

TABLE OF CONTENTS

Requirement 1.1.1 1

Formal Process for Testing and Approval of All Network Connections and Changes to Network Configurations..... 1

 1.1.1 Overview..... 1

 List of Network Connections Devices..... 1

 Table 1.1.1.a..... 1

 Table 1.1.1.b..... 2

 Table 1.1.1.c..... 3

 1.1.1 Responsibility for Policy Maintenance 3

Requirement 1.1.2 4

Current Network Diagram with All Connections to Cardholder Data, Including Wireless Networks..... 4

 1.1.2 Overview..... 4

 1.1.2 Policy..... 4

 1.1.2 Procedure 4

 Table 1.1.2..... 4

 Network Diagram Details 4

 1.1.2 Responsibility for Policy Maintenance 5

Requirement 1.1.4 6

Description of Groups, Roles and Responsibilities for Logical Management of Network Components..... 6

 1.1.4 Overview..... 6

 1.1.4 Policy..... 6

 1.1.4 Procedure 6

 Table 1.1.4.a 6

 Table 1.1.4.b..... 7

 1.1.4 Additional Supporting Documentation 8

 Table 1.1.4.c 8

Additional Supporting Documentation	8
1.1.4 Responsibility for Policy Maintenance	9
Requirement 1.1.5	10
Documentation and Business Justification for Use of All Services, Protocols and Ports Allowed	10
1.1.5 Overview	10
1.1.5 Policy	10
1.1.5 Procedure	10
1.1.5 Additional Supporting Documentation	10
Table 1.1.5.A.....	11
Additional Supporting Documentation	11
1.1.5 Responsibility for Policy Maintenance	11
Checklist 1.1.5.A.....	11
All Services, Protocols and Ports Checklist.....	11
Requirement 1.1.6	14
Requirements to Review Firewall and Router Rules Sets at least Every Six (6) Months.....	14
1.1.6 Overview	14
1.1.6 Policy	14
1.1.6 Procedure	14
1.1.6 Additional Supporting Documentation	14
Table 1.1.6.A.....	15
Additional Supporting Documentation	15
1.1.6 Responsibility for Policy Maintenance	15
Checklist 1.1.6.A.....	15
Firewall and Router Review Checklist	15
Requirement 1.3.1 to 1.3.8.....	17
DMZ Configuration and Internet Access to the Cardholder Data Environment Policy and Procedures	17
1.3.1 to 1.3.8 Overview	17
1.3.1 to 1.3.8 Policy	17
1.3.1 to 1.3.8 Procedure	18

1.3.1 to 1.3.8 Additional Supporting Documentation	18
Table 1.3.1 to 1.3.8 (A)	18
Additional Supporting Documentation	18
1.3.1 to 1.3.8 Responsibility for Policy Maintenance	18
Checklist 1.3.1 to 1.3.8 (A)	18
DMZ Configuration Checklist.....	18
Requirement 1.4	21
Personal Firewall Software Policy and Procedures	21
1.4 Overview.....	21
1.4 Policy.....	21
1.4 Procedure	21
Defining Mobile and/or Employee-Owned Computers	21
Approved Personal Firewall Software and System Settings	22
System Administrative Rights for Personal Firewall Software.....	22
1.4 Additional Supporting Documentation	22
1.4 Responsibility for Policy Maintenance	22
Requirement 2.1 to 2.1.1	23
Changing of Vendor Default Settings Policy and Procedures.....	23
2.1 to 2.1.1 Overview	23
2.1. to 2.1.1 Policy	23
2.1 to 2.1.1 Procedure.....	23
Changing of Vendor-supplied Defaults for All System Components	24
Initiation and Justification of Wireless Environment.....	24
Wireless Infrastructure	24
Implementation.....	24
Operations and Maintenance	24
Disposition.....	24
2.1 to 2.1.1 Responsibility for Policy Maintenance	24
Requirement 2.2 to 2.3	25

