# Guide to Remote Access Management

## PCATS Recommendation, April 7, 2011

## Abstract

This document provides guidance on protecting Convenience Store systems by deploying and using Secure Remote Access Management practices to thwart undesirable access that would compromise cardholder data.

## Contributors

The PCATS Data Security Committee developed the content for this guide.  They are grateful for the comments and suggestions received from the Remote Access Management SWAT Team in the creation of this document

## Revision History

| Revision Date | Revision Number | Revision Author | Revision Changes |
|---|---|---|---|
| 04/01/2011 | Draft 0.1 | Data Security Committee | Initial Draft |
| 04/06/2011 | Draft 0.2 | Linda Toth, PCATS | Standardize format, improve readability |
| | | | |

## Copyright Statement

## Disclaimers

The National Association of Convenience Stores (NACS), Petroleum Convenience Alliance for Technology Standards (PCATS), participating vendors and retailers make no warranty, express or implied, nor do they assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

## Table of Contents

## Appendices

# 1 Introduction

## 1.1 Overview

Many reports in 2010, including the Visa Franchisor Payment System Security Symposium (June 16, 2010), identified types of cardholder data compromises.  95% of the cases identified were via network intrusions.  Other identified compromises included skimming, lost or stolen receipts and lost or stolen computers.

Hackers were identified as gaining access via remote access, trivial and common passwords and limited Access Control List (ACL) and inadequate segmentation on networks.

Level 4 merchants (defined by Visa as those merchants who process less than one million Visa transactions annually) are the primary targets for hackers.

In response to these threats, the PCATS Data Security Committee (DSC) requested a SWAT Team be created to address Remote Access Management. This document provides a discussion on best practices for Remote Access Management.  Each covered topic provides a summary that addresses the high level points, followed by details that allow the reader to dive deeper into the technology specifics.

## 1.2 Audience

The target audience for this document is the C-Store owner who has no or limited Information Technology (IT) network and security resources.  While we expect that C-Store owners are level 4 merchants, this guidance is applicable for all C-Store owners, regardless of actual merchant level.

# 2 PCS DSS Requirement

For purposes of this guideline all references to the PCI DSS (Payment Card Industry Data Security Standard) requirements will be based on the elements contained in the PCI SAQ (Self-Assessment Questionnaire) C v2.0.

The pertinent requirements include:

8.3: *Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties? (For example, remote authentication and dial-in service (RADIUS) with tokens; or other technologies that facilitate two-factor authentication.)*

Note: Two-factor authentication requires that two of the three authentication methods be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.

8.5.6 (a): *Are accounts used by vendors for remote access, maintenance or support enabled only during the time period needed?*

8.5.6 (b): *Are vendor remote access accounts monitored when in use?*

12.3 (a): *Are usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all personnel, and require the following:*
12.3.1 *Explicit approval by authorized parties to use the technologies?*
12.3.2 *Authentication for use of the technology?*
*12.3.3 A list of all such devices and personnel with access?*
*12.3.5 Acceptable uses of the technologies?*
*12.3.6 Acceptable network locations for the technologies?*
*12.3.8 Automated disconnect of sessions for remote-access technologies after a specific period of inactivity?*
*12.3.9 Activation of remote-access technologies for vendors and business parties only when needed by vendors and business partners, with immediate deactivation after use?*

# 3 Considerations before Enabling Remote Access

## 3.1 Risk Assessment

If a service provider will be accessing a system remotely, that connection needs to be secure. At a minimum, that service provider should validate that their processes at least meet the security described in this document.

Before a small merchant decides to enable remote access for their own use, a risk management discussion should take place so that the proper stake holders know what is at risk. To begin with, the organization should determine that remote access is actually needed and not just a matter of convenience. There are too many risks associated with remote access if it is not done in a secure manner. If it is not absolutely needed, then it should not be activated. The organization should also determine if the benefit derived from enabling remote access outweighs the potential exposure the technology represents in the event that improperly configured or managed remote access connections lead to a data breach, especially credit card theft.

