VevoPay

Payment Module

PA-DSS Implementation Guide

VevoCart.com

support@vevocart.com

www.vevocart.com

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

Table of Contents

1. Introduction 1
   - 1.1 PCI DSS 1
   - 1.2 PA-DSS 2
   - 1.3 About This Manual 2
2. Credit Card Data Security 3
   - 2.1 Credit Card Data Storage 3
   - 2.2 Notes to Customers/Integrators 3
3. Server Environment 4
   - 3.1 Install and Maintain Firewall Configuration 4
   - 3.2 User and Password Policies 5
   - 3.3 Audit Policy 5
   - 3.4 Use Latest Security Patches 6
   - 3.5 Disable Unnecessary Services 6
4. VevoPay Software Installation 7
   - 4.1 Database User 7
   - 4.2 Passphrase Setup 7
   - 4.3 Admin Account Creation 7
   - 4.4 Secure Connection (SSL/TLS) 8
   - 4.5 Delete Sensitive Authentication Data 9
     - 4.5.1 VevoCart Database 9
     - 4.5.2 Other Shopping Cart Applications 9
     - 4.5.3 Collecting Sensitive Data for Troubleshooting 9
   - 4.6 Delete Old Cryptographic Key 10
     - 4.6.1 VevoCart 3.x and Older 10
     - 4.6.2 VevoCart 4.0 10
     - 4.6.3 Other Shopping Cart Applications 10
5. PCI-Related Configurations 11
   - 5.1 Cardholder Data History 11
   - 5.2 Audit Trails 12
6. Other Considerations 13
   - 6.1 Wireless Security 13
   - 6.2 Email and Messaging Security 13
   - 6.3 Remote Access 13

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

1. Introduction

1.1 PCI DSS

Major credit card companies, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, have formed an organization called Payment Card Industry Security Standards Council with a goal to improve credit card security.

This organization has created a worldwide security standard called "Payment Card Industry Data Security Standard" (PCI DSS). The PCI DSS applies to wide range of system components and policies, including security management, policies, procedures, network architecture, software design and other critical protective measures.

The overview of the standard can be seen below:

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security

More information for PCI DSS can be found on https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

VevoPay is a payment processing application which is part of the PCI DSS processing chain. It is designed to satisfy PCI DSS requirements for the application level. However, merchants are responsible to be PCI-compliance by implementing VevoPay in the PCI-compliance environment and maintain the PCI-compliance status.

1.2 PA-DSS

The Payment Application Data Security Standard (PA-DSS) is derived from PCI DSS to ensure that the payment application is compliance with PCI DSS. It is formally known as Payment Application Best Practices (PABP).

VevoPay application meets PA-DSS requirements and is validated by an independent qualified security assessor, which is ControlCase LLC (http://www.controlcase.com/).

Using VevoPay does not automatically make you PCI-compliance. You will need to follow advises in this document and the PCI DSS document along with the regulations set forth by your payment providers, such as Visa CISP (Cardholder Information Security Program).

http://usa.visa.com/merchants/risk_management/cisp_merchants.html

http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf

1.3 About This Manual

This guide explains how to implement VevoPay application in the PCI DSS compliance environment. However, it does not replace the actual PCI DSS documents that are published https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

This guide will be revised and republished as necessary in the following cases:

- The document will be updated at least on the yearly basis.
- The document will be updated if minor or major changes are made to the VevoPay application.
- The document will be updated if changes are made to PA-DSS requirements.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

2. Credit Card Data Security

2.1 Credit Card Data Storage

Credit card data compose of several elements such credit card number, cardholder name, and CVV2. PCI DSS specifies that some card data elements can be stored and some elements cannot be stored after authorization.

