

Tracked *Value* Virtual Payment Terminal (VPT)  
PA-DSS Implementation Guide

Version 1.0

Approval Date: <pending>

Author: Todd Neuman

## Notice

**THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. MATRIX INVENTORY SOLUTIONS INC. (“MATRIX”) MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER MATRIX NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION.**

**IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.**

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA- DSS and PCI-DSS compliance.

**The retailer may undertake activities that may affect compliance. For this reason, Matrix is required to be specific to only the standard software provided by it.**

## Revision Information

Version	Date	Changes
0.01	June 1, 2010	Initial Release of Document
0.02	June 1, 2010	Spelling corrections
0.03	July 28, 2010	Updated Key Change screen shot
0.04	August 26, 2010	Add instruction to disable any unnecessary services on host PC
0.05	August 27, 2010	Add link to Datacap DSIClientX website
0.06	August 30, 2010	Add Key Custodian Form, Multi-Factor Remote Access
0.07	March 17, 2011	Remove old reference to other Wireless Security Methodogies
0.08	November 7, 2011	Update Secure Data Storage Information
0.09	December 13, 2011	Update Encryption information

## Table of Contents

Introduction.....	6
Build and Maintain a Secure Network.....	7
Requirement 1: Install and maintain a firewall configuration to protect data.....	7
What the requirement says.....	7
How TrackedValue VPT helps you meet these requirements.....	7
What this means for you.....	7
Requirement 2: Do not use vendor-supplied defaults for system parameters and other security parameters.....	7
What the requirement says.....	7
How TrackedValue VPT helps you meet these requirements.....	7
What this means for you.....	8
Protect Cardholder Data.....	8
Requirement 3: Protect stored cardholder data.....	8
What the requirement says.....	8
How TrackedValue VPT helps you meet these requirements.....	8
What this means for you.....	8
Requirement 4: Encrypt transmission of cardholder data across open, public networks....	9
What the requirement says.....	9
How TrackedValue VPT helps you meet these requirements.....	9
What this means for you.....	9
Maintain a Vulnerability Management Program.....	9
Requirement 5: Use and regularly update anti-virus software or programs.....	9
What the requirement says.....	9
How TrackedValue VPT helps you meet these requirements.....	9
What this means for you.....	9
Requirement 6: Develop and maintain secure systems and applications.....	10
What the requirement says.....	10
How TrackedValue VPT helps you meet these requirements.....	10
What this means for you.....	10
Implement Strong Access Control Measures.....	10
Requirement 7: Restrict access to cardholder data by business need to know.....	10
What the requirement says.....	10
How TrackedValue VPT helps you meet these requirements.....	10
What this means for you.....	10
Requirement 8: Assign a unique ID to each person with computer access.....	11
What the requirement says.....	11
How TrackedValue VPT helps you meet these requirements.....	11
What this means for you.....	11
Requirement 9: Restrict physical access to cardholder data.....	11
What the requirement says.....	11
How TrackedValue VPT helps you meet these requirements.....	12
What this means for you.....	12
Regularly Monitor and Test Networks.....	12
Requirement 10: Track and monitor all access to network resources and cardholder data	

- ..... 12
  - What the requirement says..... 12
  - How TrackedValue VPT helps you meet these requirements..... 12
  - What this means for you..... 12
- Requirement 11: Regularly test security systems and processes..... 13
  - What the requirement says..... 13
  - How TrackedValue VPT helps you meet these requirements..... 13
  - What this means for you..... 13
- Maintain an Information Security Policy..... 13
  - Requirement 12: Maintain a policy that addresses information security for employees and contractors..... 13
    - What the requirement says..... 13
    - How TrackedValue VPT helps you meet these requirements..... 13
    - What this means for you..... 13
- Ensuring TrackedValue VPT is implemented properly..... 14
  - 1. Manage Sensitive Data..... 14
    - Delete Sensitive Data from Historical Versions (PA-DSS 1.1.4)..... 14
      - How does TrackedValue meet the compliance requirement..... 14
      - What you need to do to meet the compliance requirement..... 14
    - Delete Sensitive Authentication Data gathered while Troubleshooting (PA-DSS 1.1.5)..... 14
      - How does TrackedValue meet the compliance requirement..... 14
      - What you need to do to meet the compliance requirement..... 14
  - 2. Managing Secure Data..... 15
    - Purge cardholder data after customer-defined retention period (PA-DSS 2.1)..... 15
      - How does TrackedValue meet the compliance requirement..... 15
      - What you need to do to meet the compliance requirement..... 16
    - Delete cryptographic key material (PA-DSS 2.1)..... 16
      - How does TrackedValue meet the compliance requirement..... 16
      - What you need to do to meet the compliance requirement..... 16
  - 3. Managing User ID's..... 17
    - Use Unique User ID's and secure authentication for administrative access (PA-DSS 3.1)..... 17
      - How does TrackedValue meet the compliance requirement..... 17
      - What you need to do to meet the compliance requirement..... 19
    - Use Unique User ID's and secure authentication for access to PC's and Servers (PA-DSS 3.2)..... 19
      - How does TrackedValue meet the compliance requirement..... 19
      - What you need to do to meet the compliance requirement..... 19
  - 4. Automated Audit Trails..... 23
    - Implement automated audit trails (PA-DSS 4.2)..... 23
      - How does TrackedValue meet the compliance requirement..... 23
      - What you need to do to meet the compliance requirement..... 23
  - 5. Develop Secure Payment Applications..... 23
    - Do not use Unnecessary or Insecure Services and Protocols..... 23
      - How does TrackedValue meet the compliance requirement..... 23
      - What you need to do to meet the compliance requirement..... 23
  - 6. Provide a Secure Network..... 24
    - Securely implement wireless technology (PA-DSS 6.1 and PA-DSS 6.2)..... 24
      - How does TrackedValue meet the compliance requirement..... 24
      - What you need to do to meet the compliance requirement..... 25

Store cardholder data safely away from the Internet (PA-DSS 9.1 and PA-DSS 12.1).....	25
How does TrackedValue meet the compliance requirement.....	25
What you need to do to meet the compliance requirement.....	25
Encrypt cardholder data sent over end-user messaging technologies (PA-DSS 12.2).....	25
How does TrackedValue meet the compliance requirement.....	25
What you need to do to meet the compliance requirement.....	26
7. Secure Delivery of Payment Application Updates (PA-DSS 10.1).....	26
How does TrackedValue meet the compliance requirement.....	26
What you need to do to meet the compliance requirement.....	26
8. Secure Remote Access to the Payment Application (PA-DSS 11.2 and PA-DSS 11.3).....	26
How does TrackedValue meet the compliance requirement.....	26
What you need to do to meet the compliance requirement.....	27
9. Encryption Non-Console Administrative Access (PA-DSS 13.1).....	27
How does TrackedValue meet the compliance requirement.....	27
What you need to do to meet the compliance requirement.....	27
10. Key Management Techniques.....	27
Compliance with Standards.....	27
Key Storage Method.....	27
Key Rotation.....	27
Old Keys.....	28
Refreshing Keys If Data Is Compromised.....	28
11. Third Party Tools.....	29
Compliance with Standards.....	29
Appendix "A" - Sample Key Custodian Form.....	29
Compliance with Standards.....	29
How does TrackedValue meet the compliance requirement.....	29

