PA-DSS Implementation Guide
For
OneTouch® Suite

Version 4.114.05.30, May 30, 2014
# Table of Contents

## INTRODUCTION
- Product Overview .......................................................... 1
- Document Purpose and Use .............................................. 2

## 1. BUILDING AND MAINTAINING A SECURE NETWORK ..... 5
- Installing firewall and router configurations ...................... 5
- Disabling vendor-supplied default accounts ..................... 8
- Developing system component configuration standards .......... 9
- Transmitting encrypted data ............................................. 10
- Encrypting all non-console administrative access .............. 10

## 2. PROTECTING CARDHOLDER DATA ............................. 11
- Preventing magnetic stripe, validation code or PIN block data storage ......................................................... 11
- Inadvertent capture or retention of cardholder data ........... 12
- Storing cardholder data .................................................. 14
- Managing stored cardholder data .................................... 14
- Managing cryptographic material .................................... 16

## 3. MAINTAINING A VULNERABILITY MANAGEMENT PROGRAM 19
- Using and updating anti-virus software ............................ 19
- Maintaining secure systems and applications .................... 19

## 4. IMPLEMENTING STRONG ACCESS CONTROL METHODS ....... 20
- Restricting cardholder data access by business need-to-know .......................................................... 20
- Assigning unique ID and password to each application user .. 24
- Accessing cardholder data remotely .................................. 24
- Restricting physical access to cardholder data .................... 25

©2014 Triple E Technologies LLC All rights reserved
Training and monitoring administrator personnel .................. 26

5. MONITORING AND TESTING NETWORK .............................. 27
   Tracking network resources and cardholder data access .... 27
   Testing security systems and processes ............................ 28
   Delivering PCI-compliant software updates ........................ 29

6. MAINTAINING AN INFORMATION SECURITY POLICY ........... 30
   Establishing information security .................................. 30
   Sample security policy .............................................. 30
Introduction

Product Overview

Triple E Technologies LLC’s OneTouch® Suite Version 4.114.05.30 is a Microsoft Visual Basic 6.0 Point Of Sale (POS) application, developed and tested on PC platforms running Microsoft Windows XP Professional and 7, and designed for implementation on any aforementioned operating system. OneTouch® Suite uses Microsoft SQL Server 2012 and above for its database.

In keeping with industry payment application best practices and for purpose of compliance with the Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS), OneTouch® Suite includes the following security features:

- Use of Microsoft Windows’ built-in, host-based firewall to protect cardholder data; firewall drops all incoming traffic not corresponding to traffic sent in response to a host request.

- Disabled or removed vendor-supplied defaults for passwords and other security parameters prior to system use.

- Non-retention of payment card authentication data; full magnetic stripe, PIN and card validation code data are not stored, and account numbers are encrypted. Except when an employee has physical possession of a customer payment card, the full account number is never revealed.

- Supported use and updating of anti-virus software, with specific configuration settings for OneTouch® Suite servers.

- Assignment of specific User access rights and permissions based on predefined group accounts and merchant-determined privileges.

- Windows authentication of user login credentials; presentation and authorization of a unique ID and password required for each user requesting access to OneTouch® Suite.

- Event logging of user activities such as logins, logoffs, security rights changes and accesses to database objects.

In keeping with PCI requirements, the following Windows services, protocols, components and dependent software are required for OneTouch® Suite application functionality:

Windows Services

- Agere Modem Call Progress Audio
- Base Filtering Engine
- ccEngineNTService
- COM+ Event System
- Computer Browser
- Cryptographic Services
- DCOM Server Process Launcher
- Desktop Window Manager Session Manager
- DHCP Client
- Diagnostic Policy Service
- Diagnostic Service Host
- Distributed Link Tracking Client
- DNS Client
- EEEGuardianService
- EEEPluginScheduler
- Function Discovery Provider Host
- Function Discovery Resource Publication
- Group Policy Client
- Identity Finder Endpoint Service
- IKE and AuthIP IPsec Keying Modules
- IP Helper
- IPsec Policy Agent
- Microsoft Antimalware Service
- Net Driver HPZ12
- Network Connections
- Network List Service
- Network Location Awareness
- Network Store Interface Service
- Offline Files
- Plug and Play
- Pml Driver HPZ12
- Power
- Print Spooler
- Program Compatibility Assistant Service
- Remote Procedure Call (RPC)
- RPC Endpoint Mapper
- Security Accounts Manager
- Security Center
- Server
- Shell Hardware Detection
- SQL Server (MSSQLSERVER)
- SQL Server (SQLEXPRESS)
- SQL Server Browser
- SQL Server VSS Writer
- SSDP Discovery
- Superfetch
- System Event Notification Service
- Task Scheduler
- TCP/IP NetBIOS Helper
- TeamViewer 8
- Telephony
- Themes
- tPortControllerNTService
- User Profile Service
- uvnc_service
- Vigilix POS-Sentry Agent
- Vigilix POS-Sentry Agent Guardian
- Windows Audio
- Windows Audio Endpoint Buidle
- Windows Connect Now - Config Registrar
- Windows Defender
- Windows Event Log
- Windows Firewall
- Windows Font Cache Service
- Windows Management Instrumentation
- Windows Media Player Network Sharing Service
- Windows Search
- Windows Update

**Protocols**
- TCP/IP
- HTTPS/SSL
- UDP
- DHCP

**Components**
- FarPoint Spread 6.0
- Farpoint TabPro 3.1
- MS Comm Control 6.0
- MS MAPI Control 6.0
- MS NT Service Control
- MW Windows Common Control 6.0(SP6)
- MS Winsock Control 6.0
- Sax Comm Objects 7
- Sonic Progress Bar ActiveX control
- eeeButton
- MS Windows Common Controls 5.0(SP2)
- OPOS Controls
- PinPad ActiveX Control
- Sheridan 3D Controls
- SigPlus OLE Control
- Sonic Skinner ActiveX Control
- Sonic Click Ultra Button ActiveX Control
- MS Calendar control 8.0
- MS Common Dialog Control 6.0
- MS FlexGrid Control
- MS Masked Edit Control
- MS Rich Textbox Control
- MS Tabbed Dialog Control
- vbAccelerator Image List Control
- vbAccelerator VB6 PopMenu Control

**Dependent Software**
- MS Windows 7 - O/S
- MS VB 6 - Application programming
- MS Visual Studio .NET - Application programming
- MS SQL Server 2012 - for DB

*Note: There are no dependent hardware requirements.*
Document Purpose and Use

This guide provides general and detailed instructions for implementing OneTouch® Suite 4.114.05.30 into your business environment in a manner compliant with the Payment Card Industry (PCI) Data Security Standard (PCI-DSS). The PCI-DSS is a set of security standards created by the PCI Security Standards Council to guide development, implementation and use of payment card applications.

Please note that this document is not intended as a complete implementation guide for OneTouch® Suite; rather, it provides guidelines and instructions only for implementing OneTouch® Suite in a manner that facilitates and supports compliance with established PCI standards.

This guide applies only to OneTouch® Suite 4.114.05.30, and only as formally released by Triple E Technologies LLC. Any subsequent modification of the application and/or the PCI-DSS must be reviewed and evaluated to determine continued PCI compliance.

Triple E Technologies LLC makes this guide available to OneTouch® Suite owners and their designees. Triple E Technologies LLC will update the guide annually, or sooner if otherwise demanded by either product or PCI-DSS requirements. Updates can be obtained by going to the Triple E Technologies LLC website at http://www.e3tek.com. Triple E Technologies LLC will also publish and distribute updates as need arises.

For purpose of this guide, the following versions of PCI requirements and standards apply:

- PCI-DSS Version 2.0
- PA-DSS Version 2.0
1 Building And Maintaining A Secure Network

Using a VPN Router

For purpose of secure OneTouch® Suite implementation and subsequent operation, Triple E Technologies LLC strongly recommends use of a VPN router to establish the DMZ, provide secure, encrypted remote system logins and ensure that all data on the network is encrypted. VPN router configuration should follow these standards:

- Restrict inbound Internet traffic only to protocols necessary for the cardholder data environment; specifically deny all other inbound traffic.
- Use two-factor authentication (e.g., user name and password and token or certificate) for Triple E Technologies LLC support access
- Use two-factor authentication for individual user remote access accounts
- Limit external outgoing internet traffic to only those sites required by the OneTouch® Suite application, or as specified to meet business needs
- Do not use default passwords
- Require use of personal firewall product for connecting laptop or personal computer

Installing Firewall and Router Configurations

PCI-DSS 1.1-1.5 require OneTouch® Suite system owners to install network firewall and router configurations to protect cardholder data from unauthorized public access (Internet, other networks and hosts). In keeping with this requirement, adhere to the following standards and procedures before and after implementing OneTouch® Suite into your network environment.