## 3.2 Understanding why remote access is risky

The following list is by no means intended to be all inclusive. Its purpose is to provide examples of common configuration assumptions and mistakes that merchants make when configuring remote access. Many other potential issues exist, and if the technical requirements of security are beyond a merchant, then professional security consultants should be utilized before any remote access is implemented.

### 3.2.1 Access Control List

Implementing a well-crafted router access control list CANNOT stop either a person or software from jumping to one machine from another if remote software is configured to work on the inside of a location.

- For example, an operator connects from home to a back office machine via PC Anywhere over the Internet. Once on that machine, the operator invokes a local copy of PC Anywhere to access another machine inside the location. The firewall or router that allowed the remote communication to the back office does not have means to disallow the connection to the other machine at the location. Many breaches have been caused by this inappropriate setup.
- Some malware (computer viruses, Trojans, or other malicious software) is designed to specifically look for remote software to assist in the process of spreading itself to all the computers at a location.
- Simple Solution – Limit what software is installed on the inside of the location. Disallow unnecessary remote access software, and implement a policy specifically forbidding the installation of any new software without management's approval.

### 3.2.2 Firewalls and Network Segmentation

Limiting the connections from the Internet will require a firewall that allows for port blocking and network segmentation. In many cases, proper firewall configuration is beyond a merchant's ability to manage without technical assistance.

- Enabling remote software to work requires an understanding of Internet Addresses and Network Ports. Connecting remotely to a computer requires knowing how to reach that computer on the Internet using its address, and each software package requires certain Network Ports to be available so that the proper traffic can pass through the network. These are terms and concepts that are beyond the technical abilities of many merchants.
- As a general rule, enabling remote communication requires a deep understanding of networking and computer security. The best practices surrounding remote access include concepts that may require a small operator to engage with a consultant or other technical resource before allowing the technology to be introduced into the environment.

### 3.2.3 Policies and Procedures

Too often, operators try to rely solely upon their own internal policy and procedures to keep the use of remote access to a minimum.

- Relying on voluntary measures to keep your network secure is not acceptable. You want to prevent unauthorized access to your computers and your point-of-sale systems, especially unauthorized access from the internet.
- Once system access is granted to an outsider, security at that location is lowered to the level of the external provider. If the people coming in remotely have feeble controls, they become the weakest link in an operator's security. If a hacker compromises their system, they can use this external access to an operator's location as a means to compromise the operator's security.

# 4 Challenges of Remote Access at C-Stores

The following items were identified as common challenges with remote access at a C-Store site. Understanding each issue and ensuring appropriate practices is one measure that you can take to keep your site secure. While all challenges are identified below, only those items that a level 4 merchant can deal with will be addressed.

- Two-factor authentication
- Shared passwords in remote system
- Insecure software connected directly to the internet
- Controlling access to machines once remote access is enabled
- Limiting ability to circumvent protection methods
- Creating and managing temporary passwords for remote access
- Network segmentation so that only the systems that should be accessed, can be accessed
- O/S hardening, i.e. preventing remote access from allowing malware or other dangers from entering the system
- Managing the time for remote access (enable and disable the access). Particularly, how to ensure that the remote system was not left active.
- Maintaining security at a location so that it is not left vulnerable when allowing remote access.
- Managing the operational process (list of allowed remote access and users)

## 4.1 Remote Access in General

### 4.1.1 Remote Access Summary

Making a remote connection to a sensitive system is a complicated process that will require detailed attention to system configurations in order to keep data secure. It will require assistance from a data security expert – most likely from a network service provider familiar with the retail petroleum industry.

### 4.1.2 Remote Access Details

There are many reasons for wanting to connect to a location's computer systems when away from the location. Some examples include:

- Setting prices
- Checking inventory levels
- Collecting information/reports from the loyalty system
- Reviewing security system reports and video
- Vendor troubleshooting (remote help desk support)

After going through extensive effort to ensure in-store systems are secured, reports and other data are protected, employees are trained, it is a bad practice to allow unfettered access from a remote location. It is a poor security practice to bypass a firewall and other access controls designed to keep malicious individuals out of a system.

