you email, the address is markj@SPOTpos.com. Please include the full company name, your name and position in the email.

Requirement Details of PCI DSS Compliance

1 - Do Not Retain Full Magnetic Stripe, Card Validation Code or Value (CAV2, CID, CVC2, CVV2) or PIN block data

The magnetic stripe on the back of a credit card contains sensitive data including the cardholder's name, Primary Account Number (PAN), expiration date and other information necessary to process the card for an authorization and/or sale. The card validation code or value is either 1) the 2 or 3 digit number embedded in the magnetic stripe or 2) the 3 or 4 digit number next to the signature field on the back of a card or on the

front of an American Express card. A PIN (Personal Identification Number) is used when a debit card is used as a debit transaction rather than a credit card transaction.

Since May 2007, SPOT's credit card interface has been certified by Payment Processing, Inc that we meet their specifications and we are certified for transactions on the 'Gateway II" interface. Payment Processing, Inc and its 'Gateway II' is "a real-time payment gateway between merchants' point-of-sale systems and their bank/processor". By processing customers' credit cards through Payment Processing, Inc, the credit card number is kept by SPOT in the SPOT data base in an encrypted format.

Truncation is when a cardholder's PAN has been substantially replaced by X's. For example, XXXXXXXXXXXX4957 is a truncation format used when viewing and/or printing a customer receipt or reviewing reports in SPOT; 5474XXXXXXXX4957 is a truncation format used by Payment Processing, Inc for a stores Gateway II transaction review and reporting purposes. SPOT requires ALL properties that have the SPOT data capture interface use Payment Processing, Inc as the company's payment gateway.

When a credit card is used within the SPOT client for an authorization or sale it is either swiped through a magnetic card reader or the number and expiration date are manually entered. It is then sent by the SPOT client to Payment Processing, Inc's Gateway II (GWII) which encrypts the number and transmits it to Payment Processing, Inc. Payment Processing, Inc processes the card authorization and/or sale and returns the number in encrypted format to the GWII interface session on the SPOT client in a encrypted format. The full magnetic stripe data is not kept on your hardware and the information returned by Payment Processing, Inc GWII are of no value to a thief.

If you have ANY questions regarding Payment Processing, Inc's Gateway, its security and/or compliance, you must contact your Payment Processing, Inc representative directly.

When a credit card number is manually entered into the POS for an authorization and/or sale, the staff has the ability to include the card's validation code or value as well as the billing address's zip code. If the card's code and/or value is entered, neither are retained anywhere within the SPOT POS. (PCI DSS Req. 3.2.2) They are passed to Payment Processing, Inc who uses them only to further validate the card. They are not returned to the POS once an authorization or sale has been obtained.

A debit card's PIN and/or PIN block data is one of the most dangerous numbers to retain. The SPOT POS does not support pin based debit transactions. SPOT's credit card interface does not allow for the processing of debit cards as anything other than a credit card therefore transmitting the PIN is not possible. (PCI DSS Req. 3.2.3)

SPOT versions prior to Version 4.10.0120 could retain the PAN and expiration date in an un-truncated format within the SPOT database as well as on database backups. Beginning with SPOT version 5.0.0005, the SPOT follows PCI DSS specifications for storing and reporting PANs and expiration dates. (PCI DSS Reqs. 3.2-3.4)

Existing SPOT installation may have legacy data on computers, removable media or on paper. Legacy data includes, but is not limited to, neglected and/or forgotten SPOT backups and/or SPOT POS databases on computers that have been replaced; data copied to perform computer upgrades or to set up additional stations; and data copied for system maintenance. All of this data is outside of the SPOT active data and poses a security risk if not found and securely deleted.

You MUST investigate and locate all the computers where a customer's credit card information may still be within past backups and/or copied SPOT data. This may include, but is not limited to, employee laptops at their home, retired PCs, and/or computers that have been relocated at the company.

Once all the computers have been located, your network administrator MUST read and follow the steps in Appendix A to this Guide - Legacy Data Secure Deletion. The Appendix lists places within a computer

where SPOT's POS data may reside, where log files are held, and where/what other files need to be found and securely deleted. Once the deletion is complete, your network administrator must scrub the drives using a wipe tool. Eraser http://www.heidi.ie/eraser/ (free) and CyberScrub's Privacy Suite v.5.0 http://www.cyberscrub.com/ (cost) are two (2) products some of our clients have used.

Not completing these steps to securely delete all legacy data and cryptographic key material and then scrub the unused space makes the store NON-PCI DSS Compliant.

Legacy data also includes neglected and/or forgotten backups, and/or SPOT data on stored zip or other removable media. It is your responsibility to locate this legacy media. Once found, they must be securely stored or destroyed per your company's data retention policy and security policy. (PCI DSS Reqs. 3.1, 9.10) "Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility." (PCI DSS Req. 9.5) One way to destroy removable media such as zip disks is to reformat them and then scrub the magnetic surface. You can also physically destroy the media by drilling a hole through the magnetic surface and/or taking them apart to expose the magnetic disk which must then be cut with scissors.

It is your responsibility to research and locate ALL the places where a customer's full PAN may still be outside of residing on computers or other electronic media. It is considered legacy data and must be securely stored and/or destroyed. (PCI DSS Req. 9.10)

You MUST develop and maintain written policy and procedures for all your credit card data retention and disposal. (PCI DSS Req. 12) You must limit the retention and storage time to "that which is required for business, legal, and/or regulatory purposes". (PCI DSS Req. 3) Data storage MUST be kept to a minimum both in terms of duration as well as the physical amount. Those limitations must be part of your data retention and security policy.

Depending on your company's credit card on file policy, a credit card imprint or manually written PAN information may have been taken at signup or during the course of a customers visit. This imprint may be on paper based agreements or other forms that are retained after a customer signup or visit. All of this information is considered legacy data.

Legacy and current hard copy data, if kept and stored for legitimate business purposes, must be in a safe and secure location. Access to this data must be strictly controlled and monitored. (PCI DSS Req. 9) An example would be once the customer has filled out a new customer form; the signup form must be kept under lock and key by the company. In this example, you must also have a log for the access key, a procedure to monitor who has access to this stored data as well as how the data is handled. (PCI DSS Req. 7, 9 and 10)

As per your written security policy, all data containing credit card information, especially un-truncated PANs, must be securely deleted and/or destroyed when the time limit has been reached. If the credit card data is in paper form such as an imprint on a customer signup agreement, one way to destroy it is to cross cut shred it. (PCI DSS Req. 9.10) All electronic media must also be destroyed when it is no longer needed.