Configuration Standards for All System Components Policy and Procedures	25
2.2 to 2.3 Overview	25
2.2 to 2.3 Policy	25
2.2 to 2.3 Procedure	26
System Configuration Standards.....	26
Table 2.2.a.....	26
Only One Primary Function per Server	27
System Configuration and Hardening Procedures.....	27
Non-Console Administrative Access	28
2.2 to 2.3 Additional Supporting Documentation	28
Table 2.2B	28
Additional Supporting Documentation.....	28
2.2 to 2.3 Responsibility for Policy Maintenance	29
Requirement 2.1 to 2.3.....	30
Vendor Default Settings and Configuration Standards Checklist	30
Requirement 3.1	33
Data Retention and Disposal Policy and Procedures.....	33
3.1 Overview.....	33
3.1. Policy.....	33
Description of Data and Scope for Cardholder Environment	33
Description of Key Terms and Phrases	33
Types of Data.....	36
Electronic Media	36
Hardcopy Format	36
3.1 Procedure	36
Procedure for Obtaining Data	37
Procedure for Protecting Data	37
Procedure for Accessing, Modifying or Transferring Cardholder Data.....	37
Provisions and Procedures for Retaining Data.....	38

Provisions and Procedures for Disposing of and Destroying Data.....	38
Responsible Parties for Data Retention Activities	38
Responsible Parties for Data Disposal Activities	39
Legal and Regulatory Requirements for Retention of Cardholder Data.....	39
Business Justification for Retention of Cardholder Data	40
Table 3.1.a.....	40
Electronic Media Storage of Cardholder Data	40
Table 3.1.b.....	41
Hardcopy Format Storage of Cardholder Data	41
Programmatic (Automatic) Removal of Cardholder Data.....	41
Manual Removal of Cardholder Data.....	42
Additional Information.....	42
3.1 Responsibility for Policy Maintenance	42
Requirement 3.2.1 to 3.2.3.....	43
Sensitive Authentication Data Checklist for Network Devices	43
Requirement 3.2.1 to 3.2.3	48
Sensitive Authentication Data Checklist for Operating Systems.....	48
Requirement 3.2.1 to 3.2.3.....	53
Sensitive Authentication Data Checklist for Applications	53
Requirement 3.3	58
Primary Account Number (PAN) Policy and Procedures for Displaying the PAN Digits.....	58
3.3 Overview.....	58
3.3 Policy.....	58
3.3 Procedure	58
Table 3.3.a	58
3.3 Responsibility for Policy Maintenance	59
Requirement 3.4	60
Primary Account Number (PAN) System Protection	60
Policy and Procedures.....	60

3.4 Overview	60
3.4 Policy.....	60
3.4 Procedure	60
System used for Protecting the PAN	60
Encryption	61
Other Means Utilized for Protecting the PAN.....	61
3.4 Responsibility for Policy Maintenance	61
Requirement 3.5	62
Protection of Keys used for Encryption of Cardholder Data Policy and Procedures.....	62
3.5 Overview	62
3.5 Policy.....	62
3.5 Procedure	62
Access to Cryptographic Keys.....	62
Storage and Location of Cryptographic Keys	63
3.5 Responsibility for Policy Maintenance	63
Requirement 3.6	64
Key Management Policy and Procedures	64
3.6 Overview	64
3.6 Policy.....	64
3.6 Procedure	65
General Description of System Components that Incorporate Key-Management Procedures	65
Generation of Strong Keys	65
Secure Key Distribution	65
Secure Key Storage.....	66
Periodic Key Changes at the end of the Defined Cryptoperiod	67
Retirement and Destruction of Old Keys	67
Replacement of Known or Suspected Compromised Keys.....	68
Table 3.6.a.....	68
Key Management Compromise Plan (KMCP): Systems Components Impact	68