## Introduction

The Payment Card Industry Data Security Standard (PCI-DSS) and Payment Application Data Security Standard (PA-DSS) define a set of requirements for the configuration, operation, and security of payment card transactions in your business. If you use TrackedValue VPT to store, process, or transmit payment card information, these standards and this guide apply to you. Failure to comply with these standards can result in significant fines should a security breach occur.

For more details about PCI DSS and PA- DSS, please see the following links:

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

PA-DSS: [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

This guide is reviewed and updated regularly to incorporate changes in TrackedValue VPT and the PCI standards. Please visit our website at <http://www.trackedvalue.com/VPT/documentation.html> for the latest version of this guide.

The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 1.2 dated October, 2008).

Matrix instructs and advises its customers to deploy TrackedValue VPT applications in a manner that adheres to the PCI Data Security Standard (v1.2).

**If you do not follow the steps outlined here, your TrackedValue VPT installation will not be PA-DSS compliant.**

There are 12 basic requirements for PCI compliance which can be grouped into 6 major categories. Following is a brief review of these requirements with TrackedValue specific guidelines. Ultimately, you are responsible for knowing, implementing and maintaining PCI standards.

## Build and Maintain a Secure Network

### ***Requirement 1: Install and maintain a firewall configuration to protect data***

#### What the requirement says...

- Establish firewall and router configuration standards .
- Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.
- Prohibit direct public access between the Internet and any system component in the cardholder data environment.
- Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet

#### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT is designed to operate securely in a network behind a firewall and it works with all known firewall applications.

#### What this means for you...

You should install and maintain firewall software on any computers used on your network or to access your network. Specifically, you should block all inbound traffic to your network to required access only and document why the access is necessary. Your TrackedValue card data files must never be accessible to any system outside of your secure zone.

### ***Requirement 2: Do not use vendor-supplied defaults for system parameters and other security parameters***

#### What the requirement says...

- Always change vendor-supplied defaults before installing a system on the network
- Develop configuration standards for all system components.
- Encrypt all non-console administrative access
- Shared hosting providers must protect each entity's hosted environment and cardholder data.

#### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT supports and encourages you to have different usernames specific to each person accessing the payment system.

## What this means for you...

It is important that you change all usernames and passwords to something different for your company for each piece of equipment. If your system is properly secured, Hackers would need to modify settings for them to gain access to your card holder data. This is easily accomplished if you don't change the passwords away from "default" or <blank>, etc. It is an easy task to search the internet to find the default username and password for any given network device, all you need is the manufacturer and model number.

## Protect Cardholder Data

### **Requirement 3: Protect stored cardholder data**

#### What the requirement says...

- Keep cardholder data storage to a minimum.
- Do not store sensitive authentication data after authorization (even if encrypted).
- Mask the Primary Account Number (PAN) when displayed.
- Render PAN, at minimum, unreadable anywhere it is stored.
- Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.
- Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

#### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT allows you to specify how many days the full PAN is stored for a completed transaction including the option to never store it. If your Merchant Bank and connection method support batch settling without the PAN, we suggest that you never store the PAN on any of your systems. If you don't have it – then no one can get it from you.

TrackedValue VPT never stores sensitive authentication data. If the PAN is retained, it is stored encrypted using industry standard, strong cryptography. Please see the section titled "Encryption Management" for further details on this area.

Whenever TrackedValue VPT presents a PAN in a report or customer invoice it is always a truncated version of the PAN not exceeding the first 6 digits and last 4 digits.

#### What this means for you...

It's up to the software to only store permitted data and to store it safely and securely. It's up to you to protect the keys necessary to make the data useful. This includes generating a Key Management Plan and having each staff member who handles the encryption keys sign a Key Custodial Agreement. A sample Key Management Plan and Key Custodial Agreement are available at <http://www.trackedvalue.com/VPT/documentation.html>.

You should regularly change your passwords and make sure that they are not easily guessed. If you ever suspect an encryption key has been lost or compromised you must immediately perform a Key Change. Never store credit card numbers or other sensitive data in any field not specifically designed to store that type of data.

## **Requirement 4: Encrypt transmission of cardholder data across open, public networks**

### What the requirement says...

- Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.
- Never send unencrypted PANs by end-user messaging technologies.

### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT treats all transmissions over any network, including the local LAN, as potentially open and public. Whenever a PAN leaves the local TrackedValue VPT system all cardholder data is encrypted and protected. If the data is travelling to another point on your LAN that is part of the VPT chain, then the destination will have the encryption keys to decrypt and use the data as needed.

Whenever sensitive information is leaving the system running TrackedValue VPT the data is fully protected. It is either travelling to the Merchant Processing Bank over a SSL connection or it is a PAN being stored in the TrackedValue VPT database and it's encrypted before leaving the local computer. Basically, we treat every network connection as a potentially hostile connection and protect the data accordingly.

TrackedValue VPT does not use any end-user messaging technologies within the software.

### What this means for you...

If you are using a wireless network, you must have wireless security enabled and use WPA2 security only. Any previous wireless security models are no longer permitted or grandfathered.

Never transmit a card number over open email or in any kind of user-to-user chat tool.

## Maintain a Vulnerability Management Program

### **Requirement 5: Use and regularly update anti-virus software or programs**

#### What the requirement says...

- Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
- Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

#### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT is compatible with anti-virus, firewall, anti-spyware, and anti-malware software.

#### What this means for you...

You must run an anti-virus program at all times on your systems. It should have any "auto-update" feature enabled so that it stays current for new threats and you need to regularly check that it's running.

## **Requirement 6: Develop and maintain secure systems and applications**

### What the requirement says...

- Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
- Establish a process to identify newly discovered security vulnerabilities.
- Develop software applications in accordance with PCI DSS.
- Follow change control procedures for all changes to system components.
- Develop all web applications based on secure coding guidelines.
- For public-facing web applications, address new threats and vulnerabilities on an ongoing basis.

### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT is developed in accordance with all of these guidelines. We test for security problems and vulnerabilities throughout the development cycle. Secure updates are made available to registered users of the software.