It is imperative that your written security procedures be maintained and updated as necessary. In addition, they must be part of new employee training and management changeovers. (PCI DSS Reqs. 12.1, 12.5, 12.6) It must include policies on who has access; logging and monitoring access; logging 'incidents'; as well as the proper wiping, deleting and/or destroying of the data.

There may be instances when you need to retrieve a customer’s full credit card number and expiration date. Depending on the situation, you will get the card number and expiration date from within the SPOT POS.

The SPOT POS has the ability to show an unencrypted credit card number only on an existing customer and only to specific staff. View ability is based on user permissions which are set by company management

through the POS' User, Groups and Rights configuration. All views of unencrypted credit cards numbers held in the POS are logged by SPOT's event log. You must limit the number of staff who has access to this data. When setting up your users in SPOT and Payment Processing, Inc, only those employees with a 'need to know' should have access to read full card numbers, process refunds, etc. (PCI DSS Reqs. 7.1, 9)

Although you may need to access a customer's PAN and expiration date after a completed transaction, it must only be accessed for the time it takes to complete your task. If it is necessary to write down the PAN, it must be securely deleted after use. Two easy ways to accomplish this are to use a dry erase board and/or if you have the credit card information in a paper form, crosscut shred the paper.

SPOT support staff or an integrator will only transfer required data for specific troubleshooting. The data is transferred to a known location with limited access. The backed up data being transferred is already in an encrypted format. In addition, the credit card numbers within the data are already truncated or encrypted. Once the data has been used, it is securely deleted.

When trouble shooting hardware or software issues you must not maintain sensitive authentication data (pre authorization) must only be collected when needed to solve a specific problem.

2 - Protect Stored Cardholder Data

SPOT's POS' responsibility is to make sure that any PAN is masked when displayed, but can be displayed "to those employees and other parties with a specific need to see full PAN." (PCI-DSS Req. 2.1) The PAN is unreadable anywhere it is stored. The POS stores credit card PANs using encryption. (PCI DSS Reqs. 2.1-2.2)

The SPOT POS' encryption keys are managed in the SPOT POS configuration utility. They are protected by the user groups and rights configuration, when properly set up, prevents access by any network user or any user of the same computer without the correct credentials. (PCI DSS Req. 2.4)

Encryption keys and log ins are controlled by company management. When the credit card encryption key has expired, or on demand, an administrative user can invoke the key manager program and generate generate new keys, re-encrypt every cc number in the data set, and install the new key. This key must be changed at least once a year, or when any compromise of the key is suspected. (PCI DSS Req. 3.6)

You must change the encryption key of your Company Setting interface at least once a year or when the possibility of a security compromise has occurred. The encryption key is used to protect cardholder data transmitted over the Internet. These keys are used in conjunction with an AES 256 encryption algorithm to store card and user data in the data base.

It is your responsibility to 1) protect stored cardholder data (PCI DSS Req. 3); 2) restrict access to cardholder data (PCI DSS Reqs. 7 and 9); and 3) develop and maintain a strong information security policy for employees and contractors. (PCI DSS Req. 12)

3 - Provide Secure Password Features

Per SPOT's System Specifications (Appendix B) and a requirement for your PCI DSS compliance, every employee who has computer access must have a unique user name and password. (PCI DSS Reqs. 8.1, 8.2) Your network administrator must set up every network user with a unique user name and complex password for logging onto Windows on the computer(s) they will be using during their shift.

User names must always be unique and cannot be any vendor supplied default. (PCI DSS Req. 2.1) The users must NOT have Windows administrative rights. Any Windows user account with administrative rights

MUST also have an additional account that is used day-to-day with non-administrative rights. All Administrative users are advised to not use the account or have the account disabled.

Windows passwords must be 'complex' in that they must contain at least 7 characters and include both letters and numbers. Passwords can be even more secure by including upper and lower case and/or symbols. (See Appendix B and PCI DSS Section 8.5 for additional Windows password requirements)

Every employee using the SPOT POS must have a unique user name and password that is used when they log into an SPOT session. You cannot have duplicate user names or initials. Individual user permissions are based on groups within SPOT. SPOT passwords must be at least 7 characters and contain at least one number and one letter. In addition, they can contain at least one uppercase letter, one lowercase letter, and a special character (i.e. punctuation). The user name and password should follow at least the same rules as other users and passwords you have set up on your network. (PCI DSS Req. 8.5)

Setting up a user's log in name and password SPOT should be done before training begins. Do NOT set up or use any default SPOT user accounts or passwords. (PCI DSS Req. 8.5.8) A manager must have two (2) user accounts in SPOT: one for everyday use and another to administer user names and passwords within SPOT's User Groups and Rights configuration.

You must establish, maintain and follow a written password policy. All employees must be trained and kept current with your security policies. Procedures must be established to change all users' passwords, in both Windows and in SPOT on a regularly scheduled basis, at a minimum, every 90 days.

SPOT's users' passwords expire after 90 days and have to then be reset. They cannot use any of the past four (4) passwords. If a SPOT POS user fails to log into a workstation 6 times, they will be locked out of that terminal for 30 minutes. Rebooting the terminal does not shorten the timeout of this feature. (PCI DSS Reqs. 8.5.8 -8.5.15)

When an employee leaves your employment, you must delete ALL their users in Windows immediately. In SPOT disable the account immediately. (PCI DSS Req. 8.5.4) Take any other steps necessary depending upon the access the ex-employee had, such as changing locks on storage areas used for storing credit card data.

Your company's written security policy must include your rules regarding users, passwords and access to ALL credit card data whether it is on the current SPOT database; within Payment Processing, Inc; on removable backup media; and/or paper.

SPOT advises all its customers and resellers/integrators to apply these password guidelines to ALL systems, PCs, servers and databases that contain payment applications and/or cardholder data.

