

GlobalSCAPE®

HS-PCI Solution

High Security

Detail Review

Facilitating Enterprise PCI DSS Compliance

Table of Contents

Understanding the PCI DSS _____	3
The Case for Compliance _____	3
The Origin of the Standard _____	3
The Challenge of Compliance _____	4
Who Must Comply _____	5
The GlobalSCAPE Solution _____	6
Planning for Compliance _____	7

The PCI DSS Requirements

Requirement 1: Install and maintain a firewall configuration to protect cardholder data _____	8
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters _____	10
Requirement 3: Protect stored cardholder data _____	11
Requirement 4: Encrypt transmission of cardholder data across open, public networks _____	12
Requirement 5: Use and regularly update anti-virus software _____	13
Requirement 6: Develop and maintain secure systems and applications _____	14
Requirement 7: Restrict access to cardholder data by business need-to-know _____	15
Requirement 8: Assign a unique ID to each person with computer access _____	16
Requirement 9: Restrict physical access to cardholder data _____	19
Requirement 10: Track and monitor all access to network resources and cardholder data _____	20
Requirement 11: Regularly test security systems and processes _____	21
Requirement 12: Maintain a policy that addresses information security _____	22

Understanding the PCI DSS

The Case for Compliance.

Throughout history, people have sought to protect their valuable possessions. In today's world, credit card numbers are among the most valuable assets we have. To ensure their protection, the Payment Card Industry (PCI) Security Standards Council has created their Data Security Standard (DSS).

For any organization that stores, processes, or transmits Primary Account Number (PAN) data, failure to comply can have serious consequences: up to US\$500,000 per incident, increased fees, restrictions and even removal of processing privileges. Yet, even these fines look insignificant compared to the consequences of sensitive data being compromised. Apart from externally imposed penalties, the organization will also face irate customers, possible lawsuits, heavy regulatory oversight, costly repairs to their system, lost goodwill, and lost business. The true cost of a breach is estimated at \$90+ per record. At that level of cost, an ounce of prevention is indeed worth a pound of cure.

The PCI DSS as a Security Standard.

The PCI DSS is in the forefront of the drive toward cutting-edge security best practices, while companies are taking a heightened interest in security guidelines for their sensitive data, whether credit card related or not. Even for companies that are not obligated to comply, the PCI DSS offers an authoritative road map for high security systems and processes that can help guard a company's data.

The Origin of the Standard.

With the advent of the Internet and the explosion of e-commerce, the payment card industry faces an unprecedented level of security risk. As PAN data is transmitted across an increasingly wide range of electronic networks, industry leaders realized they had to collaborate on how to address security risks to cardholder data.

The PCI Security Standards Council created the PCI DSS—an authoritative roadmap for implementing high security systems and processes. The PCI DSS is a multifaceted security standard developed as a collaborative effort among six industry-leading companies: Visa, MasterCard, American Express, Diner's Club, Discover, and JCB USA, as well as many major merchants. Comprised of twelve major requirements, each with several individual categories,