NOTE: For general firewall or router installation instructions, refer to documentation provided with product.

1. Establish and at least quarterly review formal Change Management process for approving, testing and implementing external network connections and changes to firewall and router configurations. Ensure change process allows identification of both before and after configuration topologies. Capture change history by generating report detailing new services allowed and existing services denied as result of configuration change(s).

2. Route all proposed configuration changes through Change Management process for approval and implementation.

3. Create and at least quarterly review diagram showing topology of all connections to OneTouch® Suite cardholder environment and cardholder data flows over the network. Ensure diagram is consistent with established firewall access policies.
And associated rules. Diagram must show OneTouch® Suite SQL server segregated from DMZ.

4. Credit Card data (and therefore OneTouch® Suite) must not reside on systems directly connected to the Internet. Thus, a network DMZ (Demilitarized Zone) must be set up to segment the network so that only machines on the DMZ are Internet accessible. DO NOT INSTALL OneTouch® Suite ON ANY SYSTEM THAT DIRECTLY ACCESES OR IS ACCESSED BY THE INTERNET.

5. Use the DMZ to filter and screen all traffic, and to prohibit direct routes for inbound and outbound Internet traffic. Ensure firewalls installed at each Internet connection and between Demilitarized Zone (DMZ) and internal network zone.

6. Limit all network device access to Administrators. Such access includes exclusive rights to:
   - Install, de-install or perform maintenance on any network device, or change the physical configuration of the firewall or router.
   - Make physical connections to a network device, including direct access ports and console ports.
   - Log in directly to a device console port or other direct access port.
   - Log in remotely to a network device.

7. Use same password policy for network device access as for Windows user accounts.

8. Whenever firewall or router suffers physical damage or there is evidence of tampering, fully evaluate event by means of hardware diagnostics and check physical configuration against existing documentation.

9. Compile list of allowed services, protocols and ports (e.g., Secure Sockets Layer [SSL], Virtual Private Network [VPN], etc.). Provide business justification for each listed item.

10. For each service, protocol and port deemed insecure (e.g., FTP), specify security features implemented in their behalf. Record exit interface, source and destination addresses and service (protocol/port number).

11. For each service other than HTTP, SSL, SSH or IPSEC (e.g., ICMP), identify and provide business justification for internal and external sub-nets using the service.

12. Provide policy and enforcement mechanism to ensure firewall and router rules sets are reviewed at least every six months.

13. Build and document firewall configuration that restricts connections between un-trusted networks and OneTouch® Suite. Limit inbound traffic only to that necessary for OneTouch® Suite cardholder data environment; deny all other inbound and outbound traffic using either explicit deny all or implicit deny after allow statements.

14. Compile list of external source and destination addresses, and classify them as either trusted or untrusted. Specify policies for each un-trusted host, first as
source and then as destination. Based on protocols connecting un-trusted hosts
to internal or DMZ networks, provide business reason for each policy in report.

15. Determine whether any wireless network traffic allowed into OneTouch® Suite
cardholder data environment. If so, identify services and analyze associated allow
policies and related rules. Devise and install perimeter firewall between wireless
network and OneTouch® Suite to control traffic only as in keeping with specified
policies and rules.

16. Identify firewall interfaces allowing traffic into OneTouch® Suite’s network and
DMZ networks. Determine services destined for cardholder environment; ensure
services are necessary and originate in an interface connected to an interface
within the DMZ. Devise and install DMZ to limit inbound and outbound traffic only
to protocols necessary for OneTouch® Suite cardholder data environment.

17. Ensure firewall limits inbound Internet traffic only to IP addresses within the
DMZ. Create policy stating all traffic between Internet and Internal networks is
denied.

18. Do not allow direct inbound or outbound traffic routes between Internet and
OneTouch® Suite cardholder data environment. Identify and remove any policy
or rule that allows Internet inbound/outbound traffic to pass through firewall if it
has cardholder data network either as source or destination.

19. Require outbound traffic from cardholder data environment to Internet access IP
addresses only within DMZ. Ensure cardholder data environment source and
destination policies consistent with and justified by business need.

20. Ensure firewall performs Stateful Packet Inspection (SPI) to keep track of
each network connection (e.g., TCP stream, UDP communication, etc.) traveling
across it. Confirm firewall can distinguish legitimate packets for different types of
connections, and that only packets matching known (“remembered”) connection
states can pass through.

21. Ensure firewall configuration has anti-spoofing rule to prevent internal addresses
from passing from Internet into DMZ.

22. Identify internal network segments accessible from outside and DMZ, including
routable addresses. Examine rule trails individually for natting. Ensure firewall
hides all internal network IP addresses.

23. Verify that all mobile and/or employee-owned computers having both network access
and direct Internet connectivity have personal firewall software installed and active. Ensure personal firewall software configured by Administrator in keeping
with standards contained herein and are not alterable by mobile computer users.

24. Except for one emergency account, do not configure local user accounts on
router. Router must require user authentication, and only Administrators should
have access. Ensure ‘enable password’ on router kept in secure, encrypted form
and set to current production password.

25. Ensure router denies all inbound and outbound traffic not specifically allowed.
Add router access rules as business needs arise.
26. Document all router configuration files. Secure router configurations through use of access and physical controls, and ensure configuration files are synchronized.

27. Ensure each router has following statement in clear view:

You have accessed a [company name] restricted device. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity we may provide the evidence of such activity to law enforcement.

Disabling Vendor-Supplied Default Accounts

PCI-DSS 2.1 requires OneTouch® Suite system owners to change or disable any administrative default account as provided by vendors to install operating systems, servers, databases and applications. In keeping with this strategy, Triple E Technologies LLC disables the Microsoft SQL Server “sa” account by means of forced Windows user login authentication. However, there are five other administrative default accounts associated with OneTouch® Suite that are not PCI compliant if used as-is. Therefore, to maintain system integrity and ensure continued PCI compliance, perform the following procedures both as part of OneTouch® Suite implementation and every ninety days thereafter. Secure authentication should be used for these accounts even if they are to be disabled or not used.

NOTE: While Triple E Technologies LLC does not recommend nor otherwise support implementing OneTouch® Suite into wireless environments, instructions for securing wireless connections may be found on Page 23 of this guide.

Procedures

Change passwords for any disabled and/or not-in-use accounts, and for the following OneTouch® Suite default accounts:

- Administrator
- SiteController
- POS
- Pedestal
- etekremote

For each such account, devise (strong) replacement password using the following complexity standard:

- At least seven characters.
- No user name, real name or company name.
- No complete dictionary word.
- Characters from each of the following four groups:
Group  Examples
Uppercase letters A, B, C ...
Lowercase letters a, b, c ...
Numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols ` ~ ! @ $ % ^ & ( ) _ + - = { } [ ] : ; ‘ < > ? . /

EXAMPLE: 4&q6md13?J

Next, replace default passwords with new passwords using Windows Local Users and Groups. You must logged-on as Administrator to perform functions associated with changing default account passwords.

Developing System Component Configuration Standards

PCI-DSS Requirements 2.2 and 12.9 mandate that system owners implement OneTouch® Suite into an environment that specifically limits services to, on and from servers and other system components. For this reason, OneTouch® Suite owners must implement and quarterly review system component configuration standards and policies that support or otherwise facilitate the following:

1. Addressing known system network component and critical server vulnerabilities in manner consistent with industry-accepted hardening and lockdown standards, as specified by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST) and Center for Internet Security (CIS).

2. Installing only those system components, especially servers, having documented business justification.

3. Using 128-bit encryption for all internal, non-console data transmission.

4. Using multiple security measures for each system component (e.g., configuring firewall to allow only certain IP addresses to connect to printer and altogether disabling printer on systems where not needed).

5. Following principle of least privilege by limiting system component access to and from only those sources for which demonstrated need has been provided.

6. Mandating clear, concise and simple configuration specification for each server service.

7. Providing logging and other automatic monitoring mechanisms to demonstrate enforcement of configuration standards for each new system component.