All credit card data storage must be encrypted with the strong encryption method (such as AES). PCI DSS allows the following card data elements to be stored:

- Primary Account Number (PAN)
- Cardholder Name
- Service Code
- Expiration Date

According to PCI DSS, the following card data cannot be stored after credit card authorization has finished (even if encrypted):

- Full Magnetic Stripe Data
- CAV2/CVC2/CVV2/CID
- PIN/PIN Block

2.2 Notes to Customers/Integrators

For customers or integrators who require customization or new features in the VevoPay application, please be aware that you will need to keep the credit card data storage rules as shown above in chapter 2.1 to be PCI compliance.

The web server will need to transmit credit card data via secure channels, such as SSL (version 3) or TLS (version 1). The sensitive authentication data (magnetic stripe, CVV2, PIN) cannot be stored after credit card is authorized.

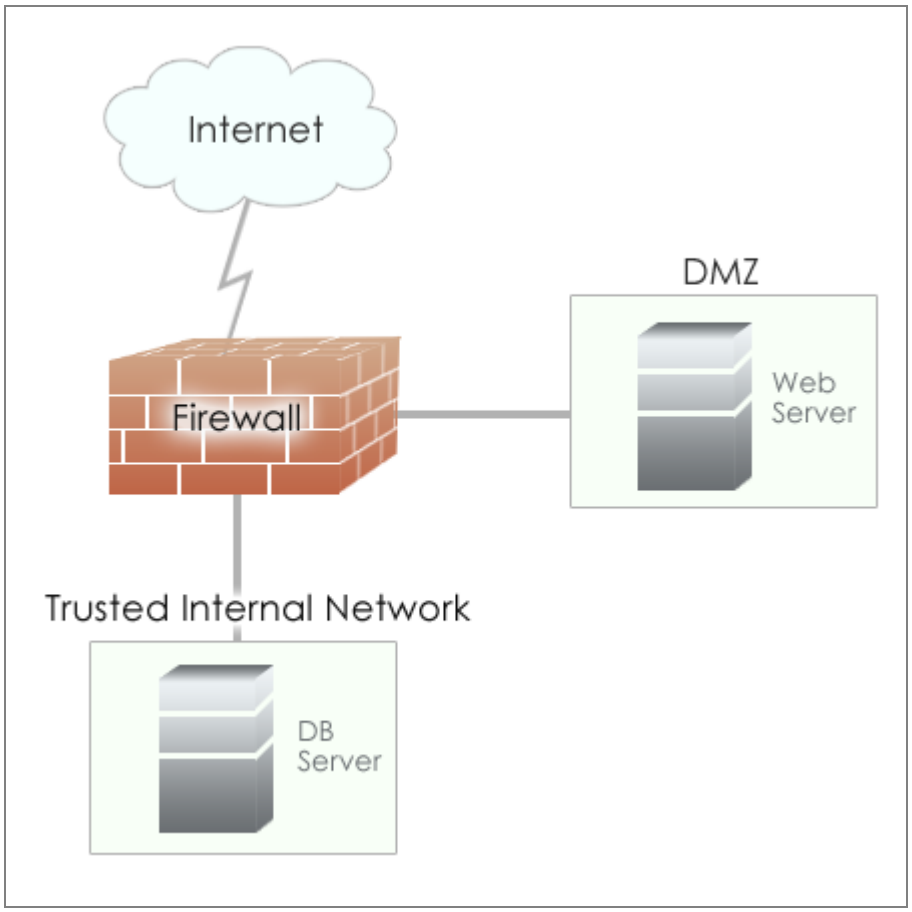
Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

3. Server Environment

To be compliance with PCI DSS, the server and network environments must meet certain security requirements.

3.1 Install and Maintain Firewall Configuration

Firewalls must be installed to control network traffic between internal network (trusted) and external/Internet network (untrusted). The firewall must product unauthorized access from untrusted networks.



The diagram above is the simplified view of network segmentation. VevoPay application is installed a web server. This web server is on the DMZ, which is the external-facing network to receive traffic from the Internet. Remote access needs to be two-factor authentication, such as user ID and password and an additional authentication item such as a token.

