PCI Data Security Standards REQUIREMENTS and RESPONSIBILITIES

DCRS recommends all Merchants take the time to review the terms of the "Merchant Agreement" that they signed with their Credit Processor (or Acquirer), to determine their specific responsibilities and liabilities. The responsibility for meeting the Requirements for PCI Compliance rests with the Merchant.

However, a DCRS Support Plan is designed to *assist with a portion* of these 12 major PCI Requirements. When a Support Plan site requests assistance, DCRS can connect remotely to confirm the current status of specific items related to some of the PCI Requirements. Findings can be provided via email by a specific DCRS individual that is knowledgeable in most of the general PCI Requirements.

For Non-Support Plan sites, DCRS can confirm the software version, the validation status of the version, and explain the areas of responsibility that the DCRS Support Plan is designed to assist (as noted below), including Managed Services that provide secure remote connections, as well as protect and update our SonicWall Firewall and AntiVirus offerings.

The PCI Requirements that a POS Vendor **can best assist** the Merchant are the following (a maximum of 7 out of the 12 high-level Requirements, as outlined in PCI PA-Data Security Standard document), listed in DCRS order of importance:

- **Requirement 3: Protect stored cardholder data.** Insure a PCI-Validated Payment Application software version is installed. The "availability" of such relates to the Payment Application software manufacturer (typically POS Vendor). **Merchants must insure their system is updated with a properly validated version, and are responsible for annual rotation of encryption keys.**

- **Requirement 6: Develop and maintain secure systems and applications.** Both the Payment Application software and Operating System should have the latest security patches installed. The "availability" of such relates to the Payment Application software manufacturer (POS Vendor) and the Operating System manufacturer (typically MICROSOFT). **Merchants must insure their system is updated with both the Application and Operating System security patches, when available.**

- **Requirement 4: Encrypt transmission of cardholder data across open, public networks.** Having a PCI-validated POS software version installed *will help* provide this (see Requirement 3).

- **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.** **Although the POS Vendor should communicate this at installation, Merchants are responsible to insure secure passwords are being used by their employees after installation.**

- **Requirement 1: Install and maintain a firewall configuration to protect cardholder data.** Insure the POS Payment system is installed inside an internal network zone, segregated from any demilitarized zone (DMZ), with a separate Firewall that has packet filtering with internet traffic restrictions. DCRS can install a SonicWall firewall to meet this requirement. **Merchants that install their own firewall, allow their SonicWall Subscription to expire, or alter the installed SonicWall configuration—take sole responsibility.**

- **Requirement 5: Use and regularly update anti-virus software or programs.** DCRS can install AntiVirus Subscription Services to meet this requirement. **Merchants that install their own (or allow their Antivirus Subscription to expire) take sole responsibility.**

- **Requirement 8: Assign a unique ID to each person with computer access.** DCRS can install Live Alert & Connect and Live Manager, which has two-factor authentication for remote access. **Merchants that install their own Remote Access, or allow other vendors remote access, take sole responsibility. Merchants remain responsible for the other multiple responsibilities associated with this requirement.**

The remaining 5 high-level Requirements are exclusively Merchant-Responsible. Over 200 sub-requirements are part of the 12 high-level Requirements. There is a limit to what a POS Vendor can do, other than to advise:

- Requirement 7: Restrict access to cardholder data by business need to know
- 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
- Requirement 12: Maintain a policy that addresses information security for all personnel

True security requires 100% consistency in the execution of procedures. However, not all security can be totally automated and some security practices must involve people. Unfortunately, people are fallible, so 100% consistency is not possible when people are involved. Security is not perfect, but is about managing and minimizing risks.

The PCI Security Standards Council certifies organizations that assess and validate adherence to PCI Security Standards. Qualified Security Assessors (QSA) are organizations qualified by PCI to assess a Merchant's compliance to PCI DSS. Merchants seeking this type of assessment should contact a QSA.

8.14.14