### What this means for you...

You should enable Microsoft Windows Updates or a similar replacement service on each system running TrackedValue VPT. Register your software with TrackedValue and apply any security updates as provided.

It is your responsibility that any e-commerce website you develop directly or have done for you must comply with PCI DSS and that you can reasonably confirm it is being kept current for new security threats.

## Implement Strong Access Control Measures

### **Requirement 7: Restrict access to cardholder data by business need to know**

### What the requirement says...

- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT has a user model that restricts access to data unless specifically granted on a per user basis.

### What this means for you...

Basically, give the minimum permissions to each employee to allow them to do their job properly, but not see or

access any information that they do not require in the performance of their duties.

### ***Requirement 8: Assign a unique ID to each person with computer access***

What the requirement says...

- Assign all users a unique ID before allowing them to access system components or cardholder data.
- Require ID's to have a password, passphrase , token or biometric authentication method.
- Incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties.
- Render all passwords unreadable during transmission and storage on all system components using strong cryptography
- Ensure proper user authentication and password management for non- consumer users and administrators on all system components

How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT has a user model that restricts access to data unless specifically granted on a per user basis. TrackedValue VPT enforces password complexity rules on Administrators and supports it on all users.

What this means for you...

You should set up individual user accounts for each user of TrackedValue VPT and not share accounts. You should also setup unique user accounts in Windows. Any user that can retrieve or reference a complete card number for more than the current transaction must use a password that meets PCI criteria.

### ***Requirement 9: Restrict physical access to cardholder data***

What the requirement says...

- Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
- Develop procedures to help all personnel easily distinguish between employees and visitors.
- Make sure all visitors are visually identifiable and authorized before entering areas where cardholder data is processed.
- Use a visitor log including the visitor's name, company, purpose and the employee authorizing them.
- Store media backups in a secure location.
- Physically secure all paper and electronic media that contain cardholder data.
- Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.
- Ensure management approves any and all media containing cardholder data that is moved from a secured area.

- Maintain strict control over the storage and accessibility of media that contains cardholder data
- Destroy media containing cardholder data when it is no longer needed for business or legal reasons.

## How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT allows you to keep your database on a separate, physically secure server so that it is less likely to be compromised and the cardholder data fall into the wrong hands.

Merchant copies of transactions do not contain the full PAN and therefore do not fall under the secure document storage requirement.

## What this means for you...

Within reason, you need to keep visitors away from your cardholder data unless they have valid business reason to access it or be near it.

You must physically secure any document, including “Merchant Copies” of receipts that contain full card numbers and you should destroy them when they will no longer be needed. As long as the paper exists, it is a potential loss risk.

By all means have a backup of your data, but make sure they are encrypted, labeled appropriately and accounted for.

## Regularly Monitor and Test Networks

### ***Requirement 10: Track and monitor all access to network resources and cardholder data***

## What the requirement says...

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

## How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT maintains two control systems to facilitate management review and forensic analysis. An internal log is generated for a significant events which include items such as Password Resets, Password Changes, User login date & time, when a card number is viewed for administrative purposes.

There is also an Audit trail integral to the system to manage any change in the VPT data files including the terminal, user, date & time, and the full details of the data change.

## What this means for you...

Review the Windows application and security logs periodically to determine which users are accessing your system. Review the VPT logs regularly to ascertain if any users are inappropriately accessing cardholder data or performing any suspicious activities.

## ***Requirement 11: Regularly test security systems and processes***

### What the requirement says...

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

### How TrackedValue VPT helps you meet these requirements...

This area is external to TrackedValue VPT and the application doesn't contribute to the success, nor does it deter, from this requirement.

### What this means for you...

Under the adage that "What is safe today, may not be safe tomorrow," you are to regularly run vulnerability tests to see if any potential issues exist. This includes, but is not limited to, confirming that there are no rogue Wireless Access Points (WAPs) and that additional firewall ports have not be opened to allow unsolicited traffic on to your network.

## **Maintain an Information Security Policy**

### ***Requirement 12: Maintain a policy that addresses information security for employees and contractors***

### What the requirement says...

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

### How TrackedValue VPT helps you meet these requirements...

TrackedValue VPT allows and recommends you set up individual user accounts with appropriate data level access controls to ensure your data is managed safely and protected.

### What this means for you...

Be clear with your employees, contractors and service partners of the importance of keeping your data private and secure. You should have a clearly written policy that defines acceptable software and its permitted uses on your systems, remote access methods and procedures. Most importantly, an incident response plan so that you are prepared to respond immediately to a system breach.

## Ensuring TrackedValue VPT is implemented properly

As you have read so far, there are many aspects to ensuring that you have a safe environment for storing and processing credit cards. Our staff have worked diligently to produce the TrackedValue VPT application under the PA-DSS guidelines so that you can maintain a PCI compliant environment. This work still requires some specific tasks on your part to make sure that the TrackedValue VPT application is implemented properly at your site.

**If you do not follow the steps outlined here, your TrackedValue VPT installation will not be PA-DSS compliant.**

### 1. Manage Sensitive Data

#### Delete Sensitive Data from Historical Versions (PA-DSS 1.1.4)

In some cases, prior versions of various payment applications may have stored sensitive cardholder data including track data, PIN blocks, PINs, or card validation codes. It is no longer acceptable for a compliant application to store these values and as such any existing data from previous versions must have this data destroyed.

How does TrackedValue meet the compliance requirement...

This is the initial release of the application and as such has no historical data that needs to be deleted

What you need to do to meet the compliance requirement...

There is no action that needs to be taken on your part.

#### Delete Sensitive Authentication Data gathered while Troubleshooting (PA-DSS 1.1.5)

When a software vendor must record Sensitive Authentication Data such as a track value or PIN Block it must only be collected when needed to solve a specific problem.

How does TrackedValue meet the compliance requirement...

We have developed a secure method to store this data that must be specifically activated and subsequently deactivated. Our method adheres to the following guidelines:

- Collect sensitive authentication data only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

What you need to do to meet the compliance requirement...

It is important that if you perform any troubleshooting that you follow these guidelines as well. It is our

recommendation that you do not capture this data unless you are operating under the direct instructions of a TrackedValue VPT Support Technician.

## 2. Managing Secure Data

### Purge cardholder data after customer-defined retention period (PA-DSS 2.1)

Cardholder data must be purged after it exceeds the customer-defined retention period in all locations where it stores cardholder data.

How does TrackedValue meet the compliance requirement...

TrackedValue VPT automatically deletes credit card data on a predefined schedule. There is no regular or on-going action required by you to delete the data beyond setting the values below. Follow the instructions to change the values as needed.

