PCI Security Standards Council®

PARTICIPATING ORGANIZATION™

PCI Standards Are Designed To Protect Your Business

As a merchant you are required by the card brands - Visa, MasterCard, Discover, American Express and JCB - to be compliant with the Payment Card Industry Data Security Standards (PCI DSS), a set of data security requirements designed to protect cardholder account information:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Avoid vendor-supplied defaults for passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
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.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Sterling and PCI Compliance

Each year, Sterling goes through an extensive review of its own systems to ensure that the highest security standards are in place for the handling, processing, transmission and storage of merchant card data.

Sterling has designed a program for merchants that will detect if they are PCI compliant. The process identifies vulnerabilities in a merchant's card processing system, including POS systems, personal computers or servers, Internet applications, shopping carts, paper-based storage systems, and unsecured transmission of cardholder data to service providers.

Complying with PCI DSS is your best defense against hackers who look for network vulnerabilities that enable them to steal cardholder data.

A full description of the PCI DSS requirements can be found online at: www.PCIsecuritystandards.org