4 - Log Application Activity

The SPOT POS automatically updates activity logs of transactions done within SPOT. The log includes the logged user's initials, date, time, transaction detail, transaction number, computer station and a completed or failed status for each transaction. These are part of the activity log process and are available for detailed reporting. (PCI DSS Req. 10.1 - 10.3)

SPOT's POS activity logs will log those events that affect security including each time a staff member logs into SPOT, successful or not; when an employee views an un truncated credit card PAN and expiration date; as well as actions taken by a SPOT POS administrator. These logs cannot be disabled. These logs are accessible only to SPOT POS administrators or DB administrators with access and understanding of these tables.

Credit card debug logs are generated during a credit card transaction. These logs are enabled by default. Turning off the credit card debug logging in your operation is not allowed under PCI compliance guidelines and will cause your implementation to be none PCI compliant.

Windows keeps its own separate logs. When setting up your computer network, your network administrator must enable the Windows logging function. Your network administrator must also familiarize you with these logs: where they are kept, how to maintain them, and how to read them, etc.

5 - Develop Secure Applications

This section of the PCI-DSS Requirements applies to SPOT Business Systems, LLC and how we write, develop, test and implement our software application. It is important you are made aware of how the POS is developed, tested, released and implemented to aide you in complying with PCI DSS Req. 6.

All upgrades to the SPOT POS client, server and/or interface applications are tested in house by our QA department per their test plans prior to being released to our clients as either a beta or a production version. (PCI DSS Req. 6.4) If necessary, 'test only' credit cards, issued by Payment Processing, are used during testing. No 'live' credit card numbers are used.

Development, testing and production are separate departments at SPOT. Any new code comes from development to QA. QA oversees the testing of the new code. Once satisfied, QA then passes it to the production/tech department for implementation into production environments. (PCI DSS Req. 6.3) The code that is passed from QA to tech to be implemented in the field is an executable file. No test data is given to the production/tech departments.

Before a new company is put online with SPOT POS, a database is created from an Installation / Configuration form filled out by the company as part of our installation process. We start with a default database and build their configuration and dataset based on the information provided on the Installation and Configuration form. No test or individual customer credit card information is used when creating the company's dataset.

When a new version is implemented at stores, the Owner/Manager is advised they can go to http://www.SPOTpos.com for the version release notes. They can also find any documentation on new features as well as training videos.

6 - Protect Wireless Transmissions

If ANY non-SPOT workstations are wirelessly connecting to your network, they MUST be configured to meet or exceed the following specifications: encrypt the transmissions by using WiFi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS; and 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 values.
- 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.

Your network administrator must verify that the wireless technology has been protected with personal firewall software. The firewall software secure configuration must not be alterable by the employee. All vendor defaults, including keys, must be changed at installation and whenever the person knowing the key leaves or changes positions; SSID broadcast is disabled; default SNMP community strings are changed; all access point passwords are changed; enable WPA or WPA2 if possible.

7 - Test Applications to Address Vulnerabilities

This section of the PCI-DSS refers to SPOT's internal processes to keep up to date on potential security risks to the SPOT program and credit card data.

We subscribe to several Internet alert services, including the SANS Institute, Microsoft, BZ Media (Software Test & Performance), Tech Republic and ComputerWorld. (PCI DSS Req. 6.2)

If any possible threats are found to the SPOT application, they are investigated, patched, tested and deployed to our customers in a 'timely' manner. All updates are delivered securely via two-factor authentication and through our internal 'chain-of-trust'.

It is your responsibility to do the same for your network including having your network administrator run regular network scans to check for any intrusions and/or unauthorized access attempts. (PCI DSS Req. 11)

8 - Facilitate Secure Network Implementation

Per SPOT's Specs, you must have certain security tools in place. These tools include, but are not limited to, an external hardware firewall, anti-virus software and traffic filtering devices.

Updates to these entities such as your Windows operating system, anti-virus program, etc. need to be managed, monitored and installed. (PCI Reqs. 5.2, 11.4) Be sure your network administrator installs these tools and trains management and staff on their use, management and maintenance.

Having these security tools implemented on your network computers does NOT interfere with the SPOT POS server, client or interface applications when they are properly configured. (PCI DSS Reqs. 1, 3, 4 and 5)

9 - Cardholder Data Must Never be Stored on a Server Connected to the Internet

Credit card data processing is sent to Payment Processing, Inc in an encrypted format to their data center where it is processed and then returned to SPOT.

The SPOT installation must NEVER be put on a server and/or computer that are directly facing the outside public Internet. At a minimum a physical hardware firewall must be configured between your SPOT server/workstations and the internet.

10 - Facilitate Secure Remote Software Updates

SPOT's Specs require that the computer running SPOT's POS program must have high speed Internet access. Examples of such broadband services would be: DSL, T1, or Cable Modem". SPOT does not access stores via a dial-up modem.

Your server must be secured behind your hardware firewall per SPOT's specs. (PCI DSS Reqs. 1.3.9 and 12.3.9) Proper configuration of the firewall will allow access only to those approved vendors/persons/entities. Any other stations must also have at a minimum a personal software firewall installed and properly configured in a secure manner.

When SPOT support staff access your system to install updates to the SPOT POS, we access the server / stations using Citrix GOTO Assist and two-factor authentication. The two-factors are an encrypted software solution (GOTO Assist) as well the remote user initiating the connection.

11 - Facilitate Secure Remote Access to Application

Per PCI DSS Req. 8.3, two-factor authentication must be used whenever ANYONE accesses your network remotely. Two-factor authentication requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors.

For all remote access, you MUST use and implement remote access software security features such as requiring a unique user name; authenticating all users; changing all default settings; enabling lockouts; enabling data encryption; enabling logging; allowing connections only from specific (known) IP/MAC addresses; and establishing customer passwords according to the PCI DSS requirements. (PCI DSS Reqs. 8.1, 8.2, 8.4, 8.5)

PCI compliant use of all remote stations must be part of your company's security policy. (PCI DSS Req. 12.3)

Neither the SPOT server nor the SPOT client programs interfere with outside entities using two-factor authentication to access your network.

SPOT support sessions are facilitated by a remote service called Citrix GOTO Assist.

Support sessions to our customers can be conducted in the following ways:
1- Customers can initiate an SPOT support session by visiting "help.SPOTpos.com" from a browser on the station they are working at, and entering a 7 digit pin code our support agent will provide them over the phone. That pin is only good for five minutes or the start of the remote session
2- A SPOT support agent may email a link to the customer.
3- The client software may be permanently installed on store computers, such as dedicated server computers, or others.