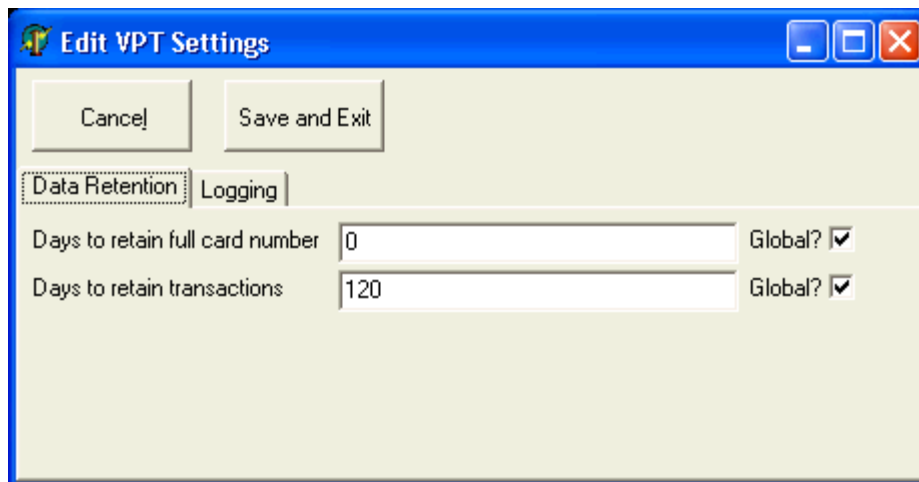
1. Open TrackedValue VPT and select Administration | System Maintenance | Edit Settings.
2. Click the “Data Retention” tab.
3. Set the value for “Days to retain full card number” to an appropriate value for your business.

**Set it to “0” to never record them. If you don’t retain any card numbers then they can’t be compromised from your data files.** This means that a card number and expiry date can be retrieved for any transaction newer than x days.

4. Set the value for “Days to retain transaction info” to a reasonable value for your business.

This means that you can reprint a transaction with a truncated card number for any transaction newer than x days. The default value for this field is 120 days.

5. Any values you change will be automatically applied to all existing transactions. **Please be sure of the settings you choose because you may delete data prematurely and it can’t be recovered.**
6. Click “Save and Exit”



## What you need to do to meet the compliance requirement...

To meet the compliance requirements you need to observe the following:

- Leave the “Days to retain full card number” setting an appropriate value and do not set it to a number exceeding the length of time you would legitimately need to be able to access the full card number of any given transaction.
- Check back on the “Edit VPT Settings” page at regular intervals to confirm that someone has not modified the number of days to an inappropriately high value. The application will automatically remove the data on a daily basis as it reaches these target days.
- Only enter credit card data into TrackedValue VPT rather than any other unsecure locations like your POS customer information screen.
- Only enter credit card data in the appropriate fields. Never enter CVV2 or magnetic stripe data into any alternative spots to store it.
- Do not keep hard or written copies of card data
- Do not include card data in any emails or other correspondence.
- Keep the card data the bare minimum amount of time. We recommend you never store the cardholder data in the system after approval.
- Backups should be encrypted if you retain any cardholder data after authorization.
- Archival backups should be destroyed or overwritten once as they become too old to be useful.

## Delete cryptographic key material (PA-DSS 2.1)

Any old cryptographic material created by past version of the payment application must be removed from data files and is re-encrypted with the current cryptographic key material.

By default, data files are stored on the local computer in the C:\VPTData\DBAnsi folder. The contents of this folder are automatically maintained / purged by the system excluding backups. There is no automated backup method built into the system and it's your responsibility to preserve the data in a safe and secure manner.

## How does TrackedValue meet the compliance requirement...

TrackedValue VPT has no prior versions and therefore no prior cryptographic material to be concerned with. Please see the section titled “Encryption Management” for further details on this area.

## What you need to do to meet the compliance requirement...

There is no action that needs to be taken on your part.

### 3. **Managing User ID's**

#### **Use Unique User ID's and secure authentication for administrative access (PA-DSS 3.1)**

How does TrackedValue meet the compliance requirement...

TrackedValue VPT allows you to define users and user groups. All activity logging tracks the user id that performs the task but the permission allowing the task is assigned at the user group level.

Here are the instructions to Add a User Group:

1. Open TrackedValue VPT and select Administration | System Maintenance | Edit User Groups
2. Click "Add"
3. Configure the following options:
  - Allow Regular Transactions – Active user can perform a "Charge" Transaction
  - Allow Return Transactions – Active user can perform a "Return" Transaction
  - Allow Gift Card Activations – Active user can "Activate" or "Increment" a Gift Card
  - Allow Voids – Active user can Void any eligible Transaction
  - Perform End of Day Routines – Active user can Settle Batches and print day end reports
  - Run General Reports – Active user can run System Reports
  - Enforce Password Restrictions – Active user is forced to have a complex password that expires. Must be selected if any Administrative Permission is granted.
  - View Cardholder Data – Administrative – Active user can recall the Card Number and Expiry Date for any past transaction if it hasn't been purged. Requires "Enforce Password Restrictions".
  - Change System Configuration – Administrative – Active user can change various system settings such as Merchant Profiles, Payment Tenders, Users, and User Groups.
  - Import Configuration Settings – Administrative – Active user can import configuration files for setting up various support tables including Users and Merchants.
  - Clear Logs – Administrative – Active user can clear the Payment Application log files.

- Manage Encryption Keys – Administrative – Active user can retrieve and generate new Encryption Keys. This is the most trusted task any user can be given, please be cautious.

User Group ID	Description	Allow Regular Transactions	Allow Return Transactions	Allow Gift Card Activations	Allow Voids	Perform End of Day Routines	Run General Reports	Enforce Password Restrictions	View Cardholder Data	Change System Configuration	Import Configuration Settings	Clear Logs	Manage Encryption Keys
ADMIN	Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Here are the instructions to Add a User:

1. Open TrackedValue VPT and select Administration | System Maintenance | Edit Users
2. Click "Add"
3. Assign a unique User ID
4. Click the "Active?" box to activate the employee. To inactivate an employee, remove this check mark and the user will no longer be permitted to access TrackedValue VPT. This should be done immediately when an employee leaves the company.
5. Enter the first and last names of the employee.
6. Assign a User Group.
7. Enter a password for the employee.
8. Click "Save And Exit"

**Edit Users**

Buttons: Add, Change, Delete, Cancel, Save And Exit, Save, Save & Add

User ID: SC

Active?:

First Name: Clerk

Last Name: Sample

User Group: CLERKS

Password: \*\*\*\*\*

Date of the last password change: 05/11/2010

Changing

### What you need to do to meet the compliance requirement...

In order to meet the compliance requirements, you will need to observe the following:

- Do not use generic User ID's such as "STAFF", each person needs a unique ID to access TrackedValue VPT
- Assign passwords to any user with administrative privileges
- Do not use common or generic passwords
- Change user passwords regularly, at least every 90 days
- Passwords must contain both numeric and alphabetic characters

### Use Unique User ID's and secure authentication for access to PC's and Servers (PA-DSS 3.2)

#### How does TrackedValue meet the compliance requirement...

TrackedValue VPT supports and encourages you to have different usernames specific to each person accessing the PC's and Servers holding the application.

