PCI-DSS Implementation Guide

Version 1.0

Refer to the following sections as a guide to provide you with some general PCI security information, tips and instructions on how to stay in accordance with PA-DSS requirements (as they relate to PCI), and your specific responsibilities for meeting PCI-DSS requirements.

Arbelsoft Inc.

June 15, 2010

Revision History			
Version	Date	Author	Comments
v 1.0	6/21/2010	Mark Shehata	Initial Released.
v 1.0.1	9/26/2011	Mark Shehata	Exporting Activity Logs to file.
v 1.0.2	10/11/2010	William Kang	Updates to new PA-DSS requirements as outlined by Halock

This policy is reviewed at least annually and updated when changes occur.

1. Payment Systems Security

1.1 Introduction

In today's world, we are all vulnerable to the attacks of cyber criminals and it has become a pressing issue to protect sensitive data and maintain secure systems and applications. There has been a great deal of national and international concern brewing over the issue of how to close the gaps that enable security breaches to persist. As an initiative to heighten credit card security, Visa issued the Cardholder Information Security Program (CISP) in April 2000, which then became a requirement for all entities that store, process, or transmit Visa cardholder data as of June 2001.

Following in Visa's footsteps, other credit card companies joined to form a new group by the name of Payment Card Industry Security Standards Council which strives to standardize security requirements across the entire credit card industry.

The new standard, called PCI DSS for short, encompasses a comprehensive set of security standards that mirror the practices set forth by the PCI Security Standards Council and has been adopted by American Express, MasterCard Worldwide, Visa Inc. International, Discover Financial Services, and JCB International. The standard lays the groundwork for establishing the universal adoption of data security measures across all merchants that store, process, and/or transit customer account data.

The document is provided to guide users of CleanMax, LaundroMax, TailorMax, and ShoeMax into making the transition towards staying PCI compliant.

1.2 Why should I be concerned about PCI Compliance?

The PCI board has set July 2010 as the date to begin enforcing all merchants who accept or process payment cards to process transactions in compliance with PCI and PCI DSS. The merchant's failure to meet compliance could lead to the denial or revocation of the organization's ability to process credit cards. Further, the merchant could be held liable in the face of credit card information or systems being compromised.

As of October 1, 2008, Credit Card Processors and Bank Card Acquirers must only accept level 3 and 4 merchants that are PCI-DSS compliant or that utilize PA-DSS compliant applications.

As of October 1, 2009, all payment applications which were not PA-DSS compliant were de-certified. As stated before, July 1, 2010 is the deadline for Credit Card Processors and Bank Card Acquirers to ensure that merchants and agents use only PA-DSS complaint applications.

1.3 PCI Data Security Standard

The PCI-DSS is a multifaceted security standard intended to help organizations close security gaps in card-processing ecosystem with requirements ranging from security management, policies, procedures, network architecture, software design, etc.

CleanMax, LaundroMax, TailorMax, and ShoeMax Version 7.5 has been certified as compliant under the Payment Application Data Security Standard 1.2. The PA-DSS is a separate security standard that applies to software vendors that develop applications for sale to merchants to process and/or store cardholder data. Just because CleanMax, LaundroMax, TailorMax, and ShoeMax has been certified as PA-DSS 1.2 compliant doesn't mean that you as a merchant are automatically PCI compliant, as it takes a series of important steps in order to ensure PCI compliance.

2. Merchant Requirements for Compliance

Generally speaking, there are about twelve requirements that the merchant must meet in order to become certified as being PCI-complaint. They are outlined below:

Build and Maintain Secure Network

Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public network

Maintain Vulnerability Maintenance program

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

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

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

Requirement 9: Restrict physical access to cardholder data

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain an Information Security Policy

To learn more about PCI visit www.pcisecuritystandards.org

3. Arbelsoft PCI Security Practices

Arbelsoft software credit card interface has been certified by Payment Processing Inc. since June 2010 as compliant under PA-DSS 1.2 requirements that we meet their specifications and we are certified for transaction on the “Gateway II” interface. The “Gateway ll” is a real time payment processing between merchant’s POS system and their processor. By processing customer’s credit card via Payment processing Inc. the credit card number is kept by Arbelsoft database in an encrypted format.

You can leverage CleanMax, LaundroMax, TailorMax, ShoeMax as tools to help you stay PCI compliant. However, there are important procedures and practices you must follow and emphasize across your organizational structure.