12 - Encrypt Sensitive Traffic over Public Networks

SPOT relies on Payment Processing, Inc's ‘Gateway II’ to securely transmit payment card data over open/public networks.

The POS has the ability to send customer reminders for expired cards, statements and declined credit card transactions via email. However, even if the email is formatted to send the credit card number used in the transaction, it is sending only the last four digits of the PAN.

You must NEVER include any full payment card information in an unencrypted email. (PCI DSS Reqs. 3, 4.2) If you must send account information via email, use an encryption solution such as PGP.

Not sending unencrypted PANs via email must be part of your company's security policy and procedures. (PCI DSS Req. 12.2)

If you are not using the Payment Processing, Inc's Gateway II you will be responsible for PCI compliance with the credit card processing provider. *If the payment application allows data transmission over public networks, examine PA-DSS Implementation Guide prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use secure encryption transmission technology.*

13 - Encrypt All Non-console Administrative Access

In order for all non-console administrative access to be encrypted, you MUST use technologies such as SSH, VPN or SSL/TLS. (PCI DSS Req. 2.3) If you have SPOT remote stations, they must use Terminal Services or other PCI DSS compliant remote access services or devices. (See Appendix B for SPOT's specs on Terminal Services)

By default, Windows Server 2003 Terminal Services uses 'high' level of encryption, which encrypts data transmission in both directions using a 128-bit key. Your network administrator should use this default level.

14 - Maintain Instructional Documentation and Training Programs for Customers, Resellers, and Integrators

SPOT's website for our customers is http://SPOTpos.com . It contains the following: SPOT's System Specifications; a link to our interactive training videos; training documentation our clients can view or print; and the Release Notes (under the 'Customer Care > Documentation > Release notes' menu) that we provide for each version and/or update.

Prior to installation or upgrade, a copy of this Implementation Guide will be provided to the company. A signature page is also provided to verify receipt and understanding which will need to be returned to SPOT Business Systems, LLC with an authorized signature

This Implementation Guide can also be found at http://www.SPOTpos.com . It will be reviewed and updated at least on a yearly basis, even if any new SPOT versions/updates do not require it.

Signature Page

Once you have read through the attached Implementation Guide, please fill out the information below and email to markj@spotpos.com or fax back to SPOT Business Systems, LLC at 801-495-1208, Attn: Mark Jones

By signing this signature, I state that I have read and understood the attached Implementation Guide and all its appendices produced by SPOT Business Systems, LLC. I understand that this signature page will be kept as part of my Client File at SPOT Business Systems, LLC.

_____

Company Name Phone

_____

Company Owner (signature) Date

_____

Company Owner (print) Email Address

_____

Company General Manager (signature) Date

_____

Network/Hardware Administrator / Company Name

_____

Network/Hardware Administrator Contact Phone

Security Disclaimer

The SPOT Licensee (Customer) acknowledges that no computer system or software can be made completely secure. The information and instructions detailed below do not guarantee the safety or security of your store's e-commerce network, or information transmitted or stored on this application. In addition, following these steps does NOT make the Customer PCI DSS compliant although it does support your effort to become compliant. Not completing these steps to securely delete and then wipe all legacy data makes the store NON-PCI DSS compliant.

The secure deletion of SPOT POS legacy data MUST be performed by the store's network administrator on EVERY store computer. The access, retention, storage and deletion of other forms of legacy data are the company's responsibility and must follow your written policy. (PCI DSS Reqs. 3.1, 7.1)

The purpose of performing these steps is to securely delete all legacy data that contains credit card data, such as a cardholder's Primary Account Number (PAN) from all network computers. You must also insure that any legacy cryptographic keys are securely deleted. This secure deletion and then wiping are requirements of PABP. (Reqs. 1.1.1 - 1.1.4)

Legacy data includes, but is not limited to, neglected and/or forgotten data on stored zip or other media backups; data on computers that have been replaced; data copied to perform computer upgrades or to set up additional stations; and data copied for system maintenance.

Legacy data also can include imprints of credit cards taken at check in; faxes with credit card guarantee information; and/or hard copies of past reports including night audits.

This document addresses legacy data, which is not part of the POS's active data that may reside on any of your computers.

The Customer's network administrator should use caution when performing the secure data deletion and wiping. If the Customer or network administrator is in doubt about any step, please contact SPOT technical support at (925) 284-1005 or SPOT president Gary Gibb at (925) 871-1801.

Background

The SPOT scheduler has integrated features for purging old data backups, but the automated purging process only works on the backups in specific directories on the SPOT server or the SPOT station #1. A common and dangerous practice when doing a computer hardware upgrade is to use an existing computer as temporary storage for a copy of the old files. When the new computer is installed on the network, the old files are bulk copied to the new computer but rarely are the files wiped from the temporary storage computer. Such actions compound a legacy data problem because the end result is that multiple computers have legacy data on them. The solution is to securely delete any legacy data before any other data is transferred. You must then wipe the storage computer's disk once the transfer is complete.

When your company was updated to SPOT's Version 5.1 and the encryption tool is run, data within the active SPOT dataset was encrypted. It is the Customer's responsibility to follow the instructions detailed below to ensure that no legacy data resides on ANY computer (server, computer or laptop) outside of the active SPOT dataset.

File Removal Basics

If you need to log onto a computer with administrative rights in order to access and securely delete data you MUST log off when you are done to prevent others from using the computer with administrative rights.

When you are finished removing files from a given computer, you MUST include all users' Windows recycle bins in a wipe of the system. Windows will automatically re-generate a recycle folder when needed in the future.

When you have securely deleted all legacy data from a computer, you MUST wipe the drives using a wipe tool program. Two programs that some of our Customers have used are eraser http://www.heidi.ie/eraser/ (freeware) or CyberScrub's Privacy Suite v.5.0 http://www.cyberscrub.com/ (purchase). These tools 'wipe' or overwrite data in the computer's unused or empty space to make it unreadable.

SPOT's Data Conventions

A Customer only has one active working SPOT dataset. It resides on the company's SPOT server computer (be it dedicated or non-dedicated). It is always within a directory called 'c:\program files\SBS\data' located on one of the SPOT server's root drives.