When you open your computer to connections from external sources, there is always the risk that a malicious intruder could enter the system using the insecure communication you have allowed. Examples of the damage that could be done include eavesdropping on your communications, unauthorized access of your files, or a spammer configuring your computer to send unauthorized e-mail advertisements. In short, you need to be extremely careful when you enable a remote access feature.

Here are some of the major things you should do when you provide remote access to your systems.

- Never access or transmit cardholder data over the remote access connection.
- Be sure to use a computer dedicated to the remote access tasks. Make sure the remote user activities are limited to only those functions that are necessary for the job at hand. Remove all unnecessary software and do not permit the computer to be used for internet browsing, instant messaging, or email activity. These activities often lead to computer virus infections.
- Limit remote communication to a defined set of IP addresses and only allow certain activities to be conducted from those specific addresses. By minimizing the IP addresses allowed into the store network, hackers will have more issues trying to penetrate the network defenses.
- Make sure the remote access software offers a high level of security. All communications between systems should be completed in a secure manner and should make use of strong encryption methods. 128 bit encryption should be considered the minimum level.
- Create unique accounts for each user. Regularly review accounts and users. Ensure only necessary accounts and permissions are enabled. Do not make everyone system administrators.
- Passwords should be complex (use mixed case characters and numbers) and make passwords at least eight characters long. Consider a longer password phrase if the software permits. Do not communicate account names and passwords through the same method (e.g. email). Passwords should never be shared. Passwords should be changed at least every 90 days and should be kept secure.
- Frequently check for software updates, especially security related updates, and install them on the remote system as appropriate.
- Disable the remote access service when it is not needed and enable it only when needed. When leaving your computer unattended, you should either shut it down or physically disconnect from the Internet connection to reduce the chance that

someone will be able to access your computer. Remember, malicious individuals may keep a different work schedule than you.

- Implement procedures for employees to follow when a vendor needs to connect to your systems. Procedures should include connecting cables and changing settings as needed. Pictures are helpful. Be sure procedures include activity monitoring and steps to disable access when work is complete.
- Make sure activity logging is enabled and occurring. Make sure successful and failed activities are recorded. Periodically review past activities for appropriateness and hints of suspicious activity.
- Finally, be prepared. If suspicious activity is noticed, disconnect the network cable and implement your security incident response plan.

Implementing remote access in a secure manner can be a challenging process. Do not take a chance with your data security. If you do not understand any of these requirements, what they mean, or how to implement them, find someone that can help you. There are several highly qualified network service providers that understand these data security requirements and can help you protect your data, your business, and your reputation. Ask questions and make sure you are comfortable they know what they are doing. Put procedures in place and periodically review them to make sure they remain appropriate and in effect.

## 4.2 Two-Factor Authentication

### 4.2.1 Two-Factor Authentication Summary

Employees and third parties who remotely access store systems need to use two factors of authentication to ensure the identity of the individual accessing the systems. Factor is a technical term that means "form of identification". The use of two-factor authentication significantly improves the security related to remote access of your store systems. Many people try to rely on the most common single factor of authentication, a user name and password. When connecting to a computer remotely, it is not uncommon to be challenged to enter a user name and password. At first glance, that seems fairly secure. The problem comes from the fact that passwords are often compromised, and if a criminal were able to steal the password, they would have the ability to access the same system remotely because the password was the only factor protecting the system.

Adding a second factor such as a signed certificate, dynamic key fob, one-time password sent to an e-mail account, biometric reader, or other method of authentication, drastically increases the security of a location. It is important to understand that having two layers of password protection is not actual two-factor authentication (it is two single factors of authentication, and it is not acceptable according to the PCI standard). The easiest way to understand two-factor authentication is by thinking of it as something you KNOW and something you HAVE that clearly identifies the person who is accessing the systems.   For example, combining a username and password with a finger print reader (biometric device), ensures that the person accessing a remote system is legitimate and not a hacker.

Two-factor authentications can be difficult to implement without technical expertise, and it may require engaging a third party to assist with its implementation.