8. Calling for initial and periodic system component risk assessments based on analysis of specified configuration rules.

9. Identifying and calling for elimination or modification of configuration rules allowing insecure services.

10. Using security profiles to identify unique server functions and restrict or prevent access to associated services and protocols.
11. Limiting servers to only one primary function (e.g., SQL database implemented on one server, DNS on another, etc.).

12. Determining whether dedicated services have common source network segment and, if so, ensuring servers on the same network segment have same security level.

13. Deploying firewall rules to block all ports and protocols not directly needed to perform server’s specified function.

14. Providing common security parameter settings for system components and critical servers.

15. Auditing firewall configurations by running port scans to ensure unexpected ports not accessible.

**Transmitting Encrypted Data**

PCI-DSS Requirement 4.1 mandates use of strong cryptography and at least 128-bit encryption techniques (either at the transport layer with SSL or IPSEC or data layer with algorithms such as RSA or Triple-DSS) to safeguard cardholder data during transmission over public networks, including the Internet and Internet-accessible DMZ network segments. In this regard, OneTouch® Suite transfers all data to the card processor via SSL (https). If applicable, any data coming into your system over the Internet should also be submitted via SSL. Owners are advised that changing encryption settings below 128-bit encryption will result in PCI non-compliance.

**Encrypting All Non-Console Administrative Access**

OneTouch® Suite provides for non-console administrative access to the cardholder data environment (application and servers). Such access requires two-factor authentication and either SSH, VPN or SSL/TLS for encryption. To satisfactorily use encryption for SQL Server communications over a network, you must provide demonstrable means for:

1. Identifying all services to the firewall and their attendant rules and policies, and noting management services with administrative access.

2. Encrypting all communication between administrative console and firewall.

3. Ensuring interface access to all management services uses strong encryption technologies such as SSH, VPN and TLS-encrypted HTTPS protocol.

4. Reviewing system service and parameter files to ensure Telnet FTP, ‘r’ protocols and other remote login commands are disabled.
2 Protecting Cardholder Data

Preventing Storage of Full Magnetic Stripe, Validation Code or Value (CAV2, CID, CVC2, CVV2) or PIN Block Data

Current and previous OneTouch Suite® versions do not store magnetic stripe, card validation code or PINs/PIN block data. OneTouch Suite® software uses multiple passes of different strong encryption algorithms (3DES and RSA-2048) to ensure that such sensitive data never appears in any audit or application log files on the hard disk or stored in the database. The software takes advantage of Microsoft's SQL Server Data Encryption Hierarchy to protect all encryption keys and ensure that a compromised database cannot be used maliciously to extract sensitive data. Preventing storage of such confidential card payment data is required for PCI compliance. It is the merchant’s responsibility to ensure that the card payment transactions they process do not store magnetic stripe data, card validation codes, PINS or PIN block data, or cryptographic key material, even when such data is encrypted; it is OneTouch® Suite’s responsibility to provide the means. In this regard, such data enters OneTouch® Suite at one of the points of sale (e.g., Register, Pedestal, etc.) through a communications port, and once in one of the applications is used only in random access memory (RAM or Volatile Memory). While in the point of sale, any sensitive that may be logged to a text file is first masked using a masking algorithm to ensure such sensitive data is never logged to the hard disk.

Further, when any POS system sends data to ccEngine (the only application in OneTouch Suite® that authorizes credit cards), the data is encrypted in memory with a 128-bit 3DES algorithm before network submission to the SQL Server. After submission to SQL server, cardholder data is encrypted a second time using an RSA-2048 algorithm. It is upon receipt of this card processing request that ccEngine will decrypt the database data where it will reside for a short period in (RAM) unencrypted before submission to the card processor for authorization. Otherwise the PAN data always resides double encrypted in the database.

As regards personnel troubleshooting problems relating to OneTouch® Suite software, PCI compliance requires that you establish and enforce security policies for dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data). Such policies must include, but are not limited to, the following:

- Never download or store authentication data outside of client’s network
- Always encrypt sensitive cardholder data when being stored
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
Inadvertent capture or retention of cardholder data

PA-DSS 2.1 requires that you configure your underlying software or systems (e.g., OS, databases, etc.) in such manner as to prevent inadvertent capture or retention of cardholder data.

Encrypting the Page File

New systems shipped from Triple E have the Windows Paging File already encrypted and are set to clear pagefile.sys upon shutdown. However, to encrypt the Page File for an upgraded system, you must first ensure your computer hard disk is formatted using NTSF, and then perform the following steps:

1. On Windows task bar, click Windows “orb”, and then type cmd in search window.
2. On menu that displays, right-click cmd.exe, and then click Run as Administrator on next menu.
3. At prompt, type fsutil behavior set EncryptPagingFile 1 to encrypt page file.
4. To verify configuration, type fsutil behavior query EncryptPagingFile; EncryptPagingFile=1 message displays.

Disabling Page File encryption

In event you need to disable Paging File encryption:

1. On Windows task bar, click Windows “orb”, and then type cmd in search window.
2. On menu that displays, right-click cmd.exe, and then click Run as Administrator on next menu.
3. At prompt, type fsutil behavior set EncryptPagingFile 0.
4. To verify configuration, type fsutil behavior query EncryptPagingFile; EncryptPagingFile=0 message displays.

Clearing the Page File

New systems shipped from Triple E are preset to clear pagefile.sys upon shutdown, thereby purging all temporary data such as application passwords and cardholder PANs. However, to clear the Page File for an upgraded system, you must first perform the steps outlined below. Note that the result of such performance may increase your Windows shutdown time.

1. On Windows task bar, click Windows “orb” and then type regedit in search window.
2. On menu that displays, right-click regedit.exe, and then click Run as Administrator on next menu.
3. On Registry Editor, click HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management.
4. Do one of the following:

- Securely delete such data immediately after use
5. Create Registry entry:
   - Right-click in right pane;
   - Click **New**, and then click **DWORD (32 bit) Value**
   - Type **ClearPageFileAtShutdown**
   - Double-click entry to change value from **0** to **1**

6. Click **OK**; close **regedit**.

To disable restore points:

To disable system restore points:

1. On desktop, click **Start**, and then click **Run**. **Run** dialog displays:

   ![Run window](image.png)

   2. In **Open** window, type “**systempropertiesprotection**”, and then click **OK**; **System Properties** dialog displays:
3. Click **System Protection** tab.

4. Click **Local Disk (C:) (System)**, and then click **Configure; System Protection for Local Disk (C:)** dialog displays:

5. Click **OK** two (2) times.

6. Restart computer to update settings.

**Storing cardholder data**
Sensitive cardholder data must always be encrypted when being stored. Per PCI-DSS Requirements 1.3 and 1.3.4, never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.) Although OneTouch® Suite does use Microsoft SQL Server to distribute the application internally to your network, this server should NOT be used for any external web applications. It is recommended that access to this server from the Internet be severely restricted through use of a VPN firewall. Please see the section on remote access for clarification on how to use VPN access to view OneTouch® Suite data remotely.

Managing stored cardholder data

OneTouch® Suite Version 4.114.117 includes provision for purging historical data on a regular basis (according to schedule you establish). OneTouch® Suite by default is configured to specify clearing encrypted card data after one calendar year. If you have a business reason for keeping card data for less than one-year, you may change the default setting to any period less than the default. Keep in mind, however, that OneTouch® Suite does not retain this data anywhere else in the system; once purged, the data is irretrievable and gone forever.

The following guidelines must be followed when dealing with cardholder data (either PAN alone or with expiry date, cardholder name or service code):

- Establish policy with business justification for sensitive data retention
- Purge data exceeding defined retention period

Listed below are the storage locations of cardholder data that should be purged:

- ccEngine database
  - ccRequests
  - CardsLockedOut
- rICustomerData Database
  - PendingSettlements
  - SalePayments

Purging cardholder data

You must be logged-on as either Administrator or PCI User to perform cardholder data purge functions. To delete selected cardholder data following OneTouch® Suite implementation, follow the procedure below:

1. From OneTouch DataManager Connect menu, click File, and then click Purge Credit Card Data in drop down menu
2. In Purge Credit Card Data dialog, type end date through which you wish to purge stored credit card data.

3. Click Purge.

NOTE: A credit card purge history record will be generated for each purge transaction. Administrators and PCI Users may view audit logs of these transactions in SQL Server 2012 and above Management Studio.

