

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD HANDBOOK

Introduction.

Part 1: The Fundamentals.

Chapter 1: PCI Fundamentals.

History of PCI.

Why PCI DSS?

Chapter 2: Security 101.

Strategy and Planning.

Information Risk Management.

Information Classification.

Risk Assessment.

Risk Analysis.

Dealing With Risk.

Defence in Depth.

Policy, Standards, and Procedures.

Adoption of a Security Framework.

Security and the System Development Life Cycle (SDLC).

Security Training and Awareness.

Metrics.

Physical Security.

Data Communications and Networking.

Perimeter Security.

Information Security Monitoring and Log Management.

Intrusion Detection and Intrusion Prevention Technology.

Logical Access Control.

Electronic Authentication.

BUY ONLINE AT:

<http://www.itgovernance.co.uk/products/2099>

Encryption.

Remote Access Control.

Secure Communications.

HTTPS.

Secure Shell.

Virtual Private Networks.

Wireless.

Incident Response.

Forensics.

Part 2: PCI Breakdown (Control Objectives and Associated Standards).

Chapter 3: Build and Maintain a Secure Network.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters.

Requirement A.1: Hosting Providers Protect Cardholder Data Environment.

Chapter 4: Protect Cardholder Data.

Requirement 3: Protect Stored Cardholder Data.

PCI DSS Appendix B: Compensating Controls for Requirement 3.4.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open Public Networks.

Chapter 5: Maintain a Vulnerability Management Program.

Requirement 5: Use and Regularly Update Antivirus Software.

Requirement 6: Develop and Maintain Secure Systems and Applications.

Chapter 6: Implement Strong Access Control Measures.

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know.

Requirement 8: Assign a Unique ID to Each Person with Computer Access.

Requirement 9: Restrict Physical Access to Cardholder Data.

BUY ONLINE AT:
<http://www.itgovernance.co.uk/products/2099>

Chapter 7: Regularly Monitor and Test Networks.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data.

Requirement 11: Regularly Test Security Systems and Processes.

Chapter 8: Maintain an Information Security Policy.

Requirement 12: Maintain a Policy that Addresses Information Security.

Part 3: Strategy and Operations.

Chapter 9: Assessment and Remediation.

PCI DSS Payment Card Industry Self-Assessment Questionnaire.

PCI DSS Security Audit Procedures.

PCI DSS Security Scanning Procedures.

Leveraging Self-Assessment.

Strategy and Programme Development.

Chapter 10: PCI Programme Management.

Case for Strategic Compliance.

Who Should Be Involved Achieving PCI DSS Compliance for Our Organisation?

PCI DSS Glossary, Abbreviations, and Acronyms.

References.

Resources.

Index.

BUY ONLINE AT:
<http://www.itgovernance.co.uk/products/2099>