



Policy Coverage Matrix for Payment Card Industry Data Security Standard*

Information Security Policies Made Easy, Version 10.0

The following table provides a high-level mapping between the security requirements of the Payment Card Industry Data Security Standard and the information security policies found within ISPME V10. ISPME also provides policy coverage for many areas not specifically mentioned in the high-level requirements, but specified in the detailed requirements of the standard.

Security Topics and Requirements	Specific Sections and Policies
Build and Maintain a Secure Network	
Requirement 1: Install and maintain a firewall configuration to protect data	9.04.09 - Security Of Network Services – Web Server Firewalls. Chapter 12 - “Sample Firewall Policy”
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	9.05.04 Password Management System (26 policies) (9.05.04-23. Vendor Default Passwords)
Protect Cardholder Data	
Requirement 3: Protect stored data	9.06.01 - Information Access Restriction 12.01.03 - Safeguarding Of Organizational Records 12.01.04 - Data Protection And Privacy Of Personal Information
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	8.07.03 - Electronic Commerce Security, including other policies related to management of encryption keys and roles and responsibilities.
Maintain a Vulnerability Management Program	
Requirement 5: Use and regularly update anti-virus software	8.03 - Protection Against Malicious Software (24 policies)
Requirement 6: Develop and maintain secure systems and applications	8.02.02 - System Acceptance (12 policies) 10.05.01 - Change Control Procedures (25 policies)
Implement Strong Access Control Measures	
Requirement 7: Restrict access to data by business need-to-know	9.02.02 - Privilege Management (Section 1. Privilege Restriction — Need To Know) Also supported by various access control and logging policies.
Requirement 8: Assign a unique ID to each person with computer access	9.02.01 - User Registration 9.02.03 User Password Management (12 polices) 9.05.03 User Identification And Authentication (6 policies) 9.05.03 - User Identification And Authentication
Requirement 9: Restrict physical access to cardholder data	7 Physical And Environmental Security 7.01.01 Physical Security Perimeter 7.01.02 Physical Entry Controls (29 policies)

	7.01.03 Securing Offices, Rooms, And Facilities (5 policies) 7.01.04 Working In Secure Areas (9 policies) 7.03.01 Clear Desks And Clear Screen Policy (8 policies) 7.03.02 Removal Of Property
Regularly Monitor and Test Networks	
Requirement 10: Track and monitor all access to network resources and cardholder data	9.07.01 - Event Logging (11 policies) also relates to policies on Access Control and unique userid creation.
Requirement 11: Regularly test security systems and processes.	12.02 Reviews Of Security Policy And Technical Compliance (also in) 4.01.03-14. Authorization To Review Any Information System
Maintain an Information Security Policy	
Requirement 12: Maintain a policy that addresses information security	Information Security Policies Made Easy, Version 10 contains over 1300 pre-written information security policies, including 10 complete sample policy documents that cover the detailed requirements of this standard. (also) 3.01.01 Information Security Policy Document (10 policies) 3.01.02 Policy Review And Evaluation 6.01.01 Information Security Training

**Information based on Payment Card Industry Data Security Standard as of 12/15/2004. To protect cardholders and merchants, a consortium of credit card companies developed a set of security standards for merchants known as Payment Card Industry Data Security Standard (PCI Standard). The standard has been adopted by a range of companies, including VISA USA, which uses it as the basis for their Cardholder Information Security Programs (CISP). More about the VISA CISP and PCI Data Security Standard is available at the [VISA CISP web site](#).*