PCI-DSS Policy Mapping Table

The following table provides a high-level mapping between the security requirements of the Payment Card Industry Data Security Standard *(PCI-DSS)* and the security policy categories of Information Security Policies Made Easy (ISO 27002). 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.

<table>
<thead>
<tr>
<th>Security Topics and Requirements</th>
<th>Specific Sections and Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Requirement 1: Install and maintain a firewall configuration to protect data | 11.4 Network Access Control  
10.6.1 Network Controls (Firewalls)  
*“Sample Firewall Policy”*                                                   |
| Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters | 11.5.3 Password Management System (26 policies)  
(11.5.3-23. Vendor Default Passwords)                                          |
| **Protect Cardholder Data**                                            |                                                                                               |
| Requirement 3: Protect stored data                                     | 11.5.1 Secure log-on procedures  
11.5.2 User identification and authentication  
11.6.1 Information access restriction  
11.6.2 Sensitive system isolation  
15.1.3 Safeguarding Of Organizational Records                                    |
| Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks | 10.8 Exchange of Information  
10.9.3 Electronic Commerce Security  
11.6 Network Security Management  
12.3 Cryptographic Controls                                                  |
| **Maintain a Vulnerability Management Program**                       |                                                                                               |
| Requirement 5: Use and regularly update anti-virus software            | 10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE  
10.4.1 Controls against malicious code.  
10.4.2 Controls against mobile code                                                 |
| Requirement 6: Develop and maintain secure systems and applications    | 10.3.2 System Acceptance (12 policies)  
12.4.1 Control of operational software  
12.5.1 Change Control Procedures (25 policies)                                 |
| **Implement Strong Access Control Measures**                           |                                                                                               |
| Requirement 7: Restrict access to cardholder data by business need-to-know | 11.1.1 Access control policy  
11.2.2 Privilege Management  
11.2.2-1 Need To Know                                                           |
| Requirement 8: Assign a unique ID to each person with computer access  | 11.2.1 User Registration  
11.2.3 User Password Management (12 polices)  
11.5.2 User Identification And Authentication (6 policies)                    |
| Requirement 9: Restrict physical access to cardholder data             | 9 Physical And Environmental Security  
9.1.1 Physical security perimeter (7 policies)  
9.1.2 Physical entry controls (26 policies)  
9.1.3 Securing offices, rooms, and facilities (5 policies)  
9.2.6 Secure disposal or re-use of equipment                                      |

Copyright 2012 – Information Shield, Inc.
### Regularly Monitor and Test Networks

| Requirement 10: Track and monitor all access to network resources and cardholder data | 10.10.1 Audit logging (11 policies)  
10.10.2 Monitoring system use  
10.10.4 Administrator and operator logs  
10.10.5 Fault logging  
10.2.2 Monitoring and review of third party services  
15.3.1 System Audit Controls (3 policies) |
| --- | --- |
| Requirement 11: Regularly test security systems and processes. | 6.1.3-14 Authorization To Review Any Information System  
11.2.4 Review of user access rights  
15.2 Reviews Of Security Policy And Technical Compliance |

### Maintain an Information Security Policy

| Requirement 12: Maintain a policy that addresses information security for all personnel. | Information Security Policies Made Easy contains over 1400 pre-written information security policies, including 15 complete sample policy documents that cover the detailed requirements of this standard. (also)  
5.1 INFORMATION SECURITY POLICY  
5.1.1 Information security policy document  
5.1.2 Review of the information security policy  
8.2.2 Information security awareness, education, and training |


For more information a security policy solutions for PCI compliance visit our Regulatory Resource Center at [http://www.informationshield.com](http://www.informationshield.com)