The database server must be on a trusted internal network that cannot be accessed directly from the Internet. Your cardholder data will be stored on this server. The cardholder data cannot be stored on the server that can be accessed directly from the Internet.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

The firewall should be configured to open only the required ports. For example, the firewall in the database server may be configured to open the port for SQL Server database, but not for HTTP service (port 80).

You will also need to install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the trusted network.

3.2 User and Password Policies

PCI DSS requires that each user must have a unique ID to access system components or cardholder data. Therefore, any PCs, servers, and databases that are installed with VevoPay or hold cardholder data must have a unique ID for each user of such systems.

In addition, passwords of these user accounts should follow the PCI DSS strong password policy below:

- Password length must be at least 7 characters.
- Password must contain both numeric and alphabetic characters.
- Each user must have a unique user account. Do not use group, shared, or generic accounts and password.
- Password must be changed at least every 90 days.
- When changing password, the last 4 passwords cannot be reused.
- Consecutive invalid login attempts will cause the account to be locked out after six times. The lockout period will be at least 30 minutes.

For Microsoft Windows, these settings can be found under “Local Security Policy” application in your “Administrative Tools”. Both web and database servers should use strong MS Windows password policies.

For Microsoft SQL Server database, the instructions on how to set password policies can be found in http://msdn.microsoft.com/en-us/library/ms161959.aspx.

Do not use a guest users, shared/system users, or users with no password to log in to the servers. These users should be disabled in both OS and database levels.

Do not use default system users to log in, such as “sa” for SQL Server. Create a unique ID for each individual user in your organization.

3.3 Audit Policy

You should enable all possible audit logs for both server OS and database software.

For Microsoft Windows, you can enable the audit logs in “Local Policies → Audit Policy” option in the “Local Security Policy” application. You should set all policy events to “Success, Failure” to log all events.

For Microsoft SQL Server, you should enable the login auditing for both failed and successful logins. This option can be set in the “Security” topic in the server properties option window.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

3.4 Use Latest Security Patches

Update all latest security patches of the software on your servers, particularly OS and database software. For Microsoft products, you can use “Windows Update” command on your Microsoft Windows operating system.

3.5 Disable Unnecessary Services

You should disable all unnecessary or unsafe services on both your web and database server OS.

Examples of services to be disabled on both web and database servers are:

- Telnet
- Messengers
- FTP

In addition, for the database server, you should also disable the following unused services:

- IIS
- SMTP

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

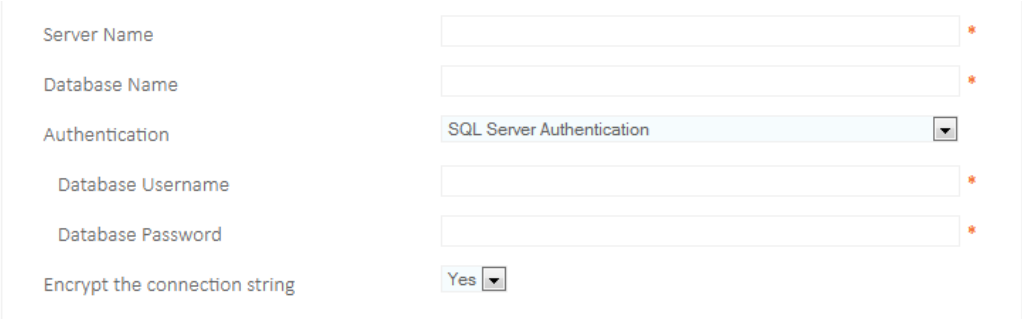
4. VevoPay Software Installation

Please follow the regular installation steps for VevoPay application. However, there are some considerations that relate to PCI DSS.

4.1 Database User

During the installation, the system will ask you to enter database information such as server name, database name, username and password.