These guidelines should be followed both when you initially install the software and as you enter transactions with your customers and begin to gather a store of sensitive data so that you can safeguard confidential customer data. Refer to the following sections as a guide to provide you with some general PCI security information, tips and instructions on how to stay in accordance with PA-DSS requirements (as they relate to PCI), and your specific responsibilities for meeting PCI-DSS requirements

If you have any questions regarding Payment Processing, Inc’s Gateway, its security and/or compliance, Contact Payment Processing, Inc representative directly at

(800) 774-6462 Extension 2 for 24/7/365 Days

4. Securely implementing Arbelsoft Software

4.1 Sensitive Authentication Data

4.1.1 Previous Versions

You must first remove sensitive customer data in order to remain PCI compliant. PA-DSS 1.0 states that you must not retain full magnetic stripe, card validation codes or values (i.e CAV2, CID, CVC2, CVV2) or PIN block data that has been stored within the previous version of the payment application.

As a necessary step to remove sensitive historical data securely and ensure PCI compliance, locate and download our software update of version 7.5 or higher. For you to gain a better grasp on how the update can secure sensitive authentication data, we include the following description of the process.

First, when a transaction by credit card is swiped through a magnetic swipe reader or when the number and expiration are entered manually for authorization, the data is transferred locally to the payment processing data center which is then sent in an encrypted form to the payment processing company for card authorization. The response data is then delivered back in encrypted format to the Arbelsoft client indicating whether or not the transaction was a success. Throughout the process, the hardware does not store full magnetic stripe data and the response data is also encrypted as an additional shield from potential third party interception. The system also does not store PIN / PIN block data.

4.2 Protect Stored Cardholder Data & User Password.

Arbelsoft software uses a data access encryption key (256-bit AES encryption key) to encrypt credit card numbers and protect sensitive information.

Every 3 months, you should re-encrypt previous data with new keys using our “Reset Encryption” utility. The process takes between 20 – 30 minutes so make sure you perform the re-encryption at a time when you can take the leisure to wait for that long. To access the feature, start at the main screen and click “Management,” then #12 Utility. Then click #17 Reset encryption, located on the lower right hand side of the utility screen.

For further security, we release our software with the “Hide Card No” utility already selected. The function conceals credit card numbers altogether from your employees in the interest of protecting cardholder data.

4.2.1 Backup

To be prepared for a case which you suspect that your data has been compromised, it is a good idea to back up your data file and keep it in a safe location.

We recommend that you back up your data files of encrypted credit card information daily. The easiest way to do this is as you sign out every day, select the Back Up & Shut Down function. Another way you can access the backup function, first click on Management located at the main screen. Then click #12 Utility and #12 Backup.

Also, it is mandatory to investigate older computers on which earlier versions of our software have been downloaded, or computers that contains backup data from previous software versions, since those versions may contain data that has not been securely encrypted.

4.2.2 Purge Stale Cardholder Data

Cardholder data including their primary account number, cardholder name, and expiration date are encrypted and stored. All Arbelsoft software of the Version 7.5 and higher offers a utility to purge stale cardholder data periodically.

After the expiration of a 6-month retention period, cardholder data must be purged from the software system. Storage of cardholder data should be limited to situations arising for business, legal and / or regulatory purposes. If a user with administrative rights accesses the workstation to securely delete data, make sure that he/she logs off upon completion to prevent others from accessing these capabilities.

The purge function automatically accesses all of the locations where the payment application stores cardholder data and clears it up to the present date.

Make sure to utilize this function semi-annually so that you do not exceed the 6-month retention period.

a) In order to navigate to this function, start at the main screen and click Management, located on the upper panel.

b) Click #12 Utilities

c) Click #9 Purge. At the pop-up screen, select "Credit Card Data," choose the date. The pop-up will have automatically input the present date for you. Then click OK.

4.3 Secure Authentication Features

4.3.1 Administrative and Privileged Access to the Application

You should implement proper user authentication and password management for all system administrators by using our access control features in which you can tailor accessibility down to every software feature for each of your employees. Default settings will result in noncompliance with PCI DSS Standards and may allow for security loopholes through which employees that may not merit access to administrative capabilities could exercise control over payment applications. Do not create any default user accounts or passwords.

To edit access control features follow these steps:

a) At the main screen, click Management
b) Click #9 – Setup
c) Click #3 – User
d) Select the appropriate security level and then click on “Security Setup”

Note that general employees should only have access to the “Time Clock Only.” For higher security levels such as “Owner,” “Manager,” or “Master Counter,” or any other custom created security level, you can deselect specific features within the Security Setup such as “AR Payment” “Allow Add “Debit / Credit,” etc. so as to block individual access from payment related applications when necessary.

It is important to assign secure authentication for all accounts for payment applications and systems whenever possible. Also make sure that you have assigned all users a unique ID and unique password before allowing them to access system components or cardholder data.