Managing cryptographic material

In keeping with PCI-DSS Requirement 3.6, all cryptographic material (encryption keys and encrypted cardholder data) must be securely removed. In this regard, the process of implementing OneTouch® Suite Version 4.114.117 will automatically purge encrypted data from previous transactions. Removal of this cryptographic material is absolutely necessary for PCI compliance.
Following implementation, system encryption keys must be changed at least annually and whenever deemed necessary or prudent because of actual or suspected security compromise. Keys must also be changed whenever anyone with knowledge of them changes positions or leaves the company. OneTouch® Suite provides system functionality to securely change encryption keys currently used to protect cardholder data, and will automatically change encryption keys annually if not otherwise performed more frequently.

Encryption Storage Key

Data encryption keys are protected by Microsoft SQL Server key encryption and protection mechanisms. All utilized keys are stored and protected in separate levels of hierarchy. Databases ccEngine, esController and rlCustomerData each contain the Asymmetric key eeeCCKey. This key is unique to each database and protected by the same Microsoft SQL Server protection mechanisms.

Viewing Audit Logs on a Centralized Log Server

Trace files automatically generated by the SQL Server for events related to card processing, encryption key maintenance and other significant events are logged to the C:\EEETechnologies\EEETrace folder and its sub-folders on the Navigator SiteController machine. These files must be transferred to a centralized logging server on a regular interval to avoid system shutdown due to the primary disk storage being exhausted.

All of the .trc audit logs can be reviewed with a SQL Trace/Profiler application. A customer can utilize the .trc audit logs that have been transferred to a log server inside SQL Server Profiler or equivalent viewer. It is through utilization of the profiler or other viewer application that customers gain the ability to view the audit logs on a centralized log server.

Encryption Key Custodian

PA-DSS 2.6 requires each Administrator or other person assigned encryption key custodianship responsibilities to formally sign a document indicating they understand and acknowledge their assigned responsibilities. A sample form is provided below:

<table>
<thead>
<tr>
<th>Encryption Key Custodianship</th>
</tr>
</thead>
<tbody>
<tr>
<td>The undersigned herewith acknowledges understanding and acceptance of all responsibilities assigned as &lt;Company Name&gt; Encryption Key Custodian.</td>
</tr>
<tr>
<td>Custodian Name: _______________ Approved By: ____________________</td>
</tr>
<tr>
<td>Custodian Signature: _______________ Approver Signature: ____________________</td>
</tr>
<tr>
<td>DATE: <em><strong><strong>/</strong></strong></em>/_______ DATE: <em><strong><strong>/</strong></strong></em>/_______</td>
</tr>
</tbody>
</table>
Changing encryption keys

You must be logged-on as Administrator to perform the encryption key maintenance function. To change the encryption key following OneTouch® Suite implementation, follow the procedure below:

1. From OneTouch DataManager **Connect** menu, click File, and then click Encryption Key Maintenance in drop-down menu.

Change Encryption Key dialog displays:

![Change Encryption Key Dialog](image)

2. Click Create.

**NOTE:** OneTouch® Suite generates an Encryption Key Change record in the audit log each time encryption key maintenance is performed. All data encrypted with old keys will no longer be recoverable as the keys are forcibly removed.
5 Maintaining a Vulnerability Management Program

Using and Updating Anti-Virus Software

Because OneTouch® Suite runs on either Windows XP Professional or 7 over a network, PCI DSS requires system owners to protect the cardholder data environment against intrusion from without by viruses and other malicious software. In keeping with this requirement, ensure the following are in place and working before implementing OneTouch® Suite:

1. Information security policies and procedures establishing requirements and responsibilities for installing, configuring and running anti-malware software.

2. Mechanisms for enforcing established anti-malware policies and procedures, including generation of audit logs demonstrating anti-malware software currency, potency and use.

3. Deployment of anti-malware software on OneTouch® Suite and all interfacing services and systems.

4. Anti-malware software settings sufficient to detect and remove all known viruses, spyware and adware while permitting security patches and other software updates from authorized sources.

Maintaining Secure Systems and Applications

For purpose of best industry practice and PCI compliance, OneTouch® Suite system owners must make every effort to protect the cardholder data environment from exploitation by employees and external hackers. In keeping with this requirement, ensure the following are in place and working both before and ongoing after OneTouch® Suite implementation:

1. Information security policies and procedures establishing responsibilities and process for installing Triple E Technology-supplied security patches.

2. Information security and daily operating policies and procedures establishing responsibilities and process for installing Triple E Technologies LLC-supplied software updates.

3. Performance standard calling for installation of all OneTouch® Suite security patches and software updates within thirty days of receipt from Triple E Technologies LLC.

4. Change management program ensuring installation of OneTouch® Suite security patches and software updates follow established change control procedures.

5. Provision in change management program for documenting OneTouch® Suite update performance and impact, back-out procedures and management sign-off.
Implementing Strong Access Control Methods

Restricting Cardholder Data Access by Business Need-To-Know

OneTouch® Suite strongly advises limiting access to any PCs, servers and databases with cardholder data by requiring unique User IDs and passwords for purpose of secure authentication. OneTouch® Suite does not have provision for setting up user accounts and relies on Microsoft Windows functionality to setup user accounts and assign users to user groups. A Windows user account defines the actions a user can perform by establishing the privileges (rights and permissions) for that user. Each OneTouch® user must be a member of at least one user group. The rights and permissions assigned to a user group are the same for all members of that group.

OneTouch® is pre-configured with five distinct user groups with the appropriate privileges already assigned. The privileges associated with each user group are described below. As good practice, you should assign users to the group or groups having the least privileges allowing satisfactory performance of assigned duties. For reason of system integrity and PCI compliance, never modify the privileges assigned to OneTouch® user groups.

Administrator Group
An Administrator Group account can make system-wide changes, install programs and access all files on the computer. Only an Administrator has complete access to other user accounts. An Administrator Group member can:

- Create, change and delete user accounts.
- Create, reset and delete user account passwords.

Administrator Group members cannot change their own account type to another account type unless there is at least one other user with an Administrator account type. This is to ensure that there is always at least one Administrator in the system.

Administrators have the following OneTouch® Suite rights and permissions:

<table>
<thead>
<tr>
<th>System Menu Functions</th>
<th>Reports</th>
<th>Database Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Customer</td>
<td>Aged Trial Balance</td>
<td>Adjustment Reasons</td>
</tr>
<tr>
<td>Add Purchase Order</td>
<td>Checks By Shift</td>
<td>Bad Check Names</td>
</tr>
<tr>
<td>Add Item</td>
<td>CP720 Gallon Summary</td>
<td>Card types</td>
</tr>
<tr>
<td>Adjust Inventory</td>
<td>Credit Card Reconciliation</td>
<td>Customer Categories</td>
</tr>
<tr>
<td>AR Reports</td>
<td>Credit Card Volume And Charges</td>
<td>Customer Pricing</td>
</tr>
<tr>
<td>Archive Records</td>
<td>Credit Limit</td>
<td>Customers</td>
</tr>
<tr>
<td>Change Prices</td>
<td>Customer Activity</td>
<td>Discount Codes</td>
</tr>
<tr>
<td>Clear Limits</td>
<td>Customer Drivers</td>
<td>Employees</td>
</tr>
<tr>
<td>Create AR Reports</td>
<td>Customer Fuel History Summary</td>
<td>Export Definitions</td>
</tr>
<tr>
<td>Credit Card Search</td>
<td>Customer Pricing and Discounts</td>
<td>Gift Cards</td>
</tr>
<tr>
<td>Edit Private Cards</td>
<td>Customer Sales Summary</td>
<td>Import Definition</td>
</tr>
<tr>
<td>Encryption Key Maintenance</td>
<td>Daily Card Sales</td>
<td>Inventory Adjustments</td>
</tr>
<tr>
<td>Export Data</td>
<td>Daily Journal Report</td>
<td>Inventory Categories</td>
</tr>
<tr>
<td>Generate Finance Charges</td>
<td>Daily Card Sales</td>
<td>Inventory Items</td>
</tr>
<tr>
<td>Generate Invoices</td>
<td>Daily Shift</td>
<td>Inventory Receipts</td>
</tr>
<tr>
<td>Generate Pin Numbers</td>
<td>Discounted Sales</td>
<td>Invoice List</td>
</tr>
<tr>
<td>Generate Priced Transactions</td>
<td>Dispensed Volume by Dispenser and</td>
<td>No Sale Reasons</td>
</tr>
<tr>
<td>Generate Statements</td>
<td>Dispenser Totals by Product and Dispenser</td>
<td>Other Payment Types</td>
</tr>
</tbody>
</table>
Administrator Group Rights and Permissions (continued)