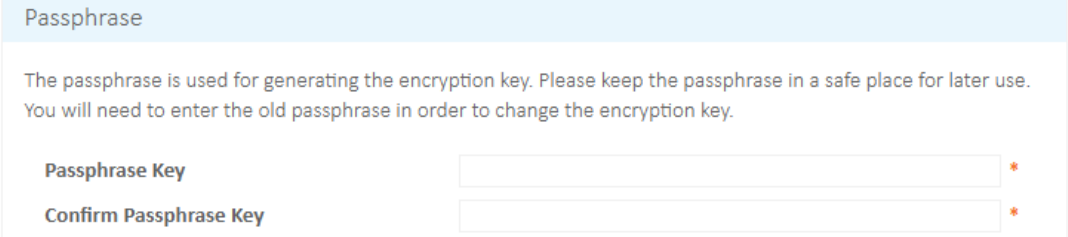
You need to specify a unique username for your database access. You cannot share the database accounts between several websites. The password of database user should be a strong password of at least 7 characters with a mix of digits and letters.



The option “Encrypt the connection string” should be set to “Yes” to encrypt the connection string to your database.

4.2 Passphrase Setup

During the installation, the system will ask you to enter passphrase. This passphrase will be used for generating a secure encryption key. This key will be used for encrypting cardholder data.



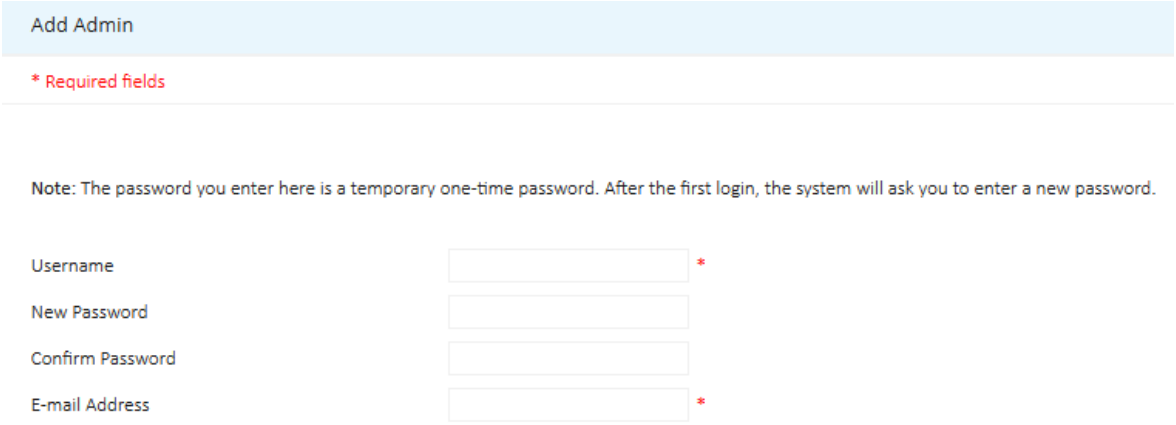
Please keep the passphrase that you enter for later use. It will be needed later when you change the encryption key.

According to PCI DSS, the encryption key needs to be changed at least manually. You can change it by going to Configuration screen of the Admin website.

4.3 Admin Account Creation

During the installation, the system will ask you to create a new user account for the default administrator. This account will have all administrator privileges upon creation.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.



Do not use the generic account name, such as “admin” or “root”, which is easy to guess. The password needs to follow PCI DSS, which have the following minimum requirements:

- Password length must be at least 7 characters.
- Password must contain both numeric and alphabetic characters.

Once the user finishes installation and log in for the first time, the system will prompt the user to enter a new password.

The default account and password policies will follow other PCI DSS requirements.

- Each user must have a unique user account. Do not use group, shared, or generic accounts and password.
- Password must be changed at least every 90 days.
- When changing password, the last 4 passwords cannot be reused.
- Consecutive invalid login attempts will cause the account to be locked out after six times. The lockout period will be at least 30 minutes.
- If the session is idle for more than 15 minutes, the user will need to re-enter the password.

Password policy can be changed in the Configuration screen of the admin website.

