

PCIPOLICYPORTAL.COM



**PCI**policyportal



**Payment Card Industry Data Security Standards  
(PCI DSS) Information Security Policy  
& Procedures Manual**

Version 3.0  
Released February, 2014

# Table of Contents

1.	<b>Requirement 1.1.1</b> - Formal Process for Testing and Approval of All Network Connections and Changes to Network Configurations	1
	• Overview	1
	• Responsibility for Policy Maintenance	3
2.	<b>Requirement 1.1.2 - 1.1.3</b> - Current Network Diagram with All Connections to Cardholder Data, Including Wireless Networks	4
	• Overview	4
	• Policy	4
	• Procedure	4
	• Responsibility for Policy Maintenance	5
3.	<b>Requirement 1.1.4</b> - Firewall Requirements Policy and Procedures	6
	• Overview	6
	• Policy	6
	• Procedure	6
	• Responsibility for Policy Maintenance	7
4.	<b>Requirement 1.1.5</b> - Description of Groups, Roles and Responsibilities for Logical Management of Network Components	8
	• Overview	8
	• Policy	8
	• Procedure	8
	• Responsibility for Policy Maintenance	10
5.	<b>Requirement 1.1.6</b> - Documentation and Business Justification for Use of All Services, Protocols and Ports Allowed	11
	• Overview	11
	• Policy	11
	• Procedure	11
	• Responsibility for Policy Maintenance	12
6.	<b>Checklist 1.1.6</b> - All Services, Protocols and Ports Checklist	13
7.	<b>Requirement 1.1.7</b> - Requirements to Review Firewall and Router Rules Sets at least Every Six (6) Months	16
	• Overview	16
	• Policy	16
	• Procedure	16
	• Responsibility for Policy Maintenance	17
8.	<b>Checklist 1.1.7</b> - Firewall and Router Review Checklist	18
9.	<b>Requirement 1.2 - 1.2.3</b> - Firewall and Router Configurations Policy and Procedures	16
	• Overview	16
	• Policy	16
	• Procedure	16
	• Responsibility for Policy Maintenance	17
10.	<b>Requirement 1.3.1 - 1.3.8</b> - DMZ Configuration and Internet Access to the Cardholder Data Environment Policy and Procedures	22
	• Overview	22
	• Policy	22
	• Procedure	23
	• Responsibility for Policy Maintenance	24

11. <b>Checklist 1.3.8</b> - DMZ Configuration Checklist .....	25
12. <b>Requirement 1.4</b> - Personal Firewall Software Policy and Procedures .....	28
• Overview .....	28
• Policy .....	28
• Procedure .....	28
• Responsibility for Policy Maintenance .....	29
13. <b>Requirement 2.1 - 2.1.1</b> - Changing of Vendor Supplied Default Settings Policy and Procedures .....	30
• Overview .....	30
• Policy .....	30
• Procedure .....	31
• Responsibility for Policy Maintenance .....	32
14. <b>Checklist 2.1 - 2.1.1</b> - Changing of Vendor Supplied Default Checklist .....	33
15. <b>Requirement 2.2. - 2.2.4</b> - Configuration Standards for All System Components Policy and Procedures .....	35
• Overview .....	35
• Policy .....	35
• Procedure .....	37
• Responsibility for Policy Maintenance .....	39
16. <b>Requirement 2.2. - 2.2.4</b> - Configurations Standards Checklist .....	40
17. <b>Requirement 2.3</b> - Non-Console Administrative Access Policy and Procedures .....	42
• Overview .....	42
• Policy .....	42
• Procedure .....	42
• Responsibility for Policy Maintenance .....	43
18. <b>Matrix for Req. 2.4</b> - Inventory of System Components Matrix .....	44
19. <b>Requirement 3.1</b> - Data Retention and Disposal Policy and Procedures .....	45
• Overview .....	45
• Policy .....	48
• Procedure .....	48
• Responsibility for Policy Maintenance .....	53
20. <b>Requirement 3.2.1 - 3.2.3</b> - Sensitive Authentication Data (SAD) Storage Policy and Procedures .....	54
• Overview .....	54
• Policy .....	54
• Procedure .....	54
• Responsibility for Policy Maintenance .....	54
21. <b>Checklist 3.2.1 - 3.2.3</b> - Sensitive Authentication Data Checklist for System Components .....	55
22. <b>Requirement 3.3</b> - Primary Account Number (PAN) Policy and Procedures for Masking & Displaying the PAN Digits .....	61
• Overview .....	61
• Policy .....	61
• Procedure .....	61
• Responsibility for Policy Maintenance .....	62