To protect against data loss, compressed backup copies of the active dataset are automatically created whenever the scheduler processes. Dataset backups are comprised of compressed files called SPOT1.zip, SPOT2.zip SPOT3.zip

All compressed backup files should reside ONLY on the SPOT server and on station #1, within specific directories (...\SPOT\backup). They should always be current, less than one month in age. No other computer should have ANY uncompressed or compressed SPOT data files.

Uncompressed COPIES of a SPOT database and compressed SPOT zip backups more than 1 month old must always be securely deleted wherever and whenever found.

Your network administrator MUST perform an all-inclusive search to locate all POS database copies. One way is to search is: at the command prompt on each local drive's root directory (e.g. c:\, d:\, etc.) type: dir spot*.zip /s /p or spot*.bak /s /p. This will show you all directories where data.zip or SQL backup files reside, and possibly where other encrypted or unencrypted legacy data files are. All copies of these files must be securely deleted.

For station #1's that are standalone, or peer-to-peer, the automated backup files in c:\program files\SBS\backup should not be older than one month.

For computers that are part of a dedicated server network, the directory c:\program files\SBS\backup should be entirely deleted. Do NOT delete c:\program files\SBS\DATA on the SPOT dedicated server.

Appendix B - SPOT System Specifications

SPOT's goal is for your company to have a reliable and secure SPOT POS installation. To ensure all SPOT POS functions and capabilities perform as specified, please follow these steps.

Your network set up and installation MUST comply with the 'Payment Card Industry Data Security Standard' (PCI DSS) version 1.2 Release: November 2009. The PCI DSS includes, but is not limited to: the firewall; anti virus programs; user accounts and their permissions; and physical and network access to the server.

You must make sure your computer/hardware/network administrator follows best practices with regards to network security and has, at a minimum, either a Microsoft Certified Systems Administrator (MCSA) or Microsoft Certified Systems Engineer (MCSE) certification. Keep a copy of their certificate with your other papers concerning your network. If you change network vendors/administrators, you should get a new certificate. Having this credential does not give assurance of Information Technology (IT) competency, but it is a good indication that your network administrator has at least a working knowledge of network basics. While MCSA is an SPOT minimum requirement, the preferred level of certification is MCSE.

SPOT Business Systems, LLC requires the purchase of business grade computers. This is important because the company operates 24/7 and many of the computers, and especially the SPOT server, will also be running 24/7. Consult with your hardware vendor to determine the appropriate computers for your company. It is also recommended that you select a hardware vendor who can provide support of the computers, network, operating system and other software during the hours your company will need such support.

SPOT technicians will NOT install the SPOT software on computers that do not meet SPOT's specifications, which can delay an installation and increase costs. To avoid costly repairs and delays PLEASE BE ABSOLUTELY SURE your hardware vendor reads and follows the Implementation Guide and SPOT's specifications, you order the correct equipment from your vendor, and your vendor delivers and properly installs the equipment you ordered.

General Installation Requirements

1. For Windows XP systems, the Implementation Guide specifies that System Restore Points must be disabled and includes instructions on how to disable them. To disable the restore points on a Windows XP computer follow these steps.

    1. Steps to turn off System Restore

    2. Click Start, right-click My Computer, and then click Properties.

    3. In the System Properties dialog box, click the System Restore tab.

    4. Click to select the Turn off System Restore check box. Or, click to select the Turn off System Restore on all drives check box.

    5. Click OK.

    6. When you receive the following message, click Yes to confirm that you want to turn off System Restore:

7. You have chosen to turn off System Restore. If you continue, all existing restore points will be deleted, and you will not be able to track or undo changes to your computer.

8. Do you want to turn off System Restore?

9. After a few moments, the System Properties dialog box closes.

10. Steps to turn on System Restore

11. Click Start, right-click My Computer, and then click Properties.

12. In the System Properties dialog box, click the System Restore tab.

13. Click to clear the Turn off System Restore check box. Or, click the Turn off System Restore on all drives check box.

14. Click OK.

15. After a few moments, the System Properties dialog box closes.

16. Back to the top

2. High Speed Internet Access is required. Examples of acceptable broadband services would be: DSL, T1, or Cable Modem.

3. External Hardware Firewall. (PCI DSS Req. 1) This is a dedicated device placed between your Internet connection and Local Area Network (LAN). It is not sufficient to rely exclusively on personal software firewalls co-resident on your LAN. Examples of software firewalls are: Windows Firewall, ZoneAlarm, BlackIce and Panda. If present, software firewalls must be configured to allow SPOT internal LAN traffic.

4. SPOT support uses a product called Citrix GOTO Assist, which will need ports open for the store staff to get out on the Internet to initiate a support session. See Section 6 – Support, under Installation below for the necessary ports.

5. 100 / 1000 Base T Network Switch made by one of:
   - o 3Com http://www.3com.com
   - o HP http://www.hp.com
   - o CISCO http://www.cisco.com (including Linksys http://www.linksys.com)
   - o Dell http://www.dell.com

In addition:

1. All equipment must be connected to mains power via a surge suppressor or an uninterruptible power supply (UPS) of sufficient capacity. All surge suppressors used should be supplied with an insurance policy.

2. All system clocks must be synchronized. (PCI DSS Req. 10.4) This is also imperative for the Best Western 2 Way Reservation Interface.

All Computers

Note: Dedicated servers have additional requirements that override those given here.

1. Windows XP Pro OS, Service Pack 2 or higher
2. Intel Pentium III or compatible processor, 600 MHz minimum
3. 2 Gig RAM (minimum)
4. Video Card capable of supporting a display resolution of 1024 x 768 with 256-bit color.
5. Monitor with resolution of 1024 x 768 minimum. If it is a touch screen monitor, a serial or USB port may be needed for the touch screen to operate. Monitors may NOT be shared.
6. Keyboard and mouse
7. 100mb/sec or Gigabit Network Interface Card (NIC)

   Intel, http://www.intel.com or
   Broadcom http://www.broadcom.com/products/brands/NetXtreme

8. Anti-virus software. The software must be current, actively running and set to generate assessment logs. (PCI DSS Req. 5.2) It should also be capable of detecting, removing and protecting against other malicious software such as adware and spyware (PCI DSS Req. 5.1).
9. Set screen savers and computer lockout to require a user to re-enter their password to re-activate the terminal if it has been idle for more than 15 minutes. (PCI DSS Req. 8.5.15)
10. SPOT's Video Training modules require speakers or headphones for full use. (Speakers may not be necessary on all computers; just those that the company wants their staff to use SPOT's training modules on.)
11. Must have unique user names and passwords for ALL users. (PCI DSS Req. 8) (See Installation instructions below for more details on users and password requirements)
12. A browser MUST be installed in order for staff to see reports within SPOT.
13. If the Internet is blocked on computers, you MUST allow access to esupport.SPOTpos.com to allow the company to get support from SPOT. Staff will also need the ability to download an applet for the support session. You should also consider allowing access to www.SPOTpos.com and www.mySPOTpos.com.