4.4 Secure Connection (SSL/TLS)

By default, all access to VevoPay website will be secure connection (https) using SSL/TLS protocols.

VevoPay needs to operate with SSL/TLS in the production environment. All pages in Admin website will use https protocol automatically. This will enable secure data transmit between the browser and the web server.

For testing or working on a local machine, this setting can be changed in the Configuration screen once a user has logged in. This setting can also be changed in the file App_Data\PaymentSettings.config as shown below:

```
...
<SSLEnabled>False</SSLEnabled>
...
```

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

4.5 Delete Sensitive Authentication Data

This section applies only if you use an existing system that stores sensitive authentication data. PCI DSS requires that all previous sensitive data be deleted securely. The sensitive authentication data include:

- Any magnetic stripe data.
- Card validation values or codes.
- PINs or PIN block data.

4.5.1 VevoCart Database

If you use Offline Credit Card payment method in an older version of VevoCart (version 4.0 and before), encrypted credit card data may be stored in the database. To delete these data, please follow the instructions below:

1) Open SQL Server Management Studio and log in.
2) Open the script file “App_Data\DeleteVevoCartSenstiveData.sql”.
3) Select the existing VevoCart database as the destination from the drop-down GUI.
4) Click “Execute” button.

This will delete all stored credit card data from the old VevoCart database. VevoPay does not accept offline credit card data from older versions of VevoCart.

4.5.2 Other Shopping Cart Applications

If you use VevoPay with another shopping cart application, to be compliance with PCI DSS, you will also need to securely delete sensitive authentication data that might be stored by the application. This includes any magnetic stripe data, card validation values or codes, and PINs or PIN block data. Please consult with your application vendor for the best way to this.

4.5.3 Collecting Sensitive Data for Troubleshooting

VevoPay never stores sensitive authentication data (e.g. CVV2) in the database or file system. However, if you need to collect these values for troubleshooting or debugging purpose, you will need to customize the application. Please keep the following guideline to be compliance with PCI DSS:

- Collect sensitive authentication data only when needed to solve a specific problem. Do not store the sensitive data in the automatic error log that always records upon application startup.
- Store such data in a specific, known location with limited access.
- Collect only a limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete of such data immediately after use.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

4.6 Delete Old Cryptographic Key

This section applies only if you have an existing system that stored credit card data in the database. PCI DSS requires that old cryptographic keys be deleted securely.

4.6.1 VevoCart 3.x and Older

If you upgrade your software from VevoCart 3.x or older, please edit the Web.config file in your VevoCart website directory. You should find a line with data similarly to below:

```
<add key="SecretKey" value="[EncryptionKeyValue]"/>
```

The value in *[EncryptionKeyValue]* is the old encryption key of VevoCart 3.x. Please change this value to a new one.

4.6.2 VevoCart 4.0

If you upgrade your software from VevoCart 4.0, please use SDelete tool to securely delete the file App_Data\System\EncryptionKey.config in your VevoCart website. An example of the command is below:

```
sdelete -p 1 [LocalWebsitePath]\App_Data\System\EncryptionKey.config
```

The *[LocalWebsitePath]* is the path of your website, such as C:\wwwroot\vevocart.com\. SDelete tool can be downloaded from:

http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

4.6.3 Other Shopping Cart Applications

If you use VevoPay with another shopping cart application, to be compliance with PCI DSS, you will also need to securely delete old encryption key. Please consult with your application vendor the best way to this.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

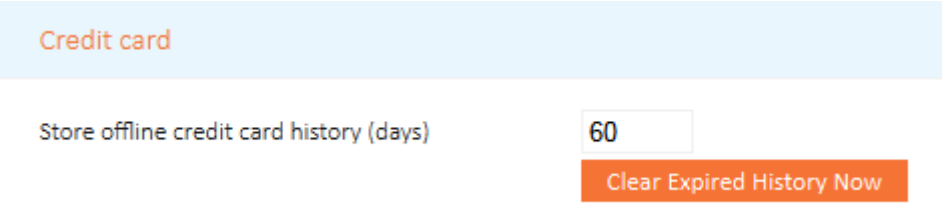
5. PCI-Related Configurations

Once the installation has completed, the user can log in to the VevoPay website and change the settings as needed. This chapter will discuss some settings that relate to PCI DSS requirements.