Table 3.6.b.....	69
Key Management Compromise Plan (KMCP): Personnel	69
Table 3.6.c.....	69
Key Management Compromise Plan (KMCP): Notification Process for External Vendors.....	69
Split Knowledge and Dual Control of Keys.....	69
Table 3.6.D	70
Prevention of Unauthorized Substitution of Keys	70
Key Custodians to Sign Form Confirming the Understanding and Acceptance of their Key Custodian Responsibilities	70
Table 3.6.e.....	71
3.6 Responsibility for Policy Maintenance	71
Requirement 4.2	72
Unencrypted Primary Account Numbers (PAN) Policy and Procedures.....	72
4.2 Overview.....	72
4.2 Policy.....	72
4.2 Procedure	72
Table 4.2.a	72
4.2 Responsibility for Policy Maintenance	73
Requirement 5.2	74
Anti-Virus Policy and Procedures.....	74
5.2 Overview.....	74
5.2 Policy.....	74
5.2 Procedure	75
Anti-Virus Software Utilized.....	75
Table 5.2.a.....	75
Anti-Virus Attributes for the Cardholder Data Environment.....	75
Table 5.2.b.....	76
Anti-Virus Attributes for Computers Not Directly Related to the Cardholder Data Environment.....	76
5.2 Responsibility for Policy Maintenance	76

Requirement 6.1 to 6.2	77
Security Patch Management Installation Policy and Procedures	77
6.1 to 6.2 Overview	77
6.1 to 6.2 Policy	77
6.1 to 6.2 Procedure	78
Security Patch Management Program Employee	79
Table 6.1.a.....	79
Security Patch Management Program Employee.....	79
Comprehensive Inventory of All System Components Directly Associated with the Cardholder Environment.....	79
Table 6.1.b.....	79
Comprehensive Inventory of all other IT Resources Not Directly Associated with the Cardholder Environment.....	80
Table 6.1.c.....	80
Industry-Leading Security Sources and Additional Supporting Resources	81
Table 6.1.d.....	81
Online Resources for Patch Management, Alerts, Security and Support, As Applicable ..	81
Risk Ranking for Security Patch Management	82
Table 6.1.E.....	83
Risk Ranking Table	83
Database of Remediation Activities that Need to be Applied	84
Table 6.1.f	84
Test Procedures for Testing Patches Regarding Remediation	84
Procedures for the Distribution, Deployment and Implementation of Patches and other Related Security-Hardening Procedures	85
Procedures for Verifying Successful Implementation of Patches and other Related Security- Hardening Procedures.....	85
6.1 to 6.2 Responsibility for Policy Maintenance	85
Requirement 6.3	86
Software Development Life Cycle Processes	86

6.3 Overview.....	86
6.3 Policy.....	86
6.3 Procedure	86
New System/Application and Feature Development	86
Request for New System/Application or Features.....	87
Feasibility Study.....	87
Estimate and HW/SW Requirements.....	87
Management Decision	87
Requirement Analysis.....	87
Design.....	87
Implementation.....	88
Quality Assurance and Testing.....	88
Release for Production.....	88
6.3 Additional Software Development Requirements for PCI DSS	88
6.3 Additional Supporting Documentation	89
Table 6.3	89
Additional Supporting Documentation	89
6.3 Responsibility for Policy Maintenance	89
Requirement 6.3.2	91
Custom Application Code Change Reviews Policy and Procedures	91
6.3.2 Overview.....	91
6.3.2 Policy.....	91
6.3.2 Procedure	91
Table 6.3.7.a	92
Custom Application Code Changes for Internally-Developed Applications.....	92
6.3.2 Additional Supporting Documentation	93
Table 6.3.7.A.....	93
Additional Supporting Documentation for Code Reviews	93
6.3.2 Responsibility for Policy Maintenance	94