### 4.2.2 Two-Factor Authentication Details

Remote access is often used by small chains from the home office location to reach into store systems for many purposes. The challenge is to ensure that the people who are accessing these systems can be identified and their actions can be tracked. PCI requires the use of two-factor authentication for remote access to the network by employees, administrators and third parties. Authentication is generally required to access secure data or enter a secure area.  In addition to assigning a unique ID, employ at least two of the following methods to authenticate all users:

1) Password - which is known to the individual
2) Physical devices (e.g., a security token/dynamic key FOB, certificates, one time passwords, or public key)
3) Biometrics – fingerprint or similar scanning

User name: john_smith
Password: •••••••••••
PASSCODE:

Two-factor authentication means using any two of these authentication methods (e.g. password + value from physical token) to increase the assurance that the bearer has been authorized to access secure systems.

Requirement 8.3 of the PCI DSS v2.0 requires two-factor authentication for remote access.  The purpose of two-factor authentication is to make sure you have something you KNOW and something you HAVE.  This allows validation without a shadow of a doubt that the person communicating is who they say they claim to be.  Requirement 8.3 also specifically disallows the use of using one factor twice such as two levels of passwords.

Smaller operators who typically access store systems from their home office need to keep this requirement in mind. All employees who use remote access must use unique passwords that are not shared with others.  Shared passwords are not a real factor of authentication, as it is impossible to uniquely identify who accessed the system since more than one person uses the factor (the same user name and password in this case). In addition the second factor as described above must be used. More often than not, this means using a Managed Service that provides secure remote access or implements a token based approach that will meet the requirements. It is not difficult to do, but it will require some effort. The simplest guidance that can be provided is to look into services that allow you to have two-factor authentication for remote access. Keep in mind that any third party who accesses your systems remotely (e.g. POS vendors) will also need to use two-factor authentication or their access will not be considered PCI compliant either.

Here are some tips when implementing two-factor authentication to support the efforts of small merchants who are trying to manage their PCI compliance.

- Two-factor authentication should be available and integrated into the environment at the time of logging in (especially for remote access) so small organizations don't have to manage a two-factor authentication system separately.
- Two-factor authentication should not require Active Directory or other enterprise class tools as small organizations typically do not have access to such tools.
- PCI is concerned about the cardholder data environment. If your network or systems are completely outside of the cardholder data environment, you are not required to implement two-factor authentication. **Please note: If any of your systems have a way to reach into the cardholder data environment, then two-factor authentication is required.**
- If you use a separate communications line for remote access that is unrelated to the VSAT communications, then you must pay attention to secure access using two-factor authentication solutions
- Since some remote access operations like retrieving files from a system that is in scope for PCI can result in a breach (not just remote control), operations such as file transfer to / from in scope systems should also be protected by two-factor authentication.

Secure two-factor authentication based methods to remotely access store systems are widely used and required to be PCI compliant.  Managed Services providers are available to assist store operators meet this requirement.

## 4.3 Passwords in Remote Systems

For validated PCI POS Systems follow manufacturers recommended guidelines.

### 4.3.1 Passwords Summary

**Unique Identification**: Shared accounts are not allowed at any time for users, vendors, customers and visitors. Individual logon ID authorizations are non-transferable. Each individual is accountable for all activity made with their logon ID.

**Password Changes**: All passwords should expire after a maximum of 90 days. Users should have the ability to change their passwords on demand. Changes should be made to their password immediately if they feel security may be compromised.

**Privilege Management**: All access rights for privileged users ID's should be restricted to the lowest privileges necessary to perform their job. All outside vendors must be assigned their own user ID and password, and it should not be a shared account.

### 4.3.2 Passwords Details

**Account & Passwords Requirements**: Every network component, operating system, application and data structure must require authorization using an account and password combination. Time outs for inactivity should be implemented by business case.

**Password Strength**: The weakest link in computer security is the personal password. Factory default passwords must be changed and contain a mix of alphabetic and numeric characters. Personal information such as birthday and social security data should not be used. Passwords should be a minimum of 7 characters according to PCI. PCI also demands that a combination of numbers and letters are used when making a password. As far as best practices go, some of which surpass the minimums stated in PCI, password length should be 8 characters long as well as contain 3 of the following 4 characteristics:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Numbers (0-9)
- Special characters (! $ # %)

**User Responsibility**:

- Systems and data are for use only by the individual granted access. Access must not be shared.