23. <b>Requirement 3.4</b> - Primary Account Number (PAN) System Protection Policy and Procedures.....	63
• Overview.....	63
• Policy.....	63
• Procedure.....	63
• Responsibility for Policy Maintenance.....	64
24. <b>Requirement 3.4.1</b> - Disk Encryption Policy and Procedures.....	65
• Overview.....	65
• Policy.....	65
• Procedure.....	65
• Responsibility for Policy Maintenance.....	66
25. <b>Requirement 3.5</b> - Protection of Keys used for Encryption of Cardholder Data Policy and Procedures.....	67
• Overview.....	67
• Policy.....	67
• Procedure.....	67
• Responsibility for Policy Maintenance.....	68
26. <b>Requirement 3.6</b> - Key Management Policy and Procedures.....	69
• Overview.....	69
• Policy.....	69
• Procedure.....	70
• Responsibility for Policy Maintenance.....	76
27. <b>Requirement 4.1</b> - Strong Cryptography and Protocols Policy and Procedures.....	77
• Overview.....	77
• Policy.....	77
• Procedure.....	78
28. <b>Requirement 4.2</b> - Unencrypted Primary Account Numbers (PAN) Policy and Procedures.....	79
• Overview.....	79
• Policy.....	79
• Procedure.....	79
• Responsibility for Policy Maintenance.....	80
29. <b>Requirement 5.2</b> - Anti-Virus Policy and Procedures.....	81
• Overview.....	81
• Policy.....	81
• Procedure.....	82
• Responsibility for Policy Maintenance.....	83
30. <b>Requirement 6.1 - 6.2</b> - Security Patch Management Installation Policy and Procedures.....	84
• Overview.....	84
• Policy.....	84
• Procedure.....	85
• Responsibility for Policy Maintenance.....	91
31. <b>Requirement 6.3</b> - Software Development Life Cycle Processes.....	92
• Overview.....	92
• Policy.....	92
• Procedure.....	92
• Responsibility for Policy Maintenance.....	95

32. <b>Requirement 6.3.2</b> - Custom Application Code Change Reviews Policy and Procedures.....	96
• Overview.....	96
• Policy.....	96
• Procedure.....	96
• Responsibility for Policy Maintenance.....	99
33. <b>Requirement 6.4</b> - Change Control Policy and Procedures.....	100
• Overview.....	100
• Policy.....	100
• Procedure.....	101
• Responsibility for Policy Maintenance.....	104
34. <b>Requirement 6.5 - 6.5.10</b> - Software Development Secure Coding Guidelines and Training Policy and Procedures.....	105
• Overview.....	105
• Policy.....	105
• Procedure.....	106
• Responsibility for Policy Maintenance.....	107
35. <b>Requirement 7.1 - 7.3</b> - Data Control & Access Control Policies and Procedures.....	112
• Overview.....	112
• Policy.....	112
• Procedure.....	112
• Responsibility for Policy Maintenance.....	117
36. <b>Requirement 8.1 - 8.4</b> - Unique ID & Authentication Methods Policy and Procedures.....	118
• Overview.....	118
• Policy.....	118
• Procedure.....	119
• Responsibility for Policy Maintenance.....	122
37. <b>Requirement 8.5 - 8.6</b> - Shared, Group, Generic, and Other Authentication Methods Policy and Procedures.....	123
• Overview.....	123
• Policy.....	123
• Procedure.....	124
38. <b>Requirement 8.7</b> - Database Access & Configuration Settings Policy and Procedures.....	126
• Overview.....	126
• Policy.....	126
• Procedure.....	126
• Responsibility for Policy Maintenance.....	129
39. <b>Requirement 9.1</b> - Physical Security Controls Checklist.....	130
40. <b>Requirement 9.2 - 9.4</b> - Personnel and Visitor Access Checklist.....	134
41. <b>Requirement 9.5 - 9.7.1</b> - Media Storage, Distribution and Classification Policy and Procedures.....	141
• Overview.....	141
• Policy.....	141
• Procedure.....	141
• Responsibility for Policy Maintenance.....	145