Requirement 6.4	95
Change Control Policy and Procedures.....	95
6.4 Overview.....	95
6.4 Policy.....	95
6.4 Procedure	96
Change Control Initiation, Implementation and Authorization Directives	96
Change Control Lifecycle	96
Formally Request a Change	96
Categorize and Prioritize the Change	96
Justification and Analysis of the Change	96
Approving and Scheduling the Change.....	97
Implementation of the Change.....	97
Post-Implementation Review for any Changes	97
Minimum Reporting Criteria for Change Control Documentation	97
Separation of Duties between Different Environments	98
Production Data and Test Data Requirements	98
6.4 Additional Supporting Documentation	98
Table 6.4.A.....	98
Additional Supporting Documentation	98
6.4 Responsibility for Policy Maintenance	99
Requirement 6.5 to 6.59.....	100
Software Development Secure Coding Guidelines and Training Policy and Procedures	100
6.5 to 6.5.9 Overview	100
6.5 to 6.5.9 Policy	100
6.5 to 6.5.9 Procedure	101
Initiatives for Secure Coding Techniques.....	101
Developing Secure Applications to Thwart Common Threats.....	101
6.5 to 6.5.9 Additional Supporting Documentation	102
Table 6.5 to 6.5.9 (A).....	102

Additional Supporting Documentation	102
6.5 to 6.5.9 Responsibility for Policy Maintenance	103
Requirement 6.5.a and 6.5.b	104
Secure Coding Training Checklist	104
Required Training Procedures for Secure Coding for OWASP-Recognized Vulnerabilities .	104
Adherence to OWASP-Recognized Vulnerabilities	105
Required Training Procedures for Secure Coding for CWE/SANS Top 25 Software Errors .	106
Secure Code Training Procedures for Specific Languages	110
Requirement 7.1 to 7.2.3	111
Data Control & Access Control Policies and Procedures	111
7.1 to 7.2.3 Overview	111
7.1 to 7.2.3 Policy	111
7.1 to 7.2.3 Procedure	111
Restricting Access to Fewest Privileges Necessary for Job Functions and RBAC Measures	111
Primary Elements of Role-Based Access Control (RBAC)	112
Permissions/Operations and Objects.....	112
Lastly, RBAC Primary Rules Consist of the Following	112
Authorization Form	113
Automated Access Control System for All System Components	113
Table 7.a.....	114
Automated Access Controls System and RBAC Architecture: Network Devices	114
Table 7.b.....	115
Automated Access Controls System and RBAC Architecture: Operating Systems.....	115
Table 7.c.....	115
Automated Access Controls System and RBAC Architecture: Applications	116
Table 7.d.....	116
Automated Access Controls System and RBAC Architecture: Databases.....	116
Table 7.e.....	117
7.1 to 7.2.3 Responsibility for Policy Maintenance	117

Requirement 8.1 to 8.4	118
Unique ID & Authentication Methods Policy and Procedures	118
8.1 to 8.4 Overview	118
8.1 to 8.4 Policy	118
8.1 to 8.4 Procedure	118
Authentication Methods used for all System Components	119
Assignment of Unique ID and Password	120
Two-Factor Authentication	120
Transmission and Storage of Passwords	120
8.1 to 8.4 Additional Supporting Documentation	120
Additional Supporting Documentation	120
8.1 to 8.4 Responsibility for Policy Maintenance	121
Requirement 8.5 to 8.5.15	122
Proper Authentication & Password Management	122
Policy and Procedures	122
8.5 to 8.5.15 Overview	122
8.5 to 8.5.15 Policy	122
8.5 to 8.5.15 Procedure	123
Authorization Form	123
Password Resets	124
First-Time Passwords	124
Terminated Employees	124
Inactive Accounts	124
Vendor Accounts	125
Generic User IDs and Shared User IDs and Passwords	125
Password Parameters	125
Familiarity and Acknowledgement of Password Policy and Procedures	125
8.5 to 8.5.15 Responsibility for Policy Maintenance	125
Requirement 8.5.1	126