- User accounts must be protected with passwords.
- The remote user must be sure that the most current anti-virus software is running on their computer before accessing a system remotely.  Viruses are often introduced by infected machines connecting to other computers remotely.
- Report unauthorized system activity to management.

**Network Access Control**: Access to network devices such as routers, switches, lines and servers is required to have formal authorized access.  Under no circumstances should anyone install hardware, software or specialized devices onto the network without approval from management.  This requirement is most critical if that equipment could be configured to allow remote communication into the environment.

**Remote Data Access Standards**:

- Review all authorized employees, vendors and business partners to ensure validity and proper access to business data.
- Approve or deny access to data.
- Assign access based on job classification or function.
- Create and maintain in-house security rules.
- Review and evaluate processes and monitor changes.
- Disable any unused user ID and password after 60 idle days.

## 4.4 Network Segmentation

Network segmentation ensures that only the systems that should be accessed can be accessed.   Network segmentation isolates systems responsible for handling cardholder data from un-trusted systems.  The purpose of segmentation is to make sure remote access to one system will not allow you to insecurely access other systems.  The selection, configuration and installation of equipment to meet the network security requirements of PCI-DSS can be challenging.  Users are encouraged to seek knowledgeable technical help.

That being said, some simple equipment configurations incorporating remote access for non-cardholder data segments are shown in the document “PCATS PCI Guidance Document:  Network Segmentation”.   These diagrams are general in nature with details dependent on specific equipment deployed and business needs.  Equipment should always be installed according to the manufacturer’s PCI implementation guidelines.

## 4.5 O/S Hardening (Preventing Malware from Entering the System)

### 4.5.1 O/S Hardening Summary:

- Always be sure that malware detection (anti-virus software) is running on remote machines.
- Be familiar with the machine used for remote access.  Do not remotely connect to your store using a computer that is out of your control.  You should be able to verify that it is a well-managed and secure machine before you use it for remote access.
- If you do a download, watch for unusual behavior afterwards.
- Helpful tip: Consider using a white list application software package to limit what types of files can be uploaded and to protect where files can be transferred during remote access.

### 4.5.2 O/S Hardening Details

The definition of "O/S hardening" is the securing of the operating system through patches authorized by the POS vendor to protect against vulnerabilities and exploits (such as viruses, malware, etc...). In the case of LDAP or FTP, remote access may allow a binary program (such as a virus) on the POS system. If the POS has an OS and a GUI that can "browse" the Internet, then it is vulnerable to exploitation if not properly patched.   An un-hardened system should have in place a process of removing sensitive card data before it becomes unhardened and insecure.

- Under PCI DSS v1.2.1, the file transfers using Remote Access technology was not allowed.  This has been reversed in the PCI DSS v2.0 so that if there is a business justification then you can upload and download files.  An example business justification is if a corrupt database with credit card numbers is being downloaded so that the database can be repaired and then reloaded on the POS system, there is adequate business justification to allow the file transfer.
- If you do not have your O/S hardened or do not know how to do this then you should not enable remote control of the payment application.
- If you haven't hardened your O/S, are not running an anti-virus program, or do not have a business justification for enabling file transfer services (any of these three things), then you should not allow remote access of that machine.

## 4.6 Managing Remote Access

Managing when remote access is allowed and ensuring that the remote system is not left active is critical to successfully implementing a remote access strategy.

### 4.6.1 Managing Remote Access Summary

Using a management system that can allow remote access into a location based on need is complicated and requires a level of sophistication that is beyond most small operators. A simple alternative that does not involve technology and is just as secure as a remote management utility is for initiating the remote software only from the location when it is needed. This means that the software should be disabled when it is not needed.

For example, if the remote communication happens over a phone line, keep the line unplugged when it is not in use for remote management. Plug it in only when an authorized third party needs remote access for management purposes. When the remote need is finished, unplug the phone line. Some systems have an “A/B” switch for remote access. Label which way (A or B) is active, and have a daily procedure making sure that the inactive state is returned daily.