<table>
<thead>
<tr>
<th>System Menu Functions</th>
<th>Reports</th>
<th>Database Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Barcodes</td>
<td>FET/SET Exemption</td>
<td>Pricing Categories</td>
</tr>
<tr>
<td>Import Receipt Details</td>
<td>Dyed Diesel Sales by Customer</td>
<td>Paid-Out Reasons</td>
</tr>
<tr>
<td>Inventory Adjustments</td>
<td>Employee Charges</td>
<td>POS Configuration</td>
</tr>
<tr>
<td>Inventory Receipts</td>
<td>Finance Charges</td>
<td>Pricing Levels</td>
</tr>
<tr>
<td>Inventory Reports</td>
<td>Fuel Sales By Date and Point Of Sale</td>
<td>Purchase Order Status Codes</td>
</tr>
<tr>
<td>Invoice List</td>
<td>Fuel Sales By Dispenser &amp; Product</td>
<td>Quick Menus</td>
</tr>
<tr>
<td>Payment Adjustments</td>
<td>Fuel Sales Volume by Dispenser</td>
<td>Sales List</td>
</tr>
<tr>
<td>Print Adjustment</td>
<td>Gallon Summary with Discounts</td>
<td>Sites</td>
</tr>
<tr>
<td>Print Receipt</td>
<td>Hourly Sales</td>
<td>Terms Codes</td>
</tr>
<tr>
<td>Purchase Order Maintenance</td>
<td>Inventory Adjustments</td>
<td>Units Of Measure</td>
</tr>
<tr>
<td>Purge Credit Card History</td>
<td>Inventory Receipts</td>
<td>Vendor Categories</td>
</tr>
<tr>
<td>Rebuild Item Balances</td>
<td>Rebuild Item Balances</td>
<td></td>
</tr>
<tr>
<td>Rebuild Sales Summary</td>
<td>Rebuild Sales Summary</td>
<td></td>
</tr>
<tr>
<td>Sales Entry</td>
<td>Sales Entry</td>
<td></td>
</tr>
<tr>
<td>Sales List</td>
<td>Sales List</td>
<td></td>
</tr>
<tr>
<td>Sales Reports</td>
<td>Sales Reports</td>
<td></td>
</tr>
<tr>
<td>Show Customer List</td>
<td>Show Customer List</td>
<td></td>
</tr>
<tr>
<td>Show Items List</td>
<td>Show Items List</td>
<td></td>
</tr>
<tr>
<td>Site Configuration</td>
<td>Site Configuration</td>
<td></td>
</tr>
<tr>
<td>Sites</td>
<td>Sites</td>
<td></td>
</tr>
<tr>
<td>Synchronize Site</td>
<td>Synchronize Site</td>
<td></td>
</tr>
<tr>
<td>System Options</td>
<td>System Options</td>
<td></td>
</tr>
<tr>
<td>Table Maintenance</td>
<td>Table Maintenance</td>
<td></td>
</tr>
<tr>
<td>Prepaid Card Status</td>
<td>Prepaid Card Status</td>
<td></td>
</tr>
<tr>
<td>Price Change History</td>
<td>Price Change History</td>
<td></td>
</tr>
<tr>
<td>Private Card Fuel Sales by Dispenser</td>
<td>Private Card Fuel Sales by Dispenser</td>
<td></td>
</tr>
<tr>
<td>Private Card Sales By Customer and Card</td>
<td>Private Card Sales By Customer and Card</td>
<td></td>
</tr>
<tr>
<td>Private Card Sales Summary</td>
<td>Private Card Sales Summary</td>
<td></td>
</tr>
<tr>
<td>Private Cards List</td>
<td>Private Cards List</td>
<td></td>
</tr>
<tr>
<td>Register Shift</td>
<td>Register Shift</td>
<td></td>
</tr>
<tr>
<td>Re-Order Limits</td>
<td>Re-Order Limits</td>
<td></td>
</tr>
<tr>
<td>Sales By Payment Method</td>
<td>Sales By Payment Method</td>
<td></td>
</tr>
<tr>
<td>Sales By Shift and Category</td>
<td>Sales By Shift and Category</td>
<td></td>
</tr>
<tr>
<td>Sales Detail by Date and Category</td>
<td>Sales Detail by Date and Category</td>
<td></td>
</tr>
<tr>
<td>Sales History with Signatures</td>
<td>Sales History with Signatures</td>
<td></td>
</tr>
<tr>
<td>Sales Profit Margins by Category</td>
<td>Sales Profit Margins by Category</td>
<td></td>
</tr>
<tr>
<td>Sales Volume by Hour</td>
<td>Sales Volume by Hour</td>
<td></td>
</tr>
<tr>
<td>Sales Volume Summary</td>
<td>Sales Volume Summary</td>
<td></td>
</tr>
<tr>
<td>Sales with Overridden Prices</td>
<td>Sales with Overridden Prices</td>
<td></td>
</tr>
<tr>
<td>Statements</td>
<td>Statements</td>
<td></td>
</tr>
<tr>
<td>Statements [Customer Name/Address Lowered]</td>
<td>Statements [Customer Name/Address Lowered]</td>
<td></td>
</tr>
<tr>
<td>Top Sellers by Category</td>
<td>Top Sellers by Category</td>
<td></td>
</tr>
<tr>
<td>Top Selling Merchandise</td>
<td>Top Selling Merchandise</td>
<td></td>
</tr>
</tbody>
</table>

Manager Group
With few exceptions, a Manager Group account provides access to system business functionality equal to that of the Administrator group. However, Managers cannot make system-wide changes, install programs or create or access other user accounts. A Manager Group member can:

- Perform most all database table maintenance functions with Add, Change and Delete privileges.
- Perform most all system menu functions, and create reports.

Manager Group members cannot change their own account type to another account type, or change password or password change frequency other than as prescribed.
Manager Group members have the following OneTouch® Suite rights and permissions:

<table>
<thead>
<tr>
<th>System Menu Functions</th>
<th>Reports</th>
<th>Database Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Customer</td>
<td>Aged Trial Balance</td>
<td>Adjustment Reasons</td>
</tr>
<tr>
<td>Add Purchase Order</td>
<td>Checks By Shift</td>
<td>Bad Check Names</td>
</tr>
<tr>
<td>Add Item</td>
<td>CP720 Gallon Summary</td>
<td>Card types</td>
</tr>
<tr>
<td>Adjust Inventory</td>
<td>Credit Card Reconciliation</td>
<td>Customer Categories</td>
</tr>
<tr>
<td>AR Reports</td>
<td>Credit Card Volume And Charges</td>
<td>Customer Pricing</td>
</tr>
<tr>
<td>Archive Records</td>
<td>Credit Limit</td>
<td>Customers</td>
</tr>
<tr>
<td>Change Prices</td>
<td>Customer Activity</td>
<td>Discount Codes</td>
</tr>
<tr>
<td>Clear Limits</td>
<td>Customer Drivers</td>
<td>Employees</td>
</tr>
<tr>
<td>Create AR Reports</td>
<td>Customer Fuel History Summary</td>
<td>Export Definitions</td>
</tr>
<tr>
<td>Credit Card Search</td>
<td>Customer Pricing and Discounts</td>
<td>Gift Cards</td>
</tr>
<tr>
<td>Edit Private Cards</td>
<td>Customer Sales Summary</td>
<td>Import Definition</td>
</tr>
<tr>
<td>Encryption Key Maintenance</td>
<td>Daily Card Sales</td>
<td>Inventory Adjustments</td>
</tr>
<tr>
<td>Export Data</td>
<td>Daily Journal Report</td>
<td>Inventory Categories</td>
</tr>
<tr>
<td>Generate Finance Charges</td>
<td>Daily Card Sales</td>
<td>Inventory Items</td>
</tr>
<tr>
<td>Generate Invoices</td>
<td>Daily Shift</td>
<td>Inventory Receipts</td>
</tr>
<tr>
<td>Generate Pin Numbers</td>
<td>Discounted Sales</td>
<td>Invoice List</td>
</tr>
<tr>
<td>Generate Priced Transactions</td>
<td>Dispensed Volume by Dispenser and Product</td>
<td>No Sale Reasons</td>
</tr>
<tr>
<td>Generate Statements</td>
<td>Dispenser Totals by Product and Dispenser</td>
<td>Other Payment Types</td>
</tr>
<tr>
<td>Import Receipt Details</td>
<td>Dyeed Diesel Sales by Customer</td>
<td>Paid-Out Reasons</td>
</tr>
<tr>
<td>Inventory Adjustments</td>
<td>Employee Charges</td>
<td>Pricing Categories</td>
</tr>
<tr>
<td>Inventory Barcodes</td>
<td>FET/SET Exemption</td>
<td>Pricing Levels</td>
</tr>
<tr>
<td>Inventory Receipts</td>
<td>Finance Charges</td>
<td>Purchase Order Status Codes</td>
</tr>
<tr>
<td>Inventory Reports</td>
<td>Fuel Sales By Date and Point Of Sale</td>
<td>Quick Menus</td>
</tr>
<tr>
<td>Invoice List</td>
<td>Fuel Sales By Dispenser &amp; Product</td>
<td>Sales List</td>
</tr>
<tr>
<td>Payment Adjustments</td>
<td>Fuel Sales Volume by Dispenser</td>
<td>Terms Codes</td>
</tr>
<tr>
<td>Print Adjustment</td>
<td>Gallon Summary with Discounts</td>
<td>Units Of Measure</td>
</tr>
<tr>
<td>Print Receipt</td>
<td>Hourly Sales</td>
<td>Vendor Categories</td>
</tr>
<tr>
<td>Purchase Order Maintenance</td>
<td>Inventory Adjustments</td>
<td>Vendors</td>
</tr>
<tr>
<td>Purge Credit Card History</td>
<td>Inventory Receipts</td>
<td></td>
</tr>
<tr>
<td>Rebuild Item Balances</td>
<td>Inventory Snapshot</td>
<td></td>
</tr>
<tr>
<td>Rebuild Sales Summary</td>
<td>Inventory Stock On Hand</td>
<td></td>
</tr>
<tr>
<td>Reports List</td>
<td>Invoice Preview</td>
<td></td>
</tr>
<tr>
<td>Sales Entry</td>
<td>Invoices</td>
<td>Invoices</td>
</tr>
<tr>
<td>Sales List</td>
<td>Invoices – Vehicle Format</td>
<td></td>
</tr>
<tr>
<td>Sales Reports</td>
<td>Loyalty Card Savings</td>
<td></td>
</tr>
<tr>
<td>Show Customer List</td>
<td>Monthly Sales Volume</td>
<td></td>
</tr>
<tr>
<td>Show Items List</td>
<td>No Sale Reasons</td>
<td></td>
</tr>
<tr>
<td>Table Maintenance</td>
<td>Payment History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pending Settlement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prepaid Card Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Price Change History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Private Card Fuel Sales by Dispenser</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Private Card Sales By Customer and Card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Private Card Sales Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Private Cards List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Register Shift</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Re-Order Limits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales By Payment Method</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales By Shift and Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales Detail by Date and Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales History with Signatures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales Profit Margins by Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales Volume by Hour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales Volume Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales with Overridden Prices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statements [Customer Name/Address Lowered]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Sellers by Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Selling Merchandise</td>
<td></td>
</tr>
</tbody>
</table>
PCI Group

PCI Group members have very limited access to OneTouch® system menu and reporting functions or data table maintenance functions. However, PCI Group members do perform two extremely critical business tasks:

• Look-up credit card transaction information.
• Purge credit card transaction history.

PCI Group members have the following OneTouch® Suite rights and permissions:

<table>
<thead>
<tr>
<th>System Menu Functions</th>
<th>Reports</th>
<th>Database Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Activity Search</td>
<td>Credit Card Reconciliation</td>
<td>None</td>
</tr>
<tr>
<td>Purge Credit Card History</td>
<td>Credit Card Volume And Charges</td>
<td></td>
</tr>
</tbody>
</table>

User Group

User Group members have limited access to system menu and reporting functions, and only Read access to certain data table maintenance functions. Basically, User Group members are primarily involved with sales and inventory activities. User Group members can:

• Generate inventory and sales reports.
• View information in certain data tables.

User Group members have the following OneTouch® Suite rights and permissions:

<table>
<thead>
<tr>
<th>System Menu Functions</th>
<th>Reports</th>
<th>Database Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Reports</td>
<td>Inventory Adjustments</td>
<td>Adjustment Reasons</td>
</tr>
<tr>
<td>Reports List</td>
<td>Inventory Receipts</td>
<td>Inventory Categories</td>
</tr>
<tr>
<td>Sales Reports</td>
<td>Inventory Snapshot</td>
<td>Inventory Items</td>
</tr>
<tr>
<td>Show Items List</td>
<td>Inventory Stock On Hand</td>
<td>Inventory Receipts</td>
</tr>
<tr>
<td>Table Maintenance</td>
<td>Sales By Payment Method</td>
<td>No Sale Reasons</td>
</tr>
<tr>
<td></td>
<td>Sales By Shift and Category</td>
<td>Other Payment Types</td>
</tr>
<tr>
<td></td>
<td>Sales Detail by Date and Category</td>
<td>Paid-Out Reasons</td>
</tr>
<tr>
<td></td>
<td>Sales History with Signatures</td>
<td>Sales List</td>
</tr>
<tr>
<td></td>
<td>Sales Profit Margins by Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales Volume by Hour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales Volume Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sales with Overridden Prices</td>
<td></td>
</tr>
</tbody>
</table>

Remote Group

Remote Group members are Triple E Technologies LLC customer support personnel assisting customers to resolve system problems. Rights and permissions granted Remote Group members are temporary and do not exceed those of the group of the customer representative with whom working to resolve the problem. For example, if customer is a member of the User Group, Remote Group rights and permissions will only be those of the User Group (i.e., not of the Administrator Group or PCI Group).
Screensaver Display Setting

To minimize observance of cardholder data displayed on temporarily vacated workstations, specify Windows screen saver default setting of 15 minutes or less.

User Account Password and Lockout Policies

OneTouch® Suite uses pre-configured Windows settings for the following account password and system lockout settings:

- Minimum Password Age = 0
- Maximum Password Age = 90
- Minimum Password Length = 7
- Password Complexity = 1
- Lockout Bad Count = 3
- Reset Lockout Count = 30
- Lockout Duration = 30

For purpose of system integrity and PCI compliance, do not change these default settings to less than values specified. NOTE: OneTouch® Suite keeps password history and requires new passwords be assigned at least every ninety (90) days and differ from previous four.

Assigning Unique ID and Password to Each Application User

Each OneTouch® Suite Version 4.114.117 user must have a unique User ID and password. You must be logged-on as Administrator to perform functions associated with setting up the required user accounts. To create a user account, follow instructions provided with your operating system software.

Accessing Cardholder Data Remotely

PCI-DSS Requirement 8.3 specifies that if employees or vendors are to be granted remote access to cardholder data, such access must employ two-factor authentication (username/password and an additional authentication method such as a token or certificate). This includes remote administrative access. Additionally, vendor access should be limited only to time necessary to provide required service, with access rights limited only to minimum required to provide that service. In all cases, remote access activity should be robustly audited daily by merchant or Administrator account personnel.

Use technologies such as remote authentication and dial-in service (RADIUS), terminal access controller access control system (TACACS) with tokens or VPN (based on IPSEC or SSL/TLS) with individual certificates. Triple E Technologies LLC again recommends using a secure, encrypted VPN for remote access; authentication may be accomplished by specifying a unique VPN user name and complex password, as well as token or certificate.