### What you need to do to meet the compliance requirement...

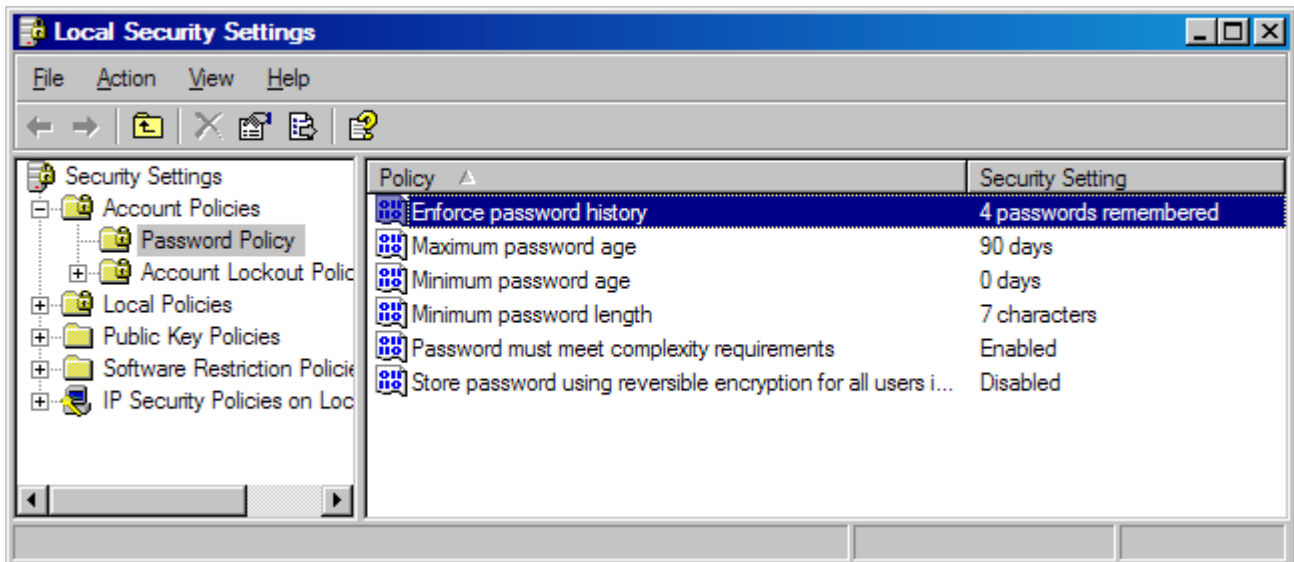
In order to meet the compliance requirements, you will need to observe the following:

- Do not use default administrative accounts for payment application logins (e.g., don't use the "Administrator" account to log in to).

- Assign secure authentication to these default accounts (even if they won't be used), and then disable or do not use the accounts.
- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
- See **“Windows password policies”**, **“Windows account lockout policies”**, and **“Screensaver and idle lockout”** below for instructions on how to configure Windows to comply with the PCI standards.

### Windows password policies.

Windows provides the ability to configure password policies. To access this configuration, go to Start > Control Panel > Administrative Tools, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Password Policy**.



You will need to use the following settings:

- Enforce password history: 4 passwords remembered
- Maximum password age: 90 days
- Minimum password age: 0 days
- Minimum password length: 7 characters
- Password must meet complexity requirements: Enabled

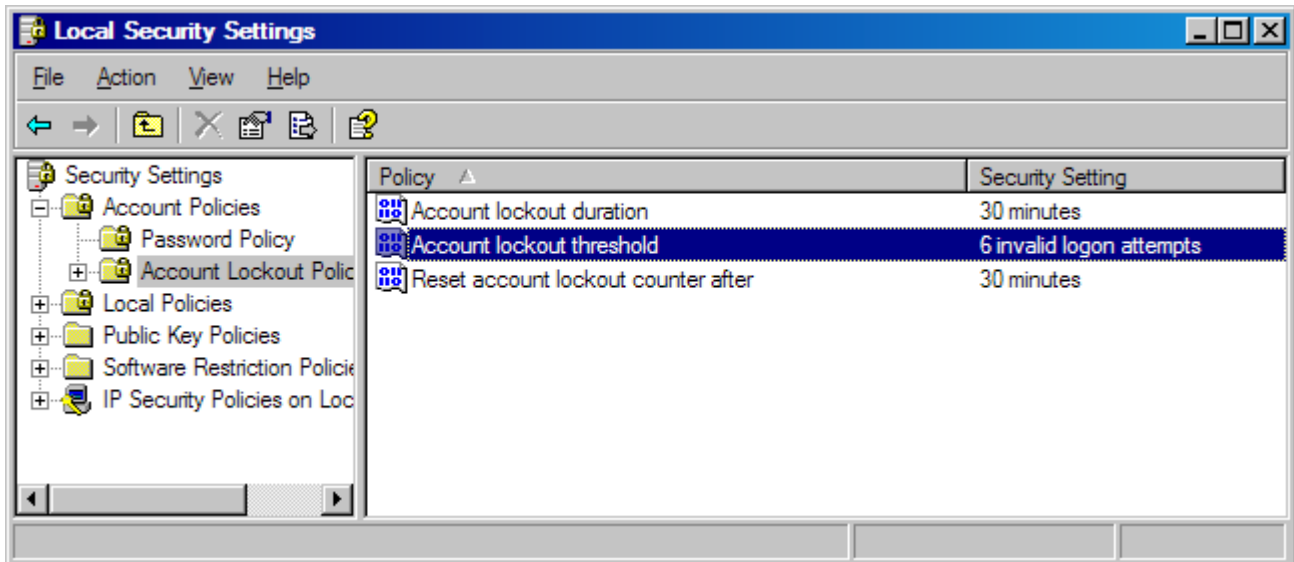
- Store password using reversible encryption: Disabled

Note that “Password must meet complexity requirements” will enforce the following requirements for all Windows passwords:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, \$, #, %)
- Complexity requirements are enforced when passwords are changed or created.