Dedicated Server (Local Installation)

SPOT recommends that ALL companies to have a dedicated network for SPOT POS usage. If you are an existing SPOT client and do not have a dedicated SPOT POS network, consider switching to one. It will provide better security and system dependability. A dedicated server network can better support strong

enterprise-level enforcement of operating system, anti-virus and anti-spyware updates, while keeping user stations restricted to non-administrative access.

If your computer set up is one or two computers, then you do not have to have a dedicated server. However, if you have three (3) or more stations you MUST have a dedicated server network.

SPOT's specifications for the SPOT dedicated server are:

Note: If a specification is listed above for ALL computers, then it also applies to the dedicated server, unless a variation and/or addition is listed below.

1. Microsoft Windows Server 2003 operating system. You can use Windows XP Pro OS ONLY if the server network has three or fewer SPOT stations.

2. Intel Pentium IV or compatible processor.

3. CD-ROM or DVD drive

4. 20GB Disk storage available for SPOT. It is highly desirable that redundant (RAID 1 or higher) disk storage be used. It may be SCSI or Serial ATA.

5. A server class Smart UPS with messaging enabled.

6. A serial parallel port extender as specified above may be required depending on how many serial interfaces the company is purchasing.

7. The server must not share a keyboard, mouse or monitor with a workstation.

8. Speakers are not necessary for a dedicated server.

9. If the company is getting the credit card interface through SPOT, they MUST use Payment Processing, Inc, a payment gateway.

10. Station #1 and any station designated as a backup station #1

If you have an SPOT dedicated server, Station #1 is your main SPOT station. If you only have 1 or 2 stations and are opting to not have an SPOT dedicated server, then Station #1 will also act as a non-dedicated server. In both cases, Station #1 is usually located at the front counter. These are additional requirements for Station #1 (and the designated backup #1 only)

1. 100 GB Disk storage

2. Removable backup media

3. UPS

Credit Card Data Capture Security Requirements

ALL stores that process and/or transmit confidential credit cardholder data, regardless of whether or not they process credit cards through SPOT MUST comply with the PCI DSS Requirements found at: https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf A summary of the current requirements are:

1. Install and maintain a working firewall to protect data
2. Keep security patches up-to-date
3. Protect stored data
4. Encrypt data sent across public networks
5. Use and regularly update anti-virus software
6. Restrict access by "need to know"
7. Assign unique ID to each person with computer access
8. Do not use vendor-supplied defaults for passwords and security parameters
9. Track all access to data by unique ID
10. Regularly test security systems and processes
11. Implement and maintain an information security policy
12. Restrict physical access to data

If a company is integrating credit card processing through SPOT, they MUST USE Payment Processing, Inc, a third party payment gateway provider. For Payment Processing, Inc pricing and ordering contact Joy Calkins, Payment Processing, Inc. sales manager. She can be reached at 8200 Central Avenue, Newark, CA 94560 or by phone at 800-774-6462 ext 3642 or at jcalkins@paypros.com

Notes:

SPOT does not endorse other application programs such as Microsoft Office or system services such as IIS, MSSQL, and cannot determine whether or not they may cause any incompatibilities.

If you choose to run other programs on a computer that is also running SPOT, you may need to increase RAM and disk capacities.

The primary front counter computer (Station #1) and the SPOT dedicated server, if you have one, are critical computers. Most stores require these computers to function 24 hours a day, seven days a week. These computers are responsible for creating a proper database backup of store data.

Business grade computers and other business grade components must be used throughout the system. Consumer grade computers as found in many discount stores are NOT suitable. Computers with Windows XP Home or Media edition pre-installed are not business grade computers.

Installation Specifications

1. Network

While this section is aimed at dedicated server networks, the SPOT POS program is a client/server application. Even on a single computer, many parts of SPOT act as a network. Please make sure you cover all portions of this section.

It is the responsibility of the merchant to establish, ensure and maintain their own security in regards to not only the physical access to computers but to the data and in particular, the credit card data through the network.

To view a PDF of our Network Topology, go to http://www.SPOTpos.com

A. Cabling CAT 5E (Minimum) - Cabling is the most critical part of any network. SPOT requires that all network cabling be wired to the Category 5E (minimum) specifications as defined by the EIA/TIA-T568-B standard.

   If the company already has cabling in place, have your network administrator scan the line with a 1 GB CAT 6 Cable Certification Scanner. If the cabling passes at CAT 5E performance or better, have the administrator sign off on the scan certification and retain it at the company. If not, then make the necessary changes.

   Sub-standard cabling is very difficult and expensive to diagnose. Many times it will start out fine and decay over time. When it does have problems, the problems may mimic other types of software and hardware problems.

   SPOT requires that the entire cabling hardware AND installation specifications be followed. This includes, but is not limited to:

      The quality of the cable

      RJ-45 Patch Cords must be used to connect the actual computers to the jacks and patch panel.

      Cable runs must avoid appliances that can cause interference such as florescent lights.

      Jacks and the Patch Panel are to be clearly marked and a wiring diagram posted at the server.

B. Wireless - Wireless connections to the SPOT network segment must NEVER be used.

   If your company has ANY type of public wireless Ethernet accessibility it MUST be on a separate network segment. In addition, you MUST follow PCI DSS Reqs. 1.3.8-1.3.9, 2.1.1 and 4.1.1. These requirements include but are not limited to configuring a perimeter firewall to deny traffic from any public access wireless environment to the SPOT Client environment; not using any default WEP keys; not using any default passwords; and enabling WPA technology, if applicable. (See Section 6 of the Implementation Guide for more information)

C. Network Switch - SPOT requires the network to be at least 100 Base T. The network switch must be plugged into the UPS so it will continue to function during a power outage.