Regardless of remote access software used, implement the following security features:
• Do not use group (shared) or generic account name and passwords

• Change default password settings in remote access software; assign unique ID and password to each remote user

• Never allow remote access connections directly from the internet; only allow connections from specific (known) IP/MAC addresses

• Use strong authentication and complex passwords for remote logins, per PCI-DSS requirements 8.1, 8.3 and 8.5.8 – 8.5.15

• Enable encrypted data transmission, per PCI-DSS Requirement 4.1

• Enable account lockout after a certain number of failed login attempts, per PCI-DSS Requirements 8.5.13

• Configure system so remote user must establish connection using VPN router and firewall before access is allowed

• Enable the logging function for auditing purposes

• Establish customer passwords per PCI-DSS Requirements 8.1, 8.2, 8.4 and 8.5

• Restrict access to customer passwords to authorized vendor personnel

• Restrict access to remote control software to administrative personnel only

• In cases of Triple E Technologies LLC technical support requests:
  - Use only authorized Triple E Technologies LLC telephone number (208.777.9300) to request support.
  - Enable remote control software only for duration of required support.
  - Confirm site-unique information provided by support representative to ensure you have reached Triple E Technologies LLC.
  - Disable remote control software immediately after use

Restricting Physical Access to Cardholder Data

For purpose of industry best practice and PCI compliance, OneTouch® Suite system owners must provide physical security for those areas housing any resource used to store, process or transmit cardholder data. In keeping with this requirement, ensure the following are in place and working before implementing OneTouch® Suite:

1. Facility entry controls to monitor personnel access to IT resources. Such controls would include cameras to record 24/7 area egress, with recorded data audited and stored at least three months (unless otherwise restricted by law).

2. Controls providing easy, immediate recognition of visitors to sensitive facility areas, including required log-in and log-out procedure and issuance of token, badge or other device to identify visitor for entire duration of stay.

3. Prohibited use of private handheld computer devices (e.g., PDAs).

4. Prohibited public access to facility network jacks, wireless access points and gateways.
5. Secure storage of retained paper media containing cardholder data, including receipts, reports and taxes.

6. Provision for electronic media backup storage in secure location, preferably in protected offsite facility specifically designed for such purpose.

7. Strict internal and external distribution controls over any media type containing cardholder data, including identification of such media as confidential and limiting offsite transport only to bonded couriers.

8. Procedure requiring management approval for any transport of cardholder data media to or from secure storage area.

9. Strict controls over inventory of any stored media containing sensitive data.

10. Procedure for end-of-retention destruction of all stored media containing cardholder data, including specification of methods ensuring data cannot be reconstructed.

Training and Monitoring Administrator Personnel

It is your responsibility to institute proper personnel management policies and techniques for Administrator access to credit cards, site data, etc. In most systems, a security breach is usually the result of personnel advantaging their system access privileges for unethical or illegal purpose. For this reason, you must give special attention to those whom you entrust viewing full decrypted and unmasked cardholder information.
7 Monitoring and testing network

Tracking network resources and cardholder data access

PCI DSS Requirement 10 specifies OneTouch® Suite system owners must track and monitor individual accesses to network resources and cardholder data. Owners must provide central log server and establish policies and procedures for server setup, log migration and log modification prevention. Review of the following keyword events, when identified in log files, is critical for PCI compliance:

- pendingsettlements
- cardslockedout
- ChangeEncryptionKey
- PurgeOldCreditCardData
- salepayments,
- ccrequests.

Specifically, you must be able to verify logging of the following seven events to satisfy this requirement:

1. All individual access to cardholder data through the payment application.
2. Actions taken by any individual with administrative privileges to the payment application.
3. Access to audit trails managed by or within the payment application.
4. Invalid logical access attempts.
5. Use of payment application’s identification and authentication mechanisms.
6. Initialization of application audit logs.
7. Creation and deletion of system-level objects within or by the application.

NOTE: Of the seven items listed above, only items 1 and 2 are tracked in SQL trace files found in C:\EEETechnologies\EEETrace and C:\EEETechnologies\EEETrace\Processed. Tracking of items 3 – 7 is your responsibility, and must be performed by your own means.

At minimum, OneTouch® Suite identifies the following for each of the above:

- Individual causing event
- Event type
- Event date and time
- Event success or failure
- Component on which event occurred
- Components or data affected by event
Because OneTouch® Suite Version 4.114.117 has pre-defined database auditing capabilities, you will have no level of customization over the audit output files. Please note, however, that disabling or subverting the logging function of OneTouch® Suite in any way will result in non-compliance with PCI-DSS. Additionally, OneTouch® Suite owners are advised to have work policies and procedures in place calling for the following prior to system installation:

- Minimum daily review of log files for activity auditing purposes
- Limitation of log file review authority to Administrator account level only
- Timely backup and secure storage of log files
- Timely backup of audit files to a centralized server or media difficult to alter
- Retention of log files for at least one year

Testing security systems and processes

Even though Triple E Technologies LLC does not support or otherwise provide for implementation of OneTouch® Suite other than into a local network, system owners are not relieved of performing security assessments for data loss or intrusion due to wireless technology implementation (PCI-DSS Requirements 1.2.3, 2.1.1 and 4.1.1). In this regard:

1. Install and configure perimeter firewalls between wireless networks and systems that store credit card data per PCI Requirement 1.2.3. Configure such firewalls to block all traffic except that required for business operation.

2. Do not implement Wired Equivalent Privacy (WEP) key-exchange.

3. Per PCI Requirement 2.1.1, change all security-related wireless vendor defaults and settings as follows:

   - Change Default Service Set Identifier (SSID)
   - Disable SSID broadcasts
   - Change default passwords
   - Change default encryption keys
   - Change SNMP community strings
   - Change other security-related wireless defaults
   - Enable WIFI protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable

4. Encrypt wireless transmissions of cardholder data using industry best practices for authentication and transmission. Never rely on Wired Equivalent Privacy (WEP) to protect confidentiality and access to a wireless LAN. Change encryption keys at least annually and whenever deemed necessary or prudent because of actual or suspected security compromise. Change encryption keys whenever anyone with knowledge of them changes positions or leaves the company.

5. Ensure firmware for any wireless device communicating with OneTouch® Suite is updated to use strong encryption algorithms for authentication and transmission.

PCI compliance also requires ongoing monitoring and periodic security assessment of local area network services and protocols. In this regard, the following should be in place prior to OneTouch® Suite implementation:
1. Policy and procedures requiring internal staff network scanning immediately following any resource change.
2. Contract service agreement with an ASV (Approved Scanning Vendor) to perform at least quarterly scans of network resources. Go to pcisecuritystandards.org for current listing of ASVs.
3. Further to ASV contract service agreement, policies and procedures calling for performance of the following:
   - Review of ASV resource scans immediately upon receipt
   - Affix approval signature and date to each scan.
   - Notation of vulnerabilities detected by scan, including description, personnel assignment for remedy and estimated completion date
   - Creation and maintenance of PCI compliance binder containing quarterly scan results, action items and plans, and correspondence relating to vulnerabilities

**Delivering PCI-compliant software updates**

As a software development company, Triple E Technologies must keep current with security concerns and vulnerabilities affecting our area of responsibility and expertise. We do this by subscribing to relevant data feeds and news services that inform us of potential security issues.

We recommend that your Windows server be maintained automatically by using Microsoft’s automatic update service to download security patches as they become available. If we identify a relevant vulnerability not covered by these automatic updates, we work to develop and test a patch to protect OneTouch® Suite and using merchants against the new vulnerability, and strive to publish a patch within thirty days of vulnerability identification. We then contact merchants to notify them of the availability of the patch on our secure (https) website. Typically, merchants are expected to respond quickly and install the patch within thirty days of receipt. In all cases, merchants should contact Triple E Technologies, LLC for assistance when applying updates and patches using only the authorized Triple E Technologies, LLC telephone number (208.777.9300) and to validate the authenticity of a software patch.

For receiving updates via remote access, use a personal firewall product to secure these “always-on” connections, per PCI Data Security Standard 1.3.10. Please see Building And Maintaining A Secure Network section (above) for description of how we recommend your high-speed connection be secured using two-factor authentication.
Maintaining Information Security Policy

Establishing Information Security

PCI DSS Requirement 12 mandates that OneTouch® Suite system owners maintain a strong information security policy to underline the sensitive nature of cardholder data and to communicate user roles and responsibilities for protecting that data. For purpose of PCI compliance, therefore, you will need to establish information security practices that demonstrate the following:

1. Item-by-item compliance with PCI DSS requirements (1–12).
2. Assignment of security policy development and enforcement responsibilities to specific individuals.
3. Provision of daily operational procedures to enforce or support security policy.
4. Provision of technology resource usage procedures to enforce or support security policy.
5. Procedure for annual security policy review, assessment and maintenance.
6. Provision for and annual testing of security policy risk assessment plan.
7. Provision for and annual testing of security policy compromise response plan.
8. Procedure for security policy dissemination and recipient acknowledgement.
9. Provision for and conduct of formal, ongoing security policy training.