4.3.2 General Non-Privileged Access to the Application

Here are some rules you should follow when issuing ID’s and passwords, and these procedures and rules should be communicated to all administrators or individuals who have access to payment applications and cardholder data:

a) Do not use group, shared, or generic accounts and passwords.
b) Passwords should be a minimum length of 7 characters.
c) Use strong passwords that incorporate both numeric and alpha characters.
d) Passwords must be changed every 90 days. Please note that without doing so, the system will lock out the user from their account.
e) Individuals will not be allowed to submit a new password that is the same as any of the last four passwords he or she has used.
f) Repeated access attempts in excess of 5 times will lock out the user ID. The lockout duration is set to be a minimum of 30 minutes before an administrator can enable the user ID.

g) If a session has been idle for more than 15 minutes, the user will be required to re-enter the password to reactive the terminal.
h) Make sure to verify user identity before performing password resets.
i) Set first-time passwords to a unique value for each user and change immediately after first use.
j) Immediately revoke access for any terminated users.
k) Remove / disable inactive user accounts at least every 90 days.

In addition to assigning unique IDs to all users, you may authenticate users by interfacing the system with a biometric device which can quickly and automatically capture and encrypt finger print images before verification. Passwords and password management can be taken out of the hands of end-users and administrators, making the device ideal for keeping track of employee attendance, maintaining security, and simplifying the management of employee passwords.

4.3.3 Setting Up Time Limits for Terminal Reactivation

Setting up time limits for reactivation terminals is quick and easy. Beginning at the main screen, first click Management, then Setup, then Default. Click on the function #107 called Log out O'Matic and set the time to 900 seconds or 15 minutes.

4.4 PA-DSS Requirement 4.0

4.4.1 Log Payment Application Activity

Arbelsoft software automatically implements an audit trail to track and monitor individual accesses to potentially sensitive data. For example, if an employee logs in to view credit card information or another tries to log in whether or not their attempt was successful, all of these will be stored as an activity log of events. The activity log contains the user name, date, time of the event, as well as the station name, which indicates at which computer this activity was performed.

To ensure compliance with PCI DSS, logging cannot be disabled by the end user. You should take the time to review the logging data regularly, and monitor instances of access to sensitive internal data such as cardholder data.

To navigate to these logs, please start at the main screen and click "Management". Then click on #6 (Report) → Counter) → #213 (Credit Card Access Log).

To export these logs, please click "Export". Then choose the target directory.

4.5 Protect Wireless Transmissions

4.5.1 Wireless Technology Included in or with the Payment Application

We strongly recommend that you use a wired network over a wireless one. In the case that you do utilize wireless technology, make sure you take the following precautions.

a) Enable WPA and WPA 2 protocols (WiFi protected access) for encryption and authentication.

b) Also, take the necessary steps to alter your default service set identifier (SSID)

c) Stop your router from broadcasting your wireless network name (SSID).

d) Use wireless MAC Authentication.

The security configuration must be compliant with PCI DSS Requirements 1.2.3, 2.1.1 & 4.1.1

Per PCI DSS Requirement 1.2.3 you must install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.5.2 General Use of Wireless Technology

Again, we strongly recommend that you use a wired network over a wireless one. Before implementing wireless technology, you should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Wireless environments must be implemented and maintained per the following PCI DSS Requirements.

PCI-DSS 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

PCI-DSS 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

PCI-DSS 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i)

a) For new wireless implementations, it is prohibited to implement WEP after March 31, 2009
b) For current wireless implementations, it is prohibited to use WEP after June 30,2010

If you are using non-Arbelsoft computer systems that are connected to a wireless network, you must configure them appropriately. First, encrypt the transmissions using WPA or WPA2 technology, SSL/TLS, or IPSEC VPN. Note from above that it is prohibited to implement WEP as an exclusive means to protect confidentiality. If you are using WEP, make sure you are using it in conjunction with WPA or WPA2 technology, SSL/TLS or IPSEC VPN.

4.6 Systems Connected to the Internet

4.6.1 Servers

Reference: PA-DSS 9.0 Cardholder data must never be stored on a server connected to the internet.

All payment applications in Arbelsoft software does not require a web server, thus cardholder data will not be stored on a system that is accessible by outside parties. We strongly recommend that you do not install a web server on the same computer with the Arbelsoft program downloaded. If you would like to install a web server, please install it on a separate computer and put the web server in the DMZ or at the minimum install a physical hardware firewall between your server and the outside public internet.