### Windows account lockout policies.

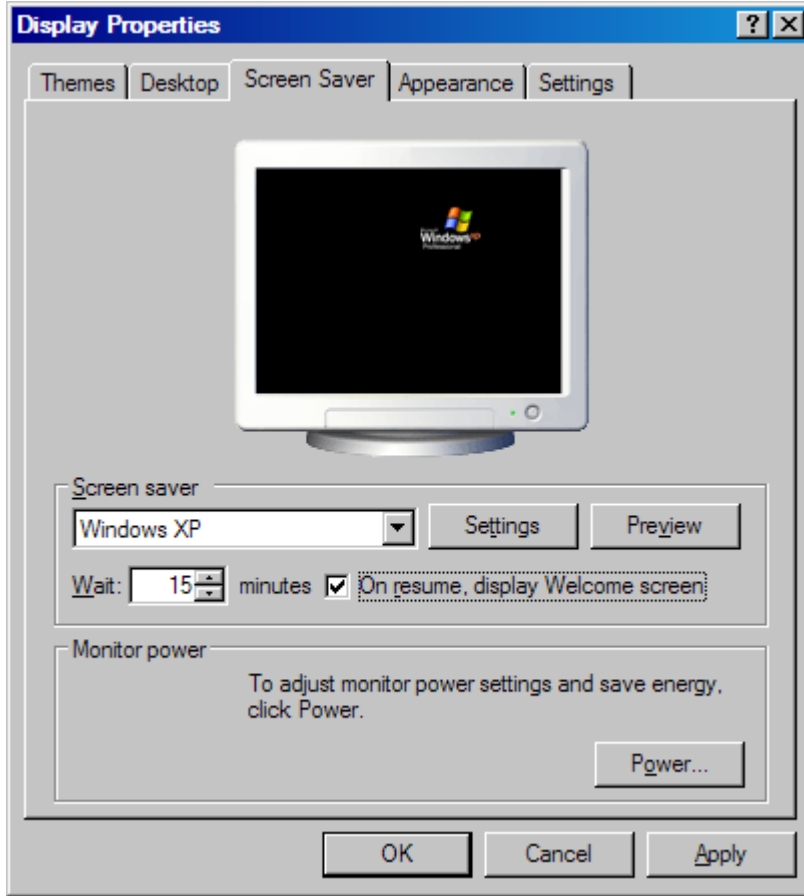
Windows provides the ability to configure account lockout policies. To access this configuration, go to Start > Control Panel > Administrative Tools, and open **Local Security Policy**. Expand **Account Policy** from the tree menu on the left, and click **Account Lockout Policy**.



You will need to make the following changes:

- Account Lockout Duration: 30 (minutes)
- Account Lockout Threshold: 6 invalid login attempts
- Reset account lockout counter after: 30 (minutes)

### Screen saver and idle lockout.



Windows provides the ability to lock the computer after the computer has been idle for a period of time and when the screen saver is active. To access this configuration, right-click on the Desktop and choose Properties or select Start > Control Panel > Display. Select the Screen Saver tab. Select a screen saver option (e.g. Windows XP), set the wait time, and check the box for “On resume, password protect”. Click Apply or OK to save the changes.

## 4. Automated Audit Trails

### Implement automated audit trails (PA-DSS 4.2)

How does TrackedValue meet the compliance requirement...

Logging is mandatory in TrackedValue VPT and cannot be disabled. The log format is a predefined to ensure compliance. TrackedValue VPT logs user and program activity to the Windows application & security logs.

To access the Windows logs, go to Start > Control Panel > Administrative Tools and open **Event Viewer**. To view user login activity and to track which accounts / users are accessing your system, select **Security** from the tree view on the left. To view application activity, including activity for TrackedValue VPT, select **Application** from the tree view on the left.

What you need to do to meet the compliance requirement...

Regularly review the Windows event logs, in particular the Security logs, to look for any suspicious or unauthorized activity.

## 5. Develop Secure Payment Applications

### Do not use Unnecessary or Insecure Services and Protocols

How does TrackedValue meet the compliance requirement...

TrackedValue VPT uses secure protocols and services only. We do not require the site to have any insecure services or protocols active for the normal operation of our software.

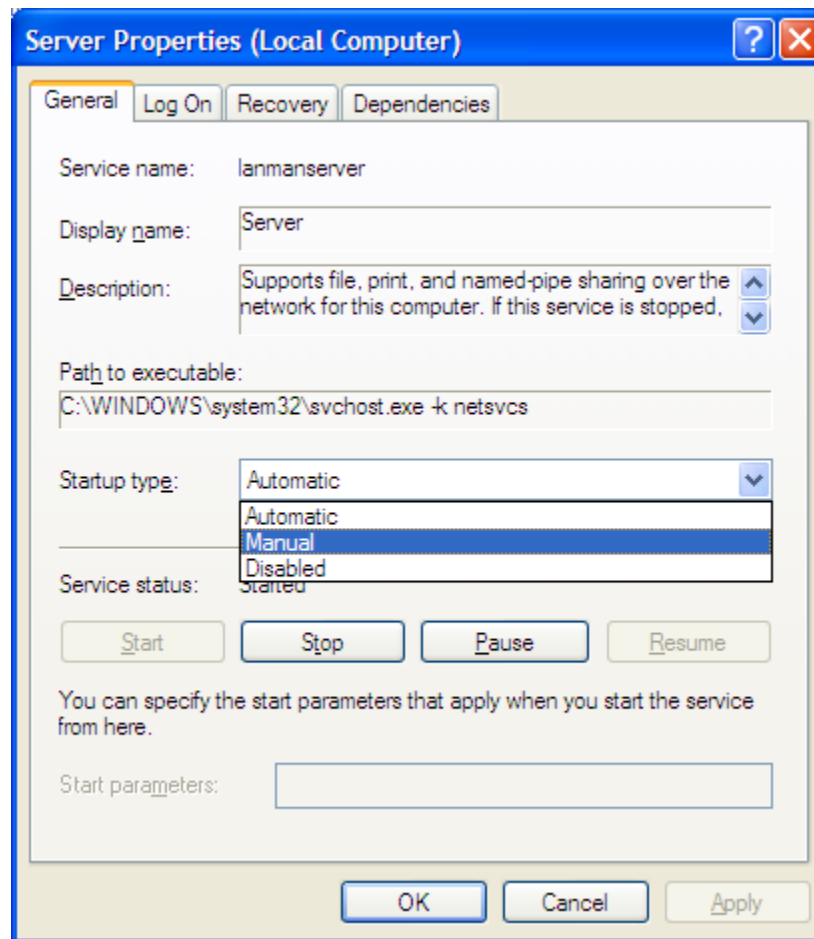
What you need to do to meet the compliance requirement...

