

First Data Merchant Services / SecurityMetrics

PCI Compliance Self-Assessment Questionnaire D 1.2

First Data Merchant Services has partnered with SecurityMetrics to help you evaluate the status of your account, to assist with any necessary remediation efforts and to certify your account's PCI compliance. You can reach SecurityMetrics by calling (800) 557-4684 or by going to their website (securitymetrics.com). Be sure to identify yourself as a merchant of First Data Merchant Services

In order to help you address those questions found in the "Self-Assessment Questionnaire D1.2" that relates to PaymentMate software, Tempus has provided this document. Below is a copy of each of the questions with a PaymentMate response.

Please call the number found above regarding any questions you may have about the "Self-Assessment Questionnaire D1.2".

Abbreviated PCI Self-Assessment Questionnaire D 1.2

1.3 Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment?
Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

You may want to contact your IT staff or internet provider to find the answer to this question.

1.3.4 Are internal addresses prohibited from passing from the Internet into the DMZ?
Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

1.5 Has IP-masquerading been implemented to prevent internal addresses from being translated and revealed on the Internet?

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).

Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

2.1 Are vendor-supplied defaults always changed before installing a system on the network?

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

3.4 Is PAN, at a minimum, rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs,) by using any of the following approaches?

- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures.

The MINIMUM account information that must be rendered unreadable is the PAN. If for some reason, a company is unable to render the PAN unreadable, refer to Appendix B: "Compensating Controls."

Note: "Strong cryptography" is defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.

Yes No

Yes ~ for PaymentMate POS

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

4.1 Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?

Examples of open, public networks that are in scope of the PCI DSS are the Internet, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).

Yes No

Yes ~ for PaymentMate POS

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

5.1 Is anti-virus software deployed on all systems, particularly personal computers and servers, commonly affected by malicious software?

Yes No

PaymentMate POS ships with Antivirus software.

It is up to the merchant to be sure that

- 1) Its subscription is current**
- 2) Its updates are applied and occurring on a regular basis**

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

6.1 Do all system components and software have the latest vendor-supplied security patches installed?

Yes No

Yes ~ for PaymentMate POS

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

6.3 Are software applications developed based on industry best practices, and do they incorporate information security throughout the software development life cycle? Is prevention of common coding vulnerabilities covered in software development processes, including invalidated input, SQL injection, buffer overflows end cross-site scripting (XSS)?

Yes No

Yes ~ for PaymentMate POS

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

8.1 Are all users assigned a unique ID before allowing them to access system components or cardholder data?

Yes No

PaymentMate POS – provides the security mechanism to do this. It is up to the merchant to define and implement a security policy for PaymentMate POS.

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

How to setup the security for PaymentMate POS

- 1) **Go to [www. TempusTechnologies.com](http://www.TempusTechnologies.com)**
- 2) **Left click on “Technical Support” and select “Support Documents”**

IF you are a Pharmacy then:

- 3) **Scroll down the list and under “Other PaymentMate support” left click on “PaymentMate Pharmacy Edition reference guide”**
- 4) **Once it opens, save the document on to your desktop by left clicking on File \ Save Page As... \ select your desktop and save the file. Later on you can reopen this document by clicking on it from the Desktop.**
- 5) **In this document go to Section 3.4 Configuring Security Options. Follow the directions on added employees to PaymentMate and configuring the security option.**

IF not then:

- 3) **Scroll down the list and under “Other PaymentMate support” left click on “PaymentMate reference guide”**
- 4) **Once it opens, save the document on to your desktop by left clicking on File \ Save Page As... \ select your desktop and save the file. Later on you can reopen this document by clicking on it from the Desktop.**
- 5) **In this document go to Section 7 - Using PaymentMate with Security**
- 6) **Enabled. Follow the directions on added employees to PaymentMate and configuring the security option.**

10.6 Are logs for all system components reviewed at least daily?

Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.

Yes No

PaymentMate provides logging capability. It is the merchant’s responsibility to maintain compliance. See “How to setup the security for PaymentMate POS” to question 8.1

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

How to Learn PaymentMate POS Logging

- 1) **Go to www.TempusTechnologies.com**
- 2) **Left click on “Technical Support” and select “Support Documents”**

IF you are a Pharmacy then:

- 3) **Scroll down the list and under “Other PaymentMate support” left click on “PaymentMate Pharmacy Edition reference guide”**
- 4) **Once it opens, save the document on to your desktop by left clicking on File \ Save Page As... \ select your desktop and save the file. Later on you can reopen this document by clicking on it from the Desktop.**
- 5) **In this document go to Section 9. Using the PaymentMate Security Features.**

IF not then:

- 3) **Scroll down the list and under “Other PaymentMate support” left click on “PaymentMate reference guide”**

- 4) **Once it opens, save the document on to your desktop by left clicking on File \ Save Page As... \ select your desktop and save the file. Later on you can reopen this document by clicking on it from the Desktop.**
- 5) **In this document go to Section 7.2 Viewing the Security Journal.**

10.7 Is audit trail history retained for at least one year, with a minimum of three months' history immediately available for analysis (for examples, online, archived, or restorable from backup)?

Yes No

PaymentMate POS – provides the backup mechanism to do this. It is up to the merchant to define and implement a backup policy for PaymentMate POS.

This question encompasses a broader topic than just PaymentMate. Therefore, the merchant needs to explore what other software applications they run which also may apply to this question.

11.2 Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)?

Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.

Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

11.4 Are network intrusion detection systems, host- based intrusion detection systems, and intrusion prevention systems used to monitor all network traffic and alert personnel to suspected compromises?

Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

11.5 Is file integrity monitoring software deployed to alert personnel to unauthorized modification of critical system or content files?

Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.

SM1.1 Have you read all PCI DSS 1.2 requirements and are all of your systems currently in compliance?

Yes No

This question does not apply to PaymentMate.

It encompasses a broader topic. Therefore, it has to be explored and answered by the merchant with the help of Security Metrics.