4.6.2 Security / CleanMax Only Screen

We strongly recommend that you download antivirus software for your computer(s) which you should keep running at all times. Norton and McAfee are commonly used by our clients. Also, the two companies oftentimes release security patches for new vulnerabilities that have been uncovered, so make sure that your computer has been enabled to receive automatic updates.

CleanMax, LaundroMax, TailorMax, ShoeMax Only Screen

We also strongly recommend that you use the CleanMax only screen in order to block employee access from the internet or other applications that are unrelated to the CleanMax interface. The only two accessible items under this setting is to exit the program using a PIN or to use the utilities in the application. In order to access this function, first begin at the main screen and click Management, then “Utility” then “CleanMax Only.” You must exit the entire program in order for the CleanMax only option to take effect. In order to remove the CleanMax only option, you have to exit the program once again and click the "Microsoft Windows XP" button located on the upper left hand side of the screen. One you have clicked it, only authorized users such as the manager with access to the PIN number can undo the effects of the CleanMax only screen.

Note: All Arbelsoft softwares are inter-changeable such CleanMax, LaundroMax, TailorMax and ShoeMax that you can select you can select your desired software at the default screen. The "xxxMax only" screen can be matched simultaneously by one touch set up at Utility.

You can see more detail on User Manual on page 23
http://www.arbelsoft.com/support/downloads.php

4.7 Secure Remote Software Updates

In case you receive payment application and/or updates via remote access to your network, make sure you follow these requirements.

PCI DSS Requirement 12.3.9: Only activate remote-access technologies for vendors only when needed, and immediately deactivate after use.

PCI DSS Requirement 1: Use a firewall or a personal firewall product if your computer is connected via VPN or other high-speed connection to secure these "always-on" connections in order to protect cardholder data.

a) Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer)
b) Allow connections only from specific (known) IP/MAC addresses
c) Use strong authentication or complex passwords for logins and establish passwords according to PCI DSS Requirements 8.1, 8.3, and 8.5.8 – 8.5.15 (see Appendix for details)
d) Enable encrypted data transmission
e) Enable account lockout after a certain number of failed login attempts
f) Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed
g) Enable logging or auditing functions
h) Restrict access to customer passwords to authorized reseller/integrator personnel

4.8 Remote Access

You should restrict remote access to authorized employees only and establish passwords for these individuals according to requirement 8 of the PCI Data Security Standard. Some tips are as follows:

a) Do not use passwords that are shared between users
b) Require complex, strong passwords
c) Configure your network such that remote users must establish an encrypted connection such as a VPN connection through a firewall before enabling access
d) Enable logging to track and record when users have connected remotely.
e) Enable account lockout after repeated failed authentication attempts.

We recommend that users setup PC Anywhere for the highest level of encryption (256-bit AES encryption). As said before, make sure that only a limited number of employees have administrative access with which to connect remotely. Properly enforce authentication by requiring two-factor authentication to connect remotely. The connections should be activated only when needed and immediately deactivated after use.

4.9 Encrypt All Non-Console administrative Access

All non-console administrative access must be encrypted using technologies such as Secure Shell (SSH), VPN or SSL/TLS for web-based management and other non-console administrative access according to PCI DSS Requirement 2.3 which states that Telnet or rlogin must never be used for administrative access. Only SSH, VPN or SSL/TLS is recommended for encryption of non-console administrative access.

5. Appendix

5.1 Computers Setup and Specifications

1. All computers must use Windows XP Professional OS with the last updates and the automatic update feature should be on. (PCS DSS Req. 6).
2. The latest version of Microsoft .Net framework Required.
3. Arbelsoft uses a feature to lock the access to windows functionalities. This feature should be activated.
4. The server/ Main PC must be located in easily accessible area in a locked cabinet. You must restrict and control physical access to its location. (PCI DSS Req. 9.1)
5. Install anti-virus software on all computers (PCI DSS Req. 5).
6. Arbelsoft strictly recommends not installing any other application on the computers running our products especially the main server (the one that that has the database).
7. Set screen savers and computer lockout to require a user to re-enter their password to re-activate the terminal if it has been idle for more than 15 minutes. (PCI DSS Req.8.5.15)
8. Must have unique user names and passwords for all users. (PCI DSS Req. 8)
9. Must be plugged to a Power UPS.

Note: If the hardware is not purchased from Arbelsoft, It is your responsibility to read the system specifications and order the correct equipments that are compatible with our products. Also, It is your responsibility, as well as your hardware vendor to make sure the equipments are working properly and do regular maintenance.

5.2 Network and Accounts Setup and Specifications

1. Install and maintain a firewall and router configuration.
2. In case that you use wireless technology, make sure you take the following steps:
    a) Enable WPA and WPA 2 protocols for encryption and authentication.
    b) Alter your default service set identifier.
    c) Stop your router from broadcasting your wireless network name (SSID).
    d) Use wireless address authentication.