In order to meet the compliance requirements you should not be running insecure services or protocols. A few specific services that should be stopped or blocked are:

- Telnet
- File and Print Services (broadcasting as a server, not acting as a client)
- FTP (unsecure)
- Internet Information Server (IIS) or other HTTP web server
- Remote Registry Service
- SMTP or POP email service (broadcasting as a server, not acting as a client)

Steps to Disable Unnecessary Services in Windows

1. Open the Windows service management console by clicking Start > Run and typing `services.msc` and click OK
2. Double click a particular service and set its Startup type to *Manual* or *Disabled*



3. Click OK

## 6. Provide a Secure Network

### Securely implement wireless technology (PA-DSS 6.1 and PA-DSS 6.2)

How does TrackedValue meet the compliance requirement...

TrackedValue VPT treats all transmissions over any network, including the local LAN, as potentially open and public. Whenever a PAN leaves the local TrackedValue VPT system all cardholder data is encrypted and protected. If the data is travelling to another point on your LAN that is part of the VPT chain, then the destination will have the encryption keys to decrypt and use the data as needed.

Whenever sensitive information is leaving the system running TrackedValue VPT the data is fully protected. It is either travelling to the Merchant Processing Bank over a SSL connection or it is a PAN being stored in the TrackedValue VPT database and it's encrypted before leaving the local computer. Basically, we treat every network connection as a potentially hostile connection and protect the data accordingly.

## What you need to do to meet the compliance requirement...

In order to meet the compliance requirements, you must observe the following:

- If a wireless network is being used, a firewall must be used as well. We recommend using both a hardware firewall and software firewall for maximum security. For laptops, a software firewall is highly recommended if you travel with the laptop.
- WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) are no longer permitted for use as they considered insecure.
- Encrypt all wireless transmissions by using WiFi protected access using WPA2 technology, IPSEC VPN, or SSL/TLS.
- Change wireless vendor defaults, including but not limited to, default service set identifier (SSID), passwords, and SNMP community strings.
- Disable SSID broadcasts.
- Install personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

## Store cardholder data safely away from the Internet (PA-DSS 9.1 and PA-DSS 12.1)

### How does TrackedValue meet the compliance requirement...

TrackedValue VPT meets compliance requirements by:

- Encrypting any data transmitted over the Internet by SSL
- Not requiring the server to sit in the DMZ or on an Internet-accessible system.
- Residing behind a firewall without any publicly accessible ports open from the Internet.

## What you need to do to meet the compliance requirement...

In order to meet the compliance requirements, you must observe the following:

- You need to install, configure, and maintain a firewall between your TrackedValue VPT system and the public Internet.
- You need to install, configure, and maintain Anti-Virus software on your TrackedValue VPT system.

## Encrypt cardholder data sent over end-user messaging technologies (PA-DSS 12.2)

### How does TrackedValue meet the compliance requirement...

TrackedValue VPT does not incorporate any end-user messaging capabilities within the software.

What you need to do to meet the compliance requirement...

Never transmit a card number over open email or in any kind of user-to-user chat tool that is not known to be a secure, encrypted channel.

## **7. Secure Delivery of Payment Application Updates (PA-DSS 10.1)**

How does TrackedValue meet the compliance requirement...

TrackedValue VPT makes secure updates available to registered users of the software. TrackedValue VPT is protected by a Code Signing Certificate in our office. End users can easily verify that the source provider of the application is legitimate. If the executable code has been tampered with in any way after leaving our office the certificate will interrupt the normal operation of the software and alert the end user.

Updates can be retrieved from our secure website by following the "Download our software" link from our website at [www.mtxinc.com](http://www.mtxinc.com). This will redirect you to a SSL secured web page to download the latest application.

What you need to do to meet the compliance requirement...

Register your software with us providing your contact information to be eligible for security patches and updates.

## **8. Secure Remote Access to the Payment Application (PA-DSS 11.2 and PA-DSS 11.3)**

How does TrackedValue meet the compliance requirement...

There is no direct remote access capability to TrackedValue VPT. The software will successfully work with common two-factor remote access tools such as LogMeIn and GoToMyPC. Other remote access tools may be used when a secure, VPN tunnel has been established between the client system and the TrackedValue VPT server.

On occasion, you may need to provide data to TrackedValue support in order to troubleshoot a problem that you are experiencing with the software. Our policy regarding your data is as follows:

- We use the Join.ME (powered by LogMeIn) remote troubleshooting application whenever it is necessary to connect to your computer, which encrypts all traffic over SSL. It includes the following features:
  - Customers must invite the technician for each use or access.
  - Customers can choose to terminate the session at any time.
  - All traces of the Customer Applet disappear from the remote PC when the session is finished.
  - Employs end-to-end, 128-bit SSL encryption.
- Whenever possible, we will not gather data locally. Instead, we use remote troubleshooting applications that require your express permission to access your computer, and encrypt all traffic over SSL.
- We will never request sensitive cardholder data such as PIN's or PIN block numbers.
- Data is only gathered with your express permission, and only when required to resolve the specific problem.
- We will never gather data that is not needed to solve the specific problem.

- Data is encrypted and stored in locations that have limited / controlled access.
- Data is deleted immediately after use.

### What you need to do to meet the compliance requirement...

If you require remote access to TrackedValue VPT, we recommend you use a secure remote access application such as LogMeIn (<http://www.logmein.com/>) or GoToMyPC (<http://www.gotomypc.com/>). These are applications that we are familiar with and can verify that they meet the security requirements. If you choose to implement an alternate application for this purpose, it must utilize at least a two factor authentication method and the data must move over a secure connection between the site and the remote workstation.

For remote locations and branch offices, we recommend you establish a VPN between the sites to facilitate secure intra-site communications.

## **9. Encryption Non-Console Administrative Access (PA-DSS 13.1)**

### How does TrackedValue meet the compliance requirement...

There is no non-console administrative access as part of TrackedValue VPT. In addition, TrackedValue VPT fully supports the use of VPN and SSL connections for remote user / site access.

### What you need to do to meet the compliance requirement...

Whenever you are connecting remotely to the server remotely you MUST use a secure connection. Technologies such as SSH, SSL/TLS, or encrypted VPN's will ensure that the data is fully encrypted between your system and the server.

Telnet or rLogin must never be used for administrative access.

## **10. Key Management Techniques**

### Compliance with Standards

All sensitive data stored in the TrackedValue VPT files, including PAN's, are encrypted using a salted SHA-512 hash and AES-256 encryption with a modified Initialization Vector.

TrackedValue VPT uses a dual-key system with a Key Encrypting Key (KEK) and a Data Encrypting Key (DEK). The salt used in the hash is controlled by the software and not user input.