5.1 Cardholder Data History

The system will not keep cardholder data, including credit card number and expiration date, once the credit card is authorized by the payment processor.

For Offline Credit Card payment method, the cardholder data will be stored for later processing in the database. This information will be stored for the number of days shown in the configuration.



Expired cardholder data in the database will be purged regularly with actions on VevoPay application, such as admin website browsing. However, the user may also purge the expired data manually by clicking the button “Clear Expired History Now”.

The VevoPay application does not store CVV2 in the database for Offline Credit Card method.

If you would like to delete the credit card data manually, you may take a look at the database table “ClientRecord”. This database table will store encrypted credit card data in the database fields below. Please note that you will need to use a secure delete method to delete credit card data.

- CreditCardType
- CreditCardNumber
- CardholderName
- ExpirationMonth
- ExpirationYear
- CardIssue
- CardStart
- BillingFirstName
- BillingLastName

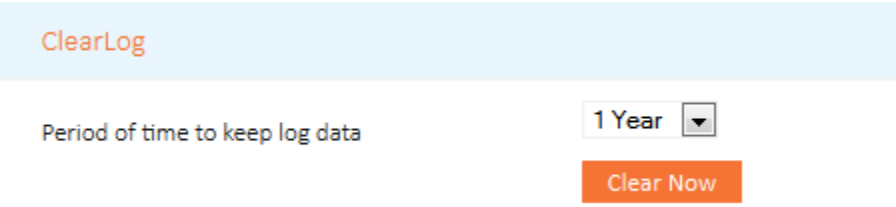
Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

5.2 Audit Trails

The system automatically records audit trails of the system events, such as log in, log out, user creation, and the viewing of credit card data and audit trail itself.

The audit trails can be viewed only with the user with appropriate user permissions, which are set in “Admin Accounts” menu of the Admin website.

Audit trails will be kept in the database for at least 1 year, which is the minimum requirement of PCI DSS. The user can clear older logs manually in the Configuration screen of the Admin website.



Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

6. Other Considerations

6.1 Wireless Security

PCI DSS also applies to wireless technology if cardholder data are transmitted over the wireless network, or wireless network is used to access database server. In those cases, the following requirements are needed:

- Wireless devices need to use strong encryption technology and use the industry best practices, such as IEEE 802.11i (WPA and WPA2). The older security technology, WEP, cannot be used for PCI DSS purpose.
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2).
- The wireless settings, such as encryption keys, SSID, passwords/passphrases, SNMP community strings, need to be changed from the default values.
- The encryption key also needs to be changed when the person who knows the key leaves the company or changes the position.
- Install a firewall between wireless environment and cardholder data environment. Configure the firewall to control the traffic from wireless environment or deny the wireless traffic altogether.
- Install personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet and are used to access the organization's network.
- Other security-related wireless vendor defaults, if applicable must be implemented.

6.2 Email and Messaging Security

Email and other end-user messaging technologies (e.g. instant messaging) are not secure channels to send sensitive information, i.e. credit card number (PAN). By default, VevoPay never sends credit card number over the email or other insecure channels.

Do not send unencrypted credit card numbers using email or other insecure technologies.

6.3 Remote Access

There are situations that you need to remotely access your network. According to PCI DSS, to access the server remotely, you need to use two-factor authentication, such as user ID and password and an additional authentication item such as a token.

Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

Some additional security considerations for remote access that you may implement are:

- Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins.
- Enable encrypted data transmission.
- Enable account lockout after a certain number of failed login attempts.
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish strong customer password management policy.

Copyright © 2006-2013 Vevo Systems Co., Ltd. All Rights Reserved.