Payment Card Industry Data Security Standard (PCI DSS) and PC-Duo Remote Desktop Software

PC-Duo's Role in a PCI Compliant Environment

The Payment Card Industry Data Security Standard (PCI DSS) consists of 12 high-level requirements put in place to enhance cardholder data security. It applies to all entities involved in payment card processing. It also applies to any other entity that stores, processes or transmits cardholder data. Vector Networks is not a payment solution and does not deal directly with any credit card data. Therefore, the PC-Duo software falls outside of the scope for PCI review. Note that no particular software product can be deemed PCI compliant by itself as compliance requires an evaluation of the complete environment, taking into account such things as physical restrictions, business practices, all software components etc. PC-Duo software provides secure remote access that, when configured properly, can easily support an organizations PCI compliant environment. Please see the PCI Security Standards Council website (https://www.pcisecuritystandards.org/) for more information about PCI DSS.

Requirements - High Level Overview

Listed below are the 12 High Level Requirements presented in the PCI DSS "Requirements and Security Assessment Procedures version 3.2" and Vector Networks' relationship to them. Note that the full document is available on the PCI Security Standards Council Website in this library: https://www.pcisecuritystandards.org/document_library (See document: "PCI DSS").

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Given these requirements, continue reading to learn how PC-Duo software can help organizations comply with PCI DSS.

1. Install and maintain a firewall configuration to protect cardholder data. PC-Duo software is an on-premise solution. All components can be located safely behind an organizations' managed firewall in their PCI compliant data center. Depending

upon the specific edition of PC-Duo software, communications can be configured so that all remote control sessions require an outbound connection from the Host computer to the RAS (Remote Access Server).

2. Do not use vendor-supplied defaults for system passwords and other security parameters. All accounts and passwords are managed by the end user. Account credentials can be maintained using Windows Active Directory or other identity providers depending upon the edition. Standard Microsoft Windows security best practices are recommended.

3. Protect stored cardholder data. As an on-premise solution, Vector Networks does not have or collect any data from remote computers. In editions of PC-Duo that support screen recording, screen data (recordings) are stored in a proprietary format on the on-premise server. Screen recording is an option that can be turned off completely if so desired.

4. Encrypt transmission of cardholder data across open, public networks. PC-Duo software uses end-to-end AES 256-bit encryption. All sessions are encrypted by default regardless of protocol chosen (UDP/TCP/SSL).

5. Protect all systems against malware and regularly update anti-virus software or programs. Since the PC-Duo solution is an on-premise deployment, this falls under the control of the end user and their IT practices.

6. Develop and maintain secure systems and applications. PC-Duo software's service accounts have limited privileges and the system is designed with security in mind. Updates to the software are released promptly when there is an update to OpenSSL.

7. Restrict access to cardholder data by business need to know. PC-Duo software offers many layers of security and customization regarding who has access to any particular resource. In addition, the software can be configured to allow attended remote access only if so desired. Machines can be placed in groups and users can be assigned granular permissions to Host machines in those groups.

8. Identify and authenticate access to system components. PC-Duo software can be configured to use Windows authentication. Accounts can be managed in Windows Active Directory or other identity providers depending upon the edition. This includes an option to require Multifactor Authentication (MFA).

9. Restrict physical access to cardholder data. PC-Duo software does not store any cardholder data. Screen recordings can be disabled or stored on a secure on-premise server.

10. Track and monitor all access to network resources and cardholder data. Depending upon the edition, PC-Duo software will log remote control connections in the Windows Event Log on the remote machine and also keep a centralized audit log of all access to remote computers. This includes who connected to which machine and at what time and for how long. The PC-Duo Web Console allows for activity reports to be generated.

11. Regularly test security systems and processes. Vector Networks is committed to staying on top of any security issues that may arise. We monitor Microsoft Windows updates and OpenSSL releases. We provide updates to our software promptly when necessary.

12. Maintain a policy that addresses information security for all personnel. As an on-premise solution, no data is ever transmitted back to Vector Networks servers or personnel. Vector personal has no access to any customer's machines unless explicitly granted.