Authorization Form for User Access	126
Requirement 8.5.16	130
Database Authentication and Configuration	130
Policy and Procedures.....	130
8.5.16 Overview.....	130
8.5.16 Policy.....	130
8.15.16 Procedures.....	130
Database Authentication Procedures	130
Table 8.15.16.a.....	131
Database Authentication Methods.....	131
Database Access Rights and Stored Procedures	131
Table 8.15.16.b	132
Database Access Rights and Stored Procedures.....	132
Database Administrators.....	132
Database Applications and Related Application IDs	133
Database Tools	133
Table 8.15.16.c.....	133
Database Tools and Uses	133
8.5.16 Responsibility for Policy Maintenance	133
Requirement 9.1	134
Physical Security Controls Checklist.....	134
Requirement 9.2 to 9.4	139
Personnel and Visitor Access Checklist.....	139
Requirement 9.7 to 9.7.2	144
Media Distribution and Classification	144
Policy and Procedures.....	144
9.7 to 9.7.2 Overview	144
9.7 to 9.7.2 Policy	144
9.7 to 9.7.2 Procedure	144

Definition of Media	144
Media in hardcopy format	144
Media in electronic format	145
Classification of Media and Information Assets.....	145
Table 9.7.....	145
Logging of Media	147
Secure Transport of Media.....	147
9.7 to 9.7.2 Responsibility for Policy Maintenance	147
Requirement 9.9	148
Storage and Maintenance of Hardcopy and Electronic Media Policy and Procedures.....	148
9.9 Overview	148
9.9 Policy.....	148
9.9 Procedure	148
Protection of All Hardcopy and Electronic Media.....	149
Storage and Inventory of Media	149
Sending, Retrieving and Receiving Media.....	149
9.9 Responsibility for Policy Maintenance	150
Requirement 9.10	151
Periodic Media Destruction Policy and Procedures	151
9.10 Overview.....	151
9.10 Policy.....	151
9.10 Procedure	151
Destruction of Hardcopy Materials.....	151
Destruction of Electronic Media	152
9.10 Responsibility for Policy Maintenance	152
Requirement 10.1 to 10.3.6.....	153
Audit Trails Checklist.....	153
Requirement 10.4	162
Time-Synchronization Technology.....	162

Policy and Procedures.....	162
10.4 Overview.....	162
10.4 Policy.....	162
10.4 Procedures.....	162
Time-Synchronization Security Requirements.....	163
Correct and Consistent Time.....	163
Time-Synchronization Environment.....	163
Protection of Time.....	164
Time-Synchronization Personnel	164
10.4 Responsibility for Policy Maintenance	164
Requirement 10.5	165
Securing of Audit Trails Policy and Procedures	165
10.5 Overview.....	165
10.5 Policy.....	165
10.5 Procedures.....	165
Viewing of Audit Trail Files.....	165
Table 10.5.A	166
Personnel Allowed to View Audit Trails.....	166
Protection of Audit Trail Files.....	166
Table 10.5.B	166
Procedures for Protection of Audit Trail Files	166
Centralized Log Server Environment.....	166
Table 10.5.C.....	167
Centralized Log Server Environment	167
Logs for External-Facing Technologies.....	167
Table 10.5.D	167
External Facing Technologies and Log Requirements	167
File Integrity Monitoring	167
Table 10.5.E.....	168

File Integrity Monitoring	168
10.5 Responsibility for Policy Maintenance	168
Requirement 10.6	169
Review of Security Logs Policy and Procedures.....	169
10.6 Overview	169
10.6 Policy.....	169
10.6 Procedure	169
10.6 Responsibility for Policy Maintenance	169
Checklist 10.6.A	169
Review of Security Logs Checklist	169
Requirement 10.7	172
Audit Trail History & Log Retention Policy and Procedures	172
10.7 Overview	172
10.7 Policy.....	172
10.7 Procedure	172
Table 10.7	172
10.7 Responsibility for Policy Maintenance	173
Requirement 11.1	174
Wireless Access Points Checklist	174
Requirement 12.1	175
Information Security Policy.....	175
Requirement 12.1.2	176
Annual Formal Risk Assessment Process	176
12.1.2 Overview.....	176
12.1.2 Policy.....	176
12.1.2 Procedure	176
The Scope of Risk Assessment	176
System and Technology Risks.....	176
Table 12.1.2.....	177

