Data security for merchants and payment card processors is the vital byproduct of applying the information security best practices found in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment, but for purposes of PCI DSS compliance, their essence is three steps: Assess, Remediate and Report.

Assess is the process of taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data. **Remediate** vulnerabilities. **Report** entails the compilation of records required by PCI DSS to validate remediation, and submission of compliance reports to the acquiring bank and card payment brands you do business with. Doing these three steps is an ongoing process for compliance with the PCI DSS requirements. These steps also enable vigilant assurance of cardholder data safety.

PCI Data Security Standard Requirements

PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements – Validated by Self or Outside Assessment
Build and Maintain a Secure Network	1. data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use 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. Assign a unique ID to each person with computer access 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

Step 1 – Assess

The primary goal of assessment is to identify all technology and process vulnerabilities posing a risk to the security of cardholder data that is transmitted, processed or stored by your business. Study the PCI DSS on our web site (www.pcisecuritystandards.org) for detailed requirements. It describes IT infrastructure and processes that access the payment card infrastructure. Determine how