D. Power, UPS and Smart communications - Computers will not run without power, and will not run well without proper power.

   Like cabling, clean power is critical! Each computer must have clean power. The file server must have a dedicated line with an isolated ground.

   Server/Station #1 must have a battery backup (UPS). Make sure all components of Server/Station #1 are plugged into the battery. (CPU and monitor. Laser printers may overload a UPS and therefore should not be plugged into it.) Printers should be plugged into a surge protector. Some UPSs have surge protector outlets that are not UPS protected.

   The SPOT dedicated server requires a UPS with Smart messaging software. All components (CPU, Monitor, Network Switches ...etc) must be plugged into this UPS. APC and PowerChute have proven to be reliable and our staff is familiar with these products.

   As batteries age, the amount of power and the amount of time they can provide emergency power declines. The typical life expectancy is about 18 months. This life expectancy can be substantially shortened if the battery is used often. Depending on the quality of the power in your area, you may want a larger capacity UPS and may even need to consider installing a line conditioner to assure that the power is clean.

E. Server Location - The SPOT server must not be located in a heavy traffic area. It should be in a well ventilated, easily accessible but locked cabinet or rack. As your credit card data is transmitted through the server, you MUST restrict and control physical access to the server location. (PCI DSS Req. 9.1)

F. Server Operating System (If dedicated on a network of three (3) or more computers) - Must run Windows 2003 Server Edition, as a Primary Domain Controller. Set it to automatically download updates so the system always has the latest updates and patches. (PCS DSS Req. 6) Installation should be managed by your network administrator.

G. User Accounts - Administrator(s)

   Create an Administrator user with a unique user name and complex/strong password. Do NOT use any vendor supplied defaults for any system passwords or other security parameters. (PCI DSS Req. 2)

   Create another administrative user, again with a unique user name and complex/strong password that will ONLY be used by SPOT. Call SPOT (801-208-2210) with that user name and password. We will need it to install our software and interfaces. Once the SPOT installation is complete and ALL interfaces have been installed and tested, you MUST disable that account. The account must be re-enabled "only when needed..., and monitored while being used". (PCI DSS Req. 8.5.6)

   Company management must either disable or not use ANY users with Administrative rights on a day to day basis. (PCI DSS 8.5)

H. User Accounts – Everyone

   ALL USERS MUST HAVE THEIR OWN UNIQUE ID (PCI DSS Req. 8) Get a list all current users from the store Manager and set them up in Windows with a unique user name. These users must NOT have administrative rights. There must be an additional method of login authentication. Accepted methods include: a password, a token device or biometrics. If the

company chooses to use passwords, then the passwords MUST follow the requirements listed below.

I. Password Requirements

a. Any vendor supplied defaults must be changed prior to installing a system on the network (PCI DSS Req. 2.1)

b. Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

c. Verify the user's identity before resetting a password

d. Set first-time passwords to a unique value for each user and set so it must be changed immediately after the first use

e. Revoke access for any terminated users immediately upon their dismissal

f. Remove any inactive user accounts at least every 90 days

g. Enable accounts used by vendors for remote maintenance only during the time period needed

h. Store management must communicate password procedures and policies to all users who have access to cardholder data

i. Do not use any group, shared, or generic accounts and passwords

j. Change user passwords at least every 90 days

k. Contains at least 7 characters

l. Contains both letters and numbers

m. Cannot duplicate any of the last 4 passwords

n. Lockout ANY user after 6 failed attempts. This includes an administrator.

o. Set the lockout duration to 30 minutes or until administrator enables the user ID

p. If a computer session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

q. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

J. Disable Automatic Logon - Windows allows you to automate the logon process by storing your password and other pertinent information in the Registry database. Automatic logon MUST be disabled on EVERY computer on the network. In addition, if a computer session has been idle for more than 15 minutes, require the user to re-enter their Windows user and password to re-activate the terminal. (PCI DSS 8.5.15)

K. Windows Components - On the SPOT server running Windows 2003 OS, you must disable all unnecessary and insecure services and protocols. You must also remove all unnecessary functionality. (PCI DSS Reqs. 2.2.2 and 2.2.4)

2. Workstations

A. All non-server network computers must use Windows XP Pro OS. Ensure your network administrator is managing the OS updates so the system always has the latest updates and patches by enabling automatic updates. (PCS DSS Req. 6)

B. Check for maverick applications. (PCI DSS Req. 2.2)

C. Make computers as basic as possible. Remove all icons from the desktop except 'My Computer', 'Network Neighborhood', and 'Recycle'. Consider a desktop lockdown policy.

D. Install anti-virus software on all computers. (PCI DSS Req. 5) Be sure the anti-virus programs are capable of detecting, removing, and protecting against other forms of malware. Also be sure the programs are current, actively running, and capable of generating assessment logs. They must be set to automatically update so they are always current with the program patches.

E. Remote SPOT stations MUST be accessed via Windows Terminal Services or other PCI DSS compliant remote access application/appliance. When implementing the remote stations, be sure to follow best practices. Best practices includes but is not limited to: proper implementation of the hardware and personal software firewalls (PCI DSS Reqs. 1.1.3,1.3), not using any vendor supplied defaults (PCI DSS Req. 2.1.1), implementing session timeouts, idle timeouts, using non-standard RDP ports wrapped in a VPN tunnel and enabling auditing/logging.

   By default, Windows Server 2003 Terminal Services uses ‘high’ level of encryption which encrypts data transmission in both directions using a 128-bit key. You should use this default level.

   Two-factor authentication must be used when connecting to the SPOT network segment from a remote station. Two factor authentications requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors. (See PCI DSS Req. 8.3 for more details)

   Review PCI DSS Req. 12.3 for additional restrictions for remote access such as not allowing cut and paste. Refer to the Remote Access document on http:\\www.SPOTpos.com under Specifications for more information.

   SPOT recommends you use VPN or SSL/TLS for encryption on your terminal server as you must "Encrypt all non-console administrative access." (PCI DSS Req. 2.3)

F. Disable or remove any unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others).

3. TCP/IP

Set individual (static) TCP/IP addresses for each computer as 192.168.0.N, Subnet Mask 255.255.255.0. N is replaced by the number:
server, N = 100.