   PCI DSS Req 1.2.3 you must install perimeter firewalls between any wireless network and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.
3. According to PCI DSS Req. 2 - You must not use any vendor defaults for system passwords, parameters and any settings associated with security.
4. According to PCI DSS Req. 8: All users must have their own unique ID (For Arbelsoft products, It means unique username, password and pin number). There is an additional method of login to the product either by password or Finger print reader.

5. The Password Requirements should include but not limited to: a minimum length of 7 characters, both numeric and alpha characters, must be changed every 90 days.
For more details, refer to section 4.3.2 of this document.
6. In case of more than one computer, set static IP addresses for each computer as 192.168.1.x, Subnet Mask 255.255.255.0. Where x is 100, 101, etc
Each computer must have a unique name and it is recommended to follow the following naming convention:
MAX-XXX-A Where XXX is the first 3 letters of the store name or the abbreviation of the store name.
A: refers to the first PC (usually the main pc)
If the same customer has other store, it should be like MAX-XXX-AD1.

5.3 Hardware Setup and Specifications (Monitors, Printer, Scanners, etc)

Check for the complete list of compatible hardware:
http://www.arbelsoft.com/solutions/hardware.php

5.4 Data Backup

There are 3 options for Data backup for Arbelsoft products:

- Online/Remote Backup: The customer has to subscribe to this service and the backup files will be uploaded to our server.
- Flash Drive: the user will need only a flash drive.
- If the customer PC has a RAID feature, the database itself will be on the other HDD.

Note: The customer still can do back up locally but there will be a critical risk in case of HDD Damage.

5.5 Technical Support Responsibilities

As the company's technical support you are responsible for supporting and training the users of the system:
For Supporting:

1. Hardware
2. Operating system
3. Network Problems
4. Your Company Software like Word, Excel, Internet.

For Training the users on:

1. Turning the PC on and Off.
2. Naming & Showing all the system components (Printers, scanners, scales, etc)

3. Explaining Arbelsoft Manuals (Especially on how to troubleshoot the printers, Scanners, and scales).

Notes:
- Arbelsoft is only responsible for supporting and maintaining its products and cannot help in supporting Non Arbelsoft products like MS Office.
- Arbelsoft is only responsible for supporting and maintaining the equipments it purchased/rented/leased and cannot help in installing / supporting other customer's equipments.

5.6 Data Security Requirements

This includes:

1. Antivirus Setup and update. (PCI DSS Req. 5)
2. Install and maintain a working firewall to protect data.
3. Blocking access to the windows for regular users by using our feature i.e. xxxMax only.
4. Regular testing of the security of the entire network. (PCI DSS Req. 11)
5. Internal network security, including unique user names, passwords and pin numbers for all users. (If the customer uses Finger print reader, you should make sure that the users use it).

Note:
Arbelsoft strictly recommends not installing any other application on the computers running our products especially the main server (the one that that has the database).

5.7 PCI-DSS Requirement 8

Assign a Unique ID to each Person with Computer Access

PCI DSS 8.1: Assign all users a unique ID before allowing them to access system components or cardholder data.

PCI DSS 8.2: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

-Passwords or passphrase

-Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

PCI DSS 8.3: Incorporate two-factor authentication for remote access (network-level access origination from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACAS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

PCI DSS 8.4: Render all passwords unreadable during transmission and storage on all system components use strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations and Acronyms).

PCI DSS 8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

PCI DSS 8.5.1: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

PCI DSS 8.5.2: Verify user identity before performing password resets

PCI DSS 8.5.3: Set first-time passwords to a unique value for each user and change immediately after first use

PCI DSS 8.5.4: Immediately revoke access for any terminated users

PCI DSS 8.5.5: Remove/disable inactive user accounts at least every 90 days.

PCI DSS 8.5.6: Enable accounts used by vendors for remote maintenance only during the time period needed

PCI DSS 8.5.7: Communicate password procedures and policies to all users who have access to cardholder data

PCI DSS 8.5.8: Do not use group, shared, or generic accounts and passwords

PCI DSS 8.5.9: Change user passwords at least every 90-days

PCI DSS 8.5.10: Require a minimum password length of at least seven characters

PCI DSS 8.5.11: Use passwords containing both numeric and alpha characters

PCI DSS 8.5.12: 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.

PCI DSS 8.5.13: Limit repeated access attempts by locking out the user ID after not more than six attempts.

PCI DSS 8.5.14: Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.

PCI DSS 8.5.15: If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.

PCI DSS 8.5.16: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.