42. <b>Requirement 9.8</b> - Media Destruction Policy and Procedures.....	146
• Overview.....	146
• Policy.....	146
• Procedure.....	146
• Responsibility for Policy Maintenance.....	147
• .....	
43. <b>Requirement 9.9</b> - Media Device Protection Policy and Procedures.....	148
• Overview.....	148
• Policy.....	148
• Procedure.....	148
• Responsibility for Policy Maintenance.....	149
44. <b>Requirement 9.9.3</b> -Training for Personnel.....	150
45. <b>Requirement 10.1 – 10.3.6</b> - Audit Trails Checklists.....	151
46. <b>Requirement 10.4</b> - Time-Synchronization Technology Policy and Procedures.....	161
• Overview.....	161
• Policy.....	161
• Procedure.....	161
• Responsibility for Policy Maintenance.....	163
47. <b>Requirement 10.5</b> - Securing of Audit Trails Policy and Procedures.....	164
• Overview.....	164
• Policy.....	164
• Procedure.....	164
• Responsibility for Policy Maintenance.....	167
48. <b>Requirement 10.6</b> - Security Logs & Events Policy and Procedures.....	168
• Overview.....	168
• Policy.....	168
• Procedure.....	168
• Responsibility for Policy Maintenance.....	169
49. <b>Requirement 10.6</b> - Review of Security Logs Checklist.....	170
50. <b>Requirement 11.1</b> - Wireless Security & Access Points Policy and Procedures.....	172
• Overview.....	172
• Policy.....	172
• Procedure.....	175
• Responsibility for Policy Maintenance.....	176
51. <b>Requirement 11.1</b> - Wireless Access Points Checklist.....	177
52. <b>Requirement 11.4 - 11.5.1</b> - Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Change Detection Software (CDS) Policy and Procedures.....	179
• Overview.....	179
• Policy.....	179
• Procedure.....	179
• Responsibility for Policy Maintenance.....	180

53. <b>Requirement 11.6</b> - Security Monitoring & Testing Policy and Procedures.....	181
• Overview.....	181
• Policy.....	181
• Procedure.....	183
• Responsibility for Policy Maintenance.....	185
54. <b>Requirement 12.2</b> - Risk Assessment Matrix.....	187
• Responsibility for Policy Maintenance.....	194
55. <b>Requirement 12.3</b> - Usage Policies and Procedures.....	195
• Overview.....	195
• Policy.....	195
• Procedure.....	196
• Responsibility for Policy Maintenance.....	214
56. <b>Requirement 12.4 - 12.5.5</b> - Information Security Responsibility Policy and Procedures.....	215
• Overview.....	215
• Policy.....	215
• Procedure.....	215
• Responsibility for Policy Maintenance.....	217
57. <b>Requirement 12.6</b> - Formal Security Awareness Program.....	218
• Overview.....	218
• Policy.....	218
• Procedure.....	218
• Responsibility for Policy Maintenance.....	227
58. <b>Requirement 12.8</b> - Management of Service Providers Policy and Procedures.....	228
• Overview.....	228
• Policy.....	228
• Procedure.....	228
• Responsibility for Policy Maintenance.....	229
59. <b>Requirement 12.10</b> - Incident Response Plan.....	230
• Overview.....	230
• Policy.....	230
• Procedure.....	230
• Responsibility for Policy Maintenance.....	237
60. <b>Additional Supporting Forms and Checklists (Overview)</b> .....	238
61. <b>Authorization Form for User Access   New Employees</b> .....	239
62. <b>Authorization Form for User Access   Vendors</b> .....	243
63. <b>Authorization Form for User Access   Guests</b> .....	247
64. <b>User De-Provisioning and Off-Boarding Forms   All Users</b> .....	251
65. <b>Employee Separation Form</b> .....	254
66. <b>Incident Response Form</b> .....	257