Business Administrative Risks	177
Business Revenue Risks.....	177
Operational Risks.....	178
12.1.2 Responsibility for Policy Maintenance	178
Requirement 12.3	179
Usage Policies and Procedures	179
12.3 Overview.....	179
12.3 Policy.....	179
12.3 Procedure	180
Explicit Management Approval to Use the Technologies	180
Table 12.3.a.....	180
Use of All Technology Resources Must be Authenticated.....	195
Listing and Labeling of All Devices and Personnel Authorized to Use Them.....	196
Table 12.3.b.....	196
Acceptable Use.....	197
General Guidelines, Responsibilities and Acceptable Use for the Technology	197
Unacceptable Use and Behavior	198
Disciplinary Action.....	198
Acceptable Network Locations for the Technology	198
List of Company-Approved Products	198
Table 12.3.c.....	198
Additional Usage Policy Requirements	199
12.3 Responsibility for Policy Maintenance	200
Requirement 12.4 to 12.5.5.....	201
Information Security Responsibilities	201
12.4 to 12.5.5 Overview	201
12.4 to 12.5.5 Policy	201
12.4 to 12.5.5 Procedure	201
Information Security Responsibilities for Employees and Contractors	202

Formal Assignment of Information Security	202
Table 12.4.a.....	202
Table 12.4.b.....	203
Information Security Responsibilities Matrix	203
12.4 to 12.5.5 Responsibility for Policy Maintenance	204
Requirement 12.6	205
Formal Security Awareness Program.....	205
12.6 Overview	205
12.6 Policy.....	205
12.6 Procedure	205
Program Phases.....	205
Design.....	206
Identify and Structure Organizational Training Needs	206
Centralized Mode.....	206
Moderately Decentralized Model.....	206
Entirely Decentralized Model	207
Comprehensive Assessment of Needs	207
Table 12.6.a.....	207
Develop Training Strategy Plan	208
Develop	208
Develop Material and Select Relevant Topics.....	209
Identify Source Material to be Used	210
Table 12.6.b.....	210
Refine Material and Develop Model for Training Employees.....	210
Table 12.6.c.....	211
Implement	213
Communicate the Plan to All Employees.....	213
Communicating Security Awareness to Employees.....	213
Delivering Training to Employees	213

Maintain/Oversight	214
Monitor Adherence to the Program	214
Collect Vital Feedback on the Program	214
Manage Changes as Needed for the Program	214
Table 12.6.d.....	214
Core Components.....	215
12.6 Responsibility for Policy Maintenance	215
Requirement 12.8	216
Management of Service Providers Policy and Procedures.....	216
12.8 Overview.....	216
12.8 Policy.....	216
12.8 Procedure	216
Table 12.8.....	216
List of Service Providers	216
12.8 Responsibility for Policy Maintenance	217
Requirement 12.9	218
Incident Response Plan	218
12.9 Overview.....	218
12.9 Policy.....	218
12.9 Procedure	219
Preparing for an Incident	219
Table 12.9.a.....	220
Description of Incident Response Team	220
Detecting an Incident	221
Table 12.9.b.....	221
Responding to and Containing an Incident	222
Table 12.9.c.....	222
Response Mechanisms for All Critical System Components and All Other IT Resources Deemed Critical by <i>[company name]</i>	222
Table 12.9.d.....	224

Recovery from an Incident	225
Post-Incident Activities and Awareness	225
12.9 Responsibility for Policy Maintenance	226
Reference List.....	227