### Key Storage Method

The Data Encrypting Key is encrypted by the Key Encrypting Key and stored with the cardholder data. The Key Encrypting Key is stored on a removable or remote drive and physically separated from the data.

### Key Rotation

Both of the keys are manually generated by a user with the appropriate privilege. The age of the key is recorded in the system and the users receive warnings that the keys should be changed as the 1 year anniversary approaches. Users are able to manually change the keys as frequently as they wish without any outside assistance or input.

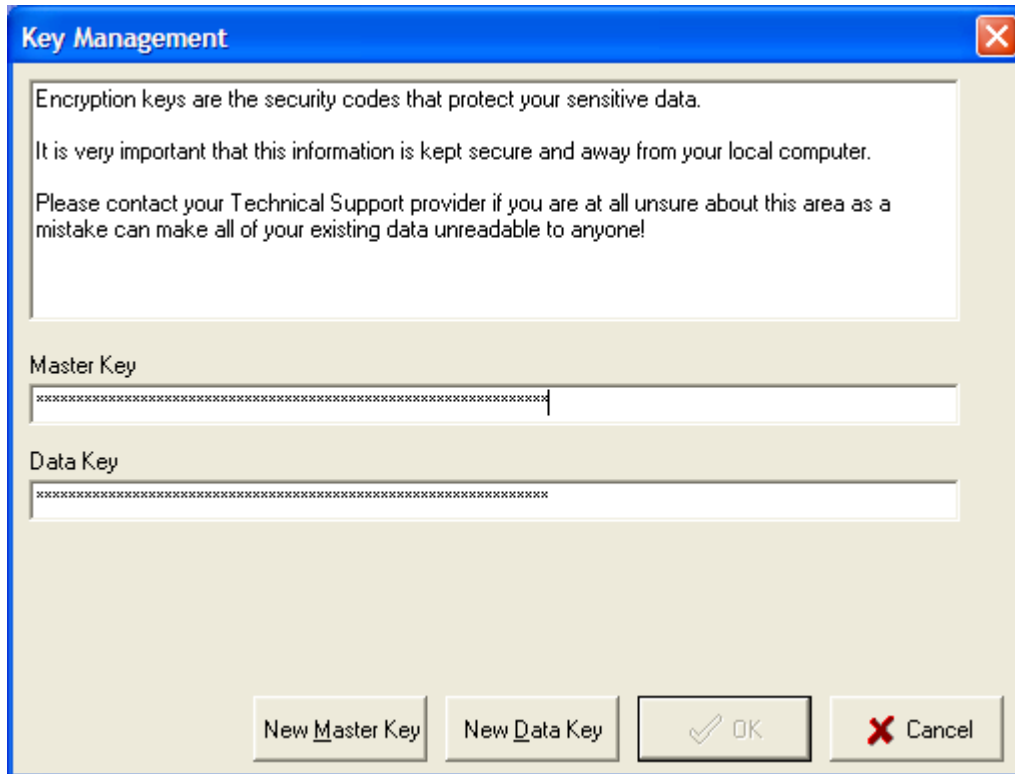
## Old Keys

Old encryption keys are overwritten whenever a new key is generated. As a result, old keys cannot be recovered.

## Refreshing Keys If Data Is Compromised

To manually refresh or rotate the encryption keys, please follow these steps:

- Make sure all other sites and users have exited the software
- Click the “Administration” Menu
- Click “Key Management” to see a screen similar to below



- Click “New Master Key” to generate a random 64 character Master Key
- Click “New Data Key” to generate a random 64 character Data Key
- As an additional security measure, you are welcome to change any characters in the string. By changing anything on these keys yourself, you are adding an additional layer of randomness and security that the keys could not be predicted in any fashion.
- Click “OK” to create or update the current Key Signature File with the new Master Key information and update the current Data Key in the active VPT data file
- When you save a new Data Key, any existing data encrypted with the old data key will automatically be:
  - Retrieved from the data files
  - Decrypted using the old Data Key
  - Encrypted using the new Data Key

- Stored back in the data files for future use
- Click “Close” to complete the process and resume normal system operation
- Update all backup copies of the Key Signature File with the new Key Signature File.

## 11. *Third Party Tools*

### Compliance with Standards

In some instances, TrackedValue VPT uses Third Party tools that are manually installed to connect to specific Merchant Processors. It is vital that you use PA-DSS compliant versions of any additional Third Party tools or order to maintain the PCI Compliance of a site.

TrackedValue VPT is capable of using Datacap's Net-ePay DSIClientX software to communicate to Net-ePay servers. You must install version 2.50 Build 385 or later to maintain your compliance. We highly recommend that you obtain the latest DSIClientX direct from the the developers website located at <http://www.datacapepay.com/dsIClient.htm>.

## Appendix “A” - Sample Key Custodian Form

### Compliance with Standards

All companies must have any employee with access to the Security Keys sign a Key Custodian Form acknowledging their awareness of their responsibilities in this area. This form should be permanently kept in their personnel file.

How does TrackedValue meet the compliance requirement...

You will find a sample Key Custodian Form on the next page that you may use to meet this requirement

# Key Custodian Form

All \_\_\_\_\_ (“Company”) staff that hold responsible authorized positions where they manage or handle encryption keys must sign the following document.

As a condition of continued employment with the Company, and as an employee that has access to key management tools and equipment, you are obligated to sign the following to indicate acceptance of your responsibility.

The signatory of this document is in full employment with the Company on the date shown below and has been afforded access to key management devices, software and equipment, and hereby agrees that, he or she

- Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of his/her ability, and has been trained in security awareness and has had the ability to raise questions and has had those questions answered satisfactory.
- Understands that non-compliance with the key management procedures can lead to disciplinary action including termination and prosecution.
- Exceptions to compliance only occur where such compliance would violate local, state, or federal law, or where a senior officer of the Company or law enforcement officer has given prior authorization.
- Agrees to never divulge to any third party any key management or related security systems, passwords, processes, security hardware or secrets associated with the Company systems, unless authorized by an officer of the Company or required to do so by law enforcement officers
- Agrees to report promptly and in full to the correct personnel, any suspicious activity including but not limited to key compromise or suspected key compromise. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.

I agree to the above and understand that this original copy will be held on my personnel record and kept by the company indefinitely.

## Employee

Signed: [ \_\_\_\_\_ ] Witnessed:[ \_\_\_\_\_ ]

Print Name: [ \_\_\_\_\_ ] [ \_\_\_\_\_ ]

Date: [ \_\_\_\_\_ ]

## Management Approval

Signed: [ \_\_\_\_\_ ]

Print Name: [ \_\_\_\_\_ ] [ \_\_\_\_\_ ]

Title: [ \_\_\_\_\_ ]

Date: [ \_\_\_\_\_ ]