Sample security policy

Following is an example of a security information policy written with PCI compliance in mind. Please note that this policy is provided for purpose of illustration; it is intended to serve only as a guideline, not as substitute for an actual PCI-compliant security policy.

<table>
<thead>
<tr>
<th>INFORMATION SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVED BY:</td>
</tr>
<tr>
<td>NAME: Robert Jones</td>
</tr>
<tr>
<td>Page 1 of 4</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

1.0 PURPOSE
Establish and communicate security policy for XYZ Stores cardholder data environment.

2.0 SCOPE
All XYZ Stores IT resources, whether owned or leased, including devices, systems, networks and applications that process, store or cardholder data.
Sample Information Security policy (continued)

INFORMATION SECURITY

APPROVED BY:
NAME: Robert Jones
TITLE: Owner
POLICY NUMBER: 01-001.01

Page 1 of 4

3.0 POLICY
3.1 General

3.1.1 For purpose of industry best practice and PCI compliance, XYZ Stores will develop, implement and enforce information security policies and procedures to protect payment card data.

3.1.2 Content of information security policies and procedures will be reviewed and updated at least annually.

3.1.3 Risk assessment to identify information policy or procedural threats and vulnerabilities will be performed at least annually.

3.1.4 Standard operating procedures will be developed and enforced to support established security policies.

3.1.5 Acceptable use policies and procedures for employee-facing devices such as modems, laptops and PDAs will be developed and enforced to support established security policies.

3.1.6 Information security management procedures will be developed and enforced to clearly define security roles and responsibilities for affected XYZ Stores personnel, including:
- Development, maintenance and enforcement of information security policies and procedures
- Establishment and administration of user accounts
- Control over all customer payment card data access
- Monitoring and follow-up of security alert and breach information

3.1.7 A formal, ongoing education program will be implemented to familiarize all affected new hires and existing XYZ Stores personnel with information security policies and procedures.

3.1.8 New hires and existing XYZ Stores personnel receiving promotions will undergo background checks prior to starting new job responsibilities.

3.2 Policy and Procedure Development

3.2.1 Existing XYZ Stores information security policies and procedures will be reviewed and updated on an as needed basis, but no less than annually.

3.2.2 All information security policies and procedures, whether new or revised, require XYZ Stores owner or designee review and approval prior to distribution.

3.2.3 Approved information security policies and procedures will be distributed to all affected XYZ Stores personnel.

3.2.4 Distribution of information security policies and procedures will be controlled to ensure consistency and currency of content.
### INFORMATION SECURITY

#### APPROVED BY:
- NAME: Robert Jones
- TITLE: Owner

<table>
<thead>
<tr>
<th>POLICY NUMBER:</th>
<th>01-001.01</th>
</tr>
</thead>
<tbody>
<tr>
<td>REPLACES POLICY:</td>
<td>01-001.00</td>
</tr>
<tr>
<td>EFFECTIVE DATE:</td>
<td>07 November 2010</td>
</tr>
<tr>
<td>REVISION DATE:</td>
<td>01 July 2013</td>
</tr>
</tbody>
</table>

**3.2.5** PCI DSS requirements will be regularly monitored for changes to ensure XYZ Stores information security policy remains compliant.

#### 3.3 Risk Assessment

**3.3.1** A plan will be developed and implemented to regularly assess information security threats and vulnerabilities.

**3.3.2** Plan will evaluate efficacy of both the information security measures put into place and related policies and procedures prescribing performance of those measures.

**3.3.3** Assessment will document findings for each area found to be at risk, as well as for attendant policies and procedures; analysis of impact shall be provided, along with prioritization of required changes in measures and affected policies and procedures.

**3.3.4** Administration and activation of plan is the responsibility of XYZ Stores owner or designee.

**3.3.5** Plan will be activated each time there is a security breach.

**3.3.6** Plan will be reviewed each time there is a security breach, else at least annually.

**3.3.7** Plan will be updated as necessary, based on lessons learned, industry developments and changes in PCI DSS requirements.

#### 3.4 Information Security Breach Response

**3.4.1** A plan will be developed and implemented to immediately respond to any breach in information security.

**3.4.2** Plan will address the following:
- Incident response team roles, responsibilities and contact information
- Incident response team training
- Incident response procedures and performance standards
- Data backup and recovery procedures
- Business recovery and continuity procedures

**3.4.3** Plan will be tested at least annually.

**3.4.4** Plan will be activated each time there is an actual or suspected security breach.

**3.4.5** Plan will be reviewed each time following a security breach.

**3.4.6** Plan will be updated as necessary, based on lessons learned, industry developments and changes in PCI DSS requirements.

#### 3.5 IT Resource Acceptable Use

**3.5.1** XYZ Stores personnel (hereinafter “users”) are granted access to computer resources only as and when approved or directed by owner or designee.

**3.5.2** User access to customer payment card data shall be granted only on strict need-to-know (least privilege) basis.
3.5.3 Users shall have no expectation of privacy as regards any information or communication residing on any IT resource.
3.5.4 Users shall exercise good judgment when accessing IT resources. If uncertain, users must consult with owner or designee before proceeding.
3.5.5 Users must take all steps necessary to prevent unauthorized access to customer payment card data.
3.5.6 Users are responsible for the security of their system accounts and passwords.
3.5.7 Users must change passwords at least every ninety days.
3.5.8 Users must logoff whenever leaving workstation unattended.
3.5.9 Users must run anti-virus and anti-malware software as directed by XYZ Stores owner or designee.
3.5.10 Workstations will always be secured by password-protected screensaver and Windows automatic lock feature.
3.5.11 Upon any user with encryption key knowledge leaving the company, encryption keys should be changed immediately.
3.5.12 The following practices are strictly prohibited:
   • Using any IT resource for purpose other than XYZ Stores business, especially accessing Internet and personal email
   • Accessing any IT resource or data for which not specifically authorized
   • Installing any software or hardware product not authorized by XYZ Stores owner or designee
   • Using personal computer or other device (e.g., laptop, PDA) to access any XYZ Stores IT resource
   • Sharing user identification and/or password information with any other person
   • Circumventing user authentication or security of any host, network or account.
   • Using IT resources to violate individual rights of any person or intellectual property rights of any entity
3.5.13 XYZ Stores owner or designee will periodically audit IT resource logs to ensure compliance with Acceptable Use policy.

3.6 Security Education
3.6.1 A formal security awareness program will be implemented to ensure XYZ Stores personnel are thoroughly trained in all areas of cardholder data security.
3.6.2 XYZ Stores personnel will undergo security program training at time of hire and at least annually thereafter.
3.6.3 XYZ Stores personnel will acknowledge in writing that they have read and understood XYZ Stores’ security policies and
Sample Information Security policy (continued)

<table>
<thead>
<tr>
<th>INFORMATION SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPROVED BY: NAME: Robert Jones TITLE: Owner</td>
</tr>
<tr>
<td>POLICY NUMBER: 01-001.01</td>
</tr>
<tr>
<td>REPLACES POLICY: 01-001.00</td>
</tr>
<tr>
<td>EFFECTIVE DATE: 07 November 2010</td>
</tr>
<tr>
<td>REVISION DATE 01 July 2013</td>
</tr>
</tbody>
</table>

3.7 Personnel Screening
   3.7.1 A formal, personnel screening program will be implemented to ensure all XYZ Stores personnel pass a thorough background check.
   3.7.2 XYZ Stores personnel will undergo security screening by independent, outside authority at time of hire and when receiving promotion.
   3.7.3 XYZ Stores personnel must sign release of all background information as necessary to satisfactorily complete personnel screening process.

3.8 Policy and Procedure Distribution
   3.8.1 Security policies and procedures will be distributed to XYZ Stores personnel at time of hire and thereafter each time revisions are made.
   3.8.2 XYZ Stores personnel must provide written acknowledgement of policy and procedure receipt, review and understanding.
   3.8.3 XYZ Stores personnel are responsible for maintaining personal set of information security policies and procedures, including replacing outdated versions with latest revisions.

4.0 RESPONSIBILITY
   It is the XYZ Stores owner’s responsibility to lead all activities that effect and maintain both card payment industry best practices and compliance with PCI DSS requirements.

5.0 COMPLIANCE
   PCI DSS Requirement 12.