Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire C- VT and Attestation of Compliance

Before You Begin

SAQ C-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet.

A virtual payment terminal is web-browser-based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Expected Testing

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the P H U F K Self-Assessment with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS). Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank)

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Self-Assessment Questionnaire C-VT

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
1.3					

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question	Expected Testing	Response

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question	Expected Testing	Response

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
4.1.1	Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?	ƒ Review documented standards ƒ Review wireless networks ƒ Examine system configuration settings	☐	☐	☐	☐
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	ƒ Review policies and procedures	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
5.3	Are all anti-virus mechanisms: ƒ Actively running? ƒ Unable to be disabled or altered by users? Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	ƒ Examine anti-virus configurations ƒ Examine system components ƒ Observe processes ƒ Interview personnel	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.1	Is there a process to identify security vulnerabilities, including the following:					

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

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

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:					
7.1.2	Is access to privileged user IDs restricted as follows: ƒ To least privileges necessary to perform job responsibilities? ƒ Assigned only to roles that specifically require that privileged access?	ƒ Examine written access control policy ƒ Interview personnel ƒ Interview management ƒ Review privileged user IDs				

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.3	Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication, as follows: Note: Multi-factor authentication requires that a minimum of two of the three authentication methods					

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	ƒ Review periodic media destruction policies and procedures ƒ Interview personnel ƒ Observe processes	☐	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	ƒ Review periodic media destruction policies and procedures ƒ Examine security of storage containers	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

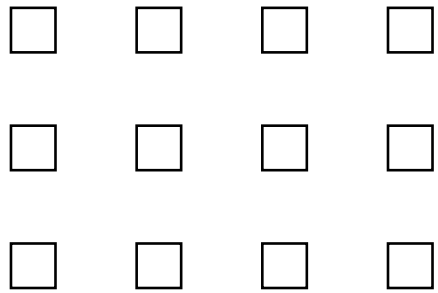
Note:) R U W K H S X U S R V H V R I 5 H T X L U H P H Q W time part-3 me E m p o y e s, t e m p o r a y e m p o y e s a n d p e r s o n n e l, a n d F R Q W U D F W R U V D Q G F R Q V X O W D Q W V Z K R D U H ³ U H V L G H Q W ´ R Q W K H H Q W L W ' a t a e n v r n m e n t. R U R W K H U Z

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	ƒ Review the information security policy	☐	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	ƒ Review the information security policy ƒ Interview responsible personnel	☐	☐	☐	☐
12.3	Are usage policies for critical technologies developed to define proper use of these technologies and require the following: Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.					
12.3.1	Explicit approval by authorized parties to use the technologies?	ƒ Review usage policies ƒ Interview responsible personnel	☐	☐	☐	☐
12.3.3	A list of all such devices and personnel with access?	ƒ Review usage policies ƒ Interview responsible personnel	☐	☐	☐	☐
12.3.5	Acceptable uses of the technologies?	ƒ Review usage policies ƒ Interview responsible personnel	☐	☐	☐	☐
12.4	Do security policy and proc586.53 2c504 reW*nBT/F4.94 1					

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.5	(b) Are the following information security management responsibilities formally assigned to an individual or team:					
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	*f* Review information security policy and procedures	☐	☐	☐	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	*f* Review security awareness program	☐	☐	☐	☐
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:					
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?	*f* Review policies and procedures *f* Observe processes *f* Review list of service providers	☐	☐	☐	☐
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent WKDW WKH\ FRXOG LPSDFW WKH V cardholder data environment? Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	*f*	☐	☐	☐	☐

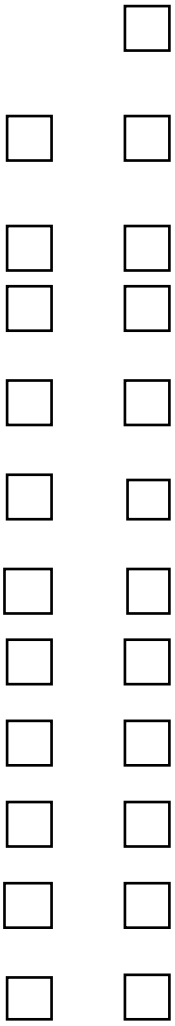
© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.



Appendix C: Explanation of Non-Applicability

If the ³1 $(Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
3.4	Cardholder data is never stored electronically

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

© 2006-2017