Train your managers or other employees to write down in a log the details of when remote access was used. The log should include: who, when, why, date, time turned on, and time turned off.

If your system has a different screen color when there is someone logged in, have a policy for people to report the fact that they saw the different color come up. In that way, there is a mechanism to report if unexpected remote access is taking place. Training of your employees is key to making this effective. Make sure that all employees know how your support personnel communicate to the store. Also, ensure that they are trained on how to enable, disable, and log remote access.

### 4.6.2 Managing Remote Access Detail

If your environment is more complicated or if it not practical to always have someone on-site who can initiate a remote session when it is needed, then more sophisticated measures will be required. For example, you may have an operational concern like what occurs when fuel is down at 2:00 am and the person on-site does not know how to enable the remote access. If needed, make sure that your supplier has in their contract the security associated with the remote access that they will use to provide you with support. Make sure that they will take responsibility for the security, the logging and the liability associated with remote access if they do not follow the guidelines in their contract. Under no circumstance, should you ever allow anyone to install remote access software that is always enabled using default passwords. If this is the method that your supplier wants to use, then it is the operator's responsibility to insist on greater security.

Another best practice is creating a kit or a notebook that specifically has what an employee should do if remote access is needed. Detailed instructions that could walk someone through the process would be included. Screen shots of enabling software if applicable could be included. The log to fill out could be kept in the back of the documentation. Make sure that the instructions highlight the importance of disabling the remote access when the session is finished.

Using a VPN instead of internet based remote access is tricky. This is a much more complicated setup and there is some disagreement in the security community as to how a VPN connection should be maintained if it is used for 3rd party support. Some experts say that as long as the 3rd party is providing Level 1 support, all calls go to the 3rd party. They can have a secure full time VPN (not public) access to the location. The 3rd party should still be required contractually to guarantee their internal processes to ensure the security of an operator's location, and there should be adequate logging of the support sessions so that their activity can be traced in the event that there is an issue. On the other hand, if the 3rd party support staff is providing Level 3 support, occasional help, then they should not have permanent access. Even over a VPN, the 3rd party should only be given access to the location as needed. It may be necessary to discuss the two scenarios with a qualified security professional if you are not sure how you are receiving support.

Employees should be trained specifically that if they are in doubt, they should call their supervisor before enabling remote access. This should be part of the location's policy and procedures.

# 5 Logging

Although logging is outside the scope for SAQ C merchants, it is a good security practice and should be addressed.

Logging is defined as a record of computer activity used for statistical, backup, recovery, or auditing purposes. In short, it is an ongoing record of what happened on a computer, at any given time, and by whom. As far as remote access is concerned, the best practice in regards to logging is to know who accesses a system, when they started their remote session, what services were running while they were connected remotely, and at what time they finished. It is important to note that logging is only a record of what happened. That information is only useful if someone is reviewing it to verify that unauthorized activity is not taking place.

To properly take advantage of a remote access log, it is important that someone is assigned the task of examining the logs for unexpected access. Also, the logs should be retained for at least a year. Keeping the logs available will help during a forensic audit if you ever need to justify remote access or validate that remote access was not the source of a credit card breach.

While creating, examining, and storing logs goes beyond the requirements of a merchant burdened with completing an SAQ C, it is still a best practice from a security stand point. If remote access is going to be enabled at a location, adding logging to the remote communication should strongly be considered.

# A. References

## A.1 Normative References

**PCI DSS Self-Assessment Questionnaire (SAQ) –** Published by the PCI Security Standards Council. Available at:

https://www.pcisecuritystandards.org/security_standards/index.php

**PCATS PCI Guidance Document: Network Segmentation** – Published by PCATS. Available at:

http://www.pcats.org

## A.2 Non-Normative References

## B. Glossary

| Term | Definition |
|---|---|
| DSC | Data Security Committee |
| NACS | National Association of Convenience Stores |
| PCATS | Petroleum Convenience Alliance for Technology Standards |
| PCI DSS | Payment Card Industry Data Security Standard |
| PCI | Alternate abbreviation for Payment Card Industry Data Security Standard |
| SAQ | Self-Assessment Questionnaire |