Station 1, N = 101;
station 2, N = 102, and so on.

The Server and Domain should have unique names for each company. In addition, each computer must have a unique name. COMPANYNAME_SRVR, COUNTER1, COUNTER2, etc. is a good naming convention. The names may NOT have spaces.

Test for TCP/IP connectivity on every computer.

4. SPOT Data Backup

SPOT Business Systems supplied scripts are available for backing up SPOT data, storing a copy on the internal hard disk of the SPOT server in c:\PROGRAM FILES\SBS\backup. It also places a copy of the backup on the internal hard disk of Station #1 in C:\PROGRAM FILES\SBS\backup. These backups are performed by default at the end of each day.

The SPOT POS scripts perform rolling purges of the SPOT backup folders on a nightly basis after a backup file has aged beyond a certain set point, as determined by store management. The number of backups kept on the drive is configurable.

Warning: If store chooses to have no zip disk backup AND also chooses to have no other external backup service or removable media, the store is at risk of catastrophic data loss in the event of a hard disk crash (on the server and/or station #1).

5. Printers

A receipt for receipts and a certified laser printer are required for use with SPOT.

There must be a default printer configured on the network used for nightly reporting and can be shared among the other networked workstations

6. SPOT Support

SPOT support sessions are facilitated by Citrix GOTO Assist. Our services integrated with SPOT's local network and can only be used by SPOT employees.

Support sessions to our customers can be conducted in the following ways:

1. Customers can initiate an SPOT support session by visiting "help.SPOTpos.com" from a browser on the station they are working at, and entering a 7 digit pin code our support agent will give them over the phone. That pin is only good for that support session.

2. An SPOT support agent may email a link to the customer.

3. The link may be accessible via other locations.

Establishing a Connection

A browser MUST be installed in order for staff to access the Internet to then get interactive support from SPOT staff. If the Internet is blocked on computers, you MUST allow access to help.SPOTpos.com. Staff will also need the ability to download an applet for the support session.

Citrix GOTO Assist is designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

- Ports 80 and 443 need to be open for outbound TCP traffic.

- Internet Security software such as software firewalls must not block GOTO assist executable files from downloading. Some examples of software firewalls include MacAfee Security, Norton Security, and Zone Alarm.

Architecture

The architecture of GOTO Assist solution lends built-in security to the support process. Because session traffic is outbound from both directions, both the customer and the support representative can work from behind corporate firewalls providing a barrier to any potentially malicious traffic.

In addition, each GOTO Assist session is initiated by the remote customer when the support issue occurs and is then discontinued automatically when the session is complete, allowing only a small, irregular period of time wherein GOTO Assist traffic is crossing the Internet. This secure architecture provides the first level of GOTO Assist security, obscuring the entire support session by leaving existing security structures in place and spontaneously generating each support session.

GOTO Assist

GOTO Assist accounts and sessions interface with the GOTO Assist Box, which offers an extremely high level of security within a managed environment. All traffic passing through the GOTO Assist is 256-bit AES SSL (Secure Socket Layer) encrypted along the entire data stream. This encryption is in addition to the heavy data compression inherent in GOTO Assist traffic. The login pages for the GOTO Assist interface and /login administrative interface are 256-bit AES SSL encrypted and password-protected, preventing unauthorized users from accessing representative or administrator accounts.

7. Network Administrator Responsibilities

As the company's network administrator you are responsible in training ALL staff on the following:

A. How to properly startup the system and log into the network

B. How to properly shut down the system and the network.

C. Label and show them where all components of the system are including, but not limited to CPU, Monitor, UPS, Server, Network Switch, and Cable connections.

D. Windows Basics including but not limited to logging onto a computer, mouse use, active window, switching windows, and displaying the taskbar.

E. All non-SPOT programs. I.e. Word, Excel

F. How to check the battery level on the UPS.

G. How to set up, delete, enable, disable and maintain Windows users and authentication.

While SPOT is the first point of contact for all SPOT related problems, you will be called upon when needed to provide support for the following:

A. Hardware

B. Operating system

C. Network Communication(TCP/IP) Problems

D. Non-SPOT programs (I.e. Word, Excel, Internet)

E. Printing

F. Data Security

If SPOT determines that you need to be brought in, the customer will normally contact you directly. You should then contact us, and we will go over the problem together and lay out a plan of attack. The idea is that by the customer calling you, you know you have the authorization needed to act. By talking to us, rather than the customer, you get accurate information on a technical level and the customer is not brought into the middle.

Should the customer contact you directly to work on the system, even if it seems non-SPOT related, we must be contacted ahead of time so we can determine if an SPOT technician will need to be available or is required. Upon arriving at the company, we need to be contacted so we can make sure proper steps are done to assure the smooth operation of the company. Once finished, contact us again, so we can run tests to make sure SPOT is running properly.

8. Security

As the network administrator, you are responsible for supporting the company's data security as stated in the PCI DSS. This includes but is not limited to:

A. Antivirus - Many of our customers use McAfee or Norton. (ALL computers on the network MUST have an antivirus program installed. It must be kept running at all times, and be enabled for automatic updates to ensure they are current with security patches. They must also be capable of detecting, removing and protecting against other forms of malware. (PCI DSS Req. 5)

B. Physical security of the dedicated server, if used. (PCI DSS Req. 9)

C. Regular testing of the security of the entire network. (PCI DSS Req. 11)

D. Internal network security, including, but not limited to unique user names and passwords for ALL users; password rules and maintenance; user permissions; and enabling logs to track access.

The company's PCI DSS compliance depends, in part, on the set up and installation of the network hardware and software. Deviation from the above specifications will make the company NON-PCI DSS

compliant as well as vulnerable to breaches. It is the company's responsibility to see that their system is set up and installed in a PCI DSS complaint manner and that it is maintained to continue its compliancy.

Appendix C - Understanding SPOT Activity Log Files

THE FOLLOWING IS A SAMPLE OF AN SPOT ACTIVITY LOG FILE:

Although many of these lines are for diagnostic purposes and can be ignored, some are very important and must be reviewed on a regular basis.

LINES TO BE AWARE OF ARE:

This tells you user named General logged in as an Administrator, added a new user, and logged out.