

---

**SECTION II SAQ D** PAYMENT CARD INDUSTRY DATA  
SECURITY STANDARDS (PCI DSS) POLICIES &  
PROCEDURES

**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.....	12
All Services, Protocols and Ports Checklist .....	12
Requirement 1.1.6 .....	15
Requirements to Review Firewall and Router Rules Sets at least Every Six (6) Months.....	15
1.1.6 Overview.....	15
1.1.6 Policy.....	15
1.1.6 Procedure .....	15
1.1.6 Additional Supporting Documentation .....	15
Table 1.1.6.A.....	16
Additional Supporting Documentation .....	16
1.1.6 Responsibility for Policy Maintenance .....	16
Checklist 1.1.6.....	17
Firewall and Router Review Checklist.....	17
Requirement 1.3.1 to 1.3.8.....	19
DMZ Configuration and Internet Access to the Cardholder Data Environment Policy and Procedures .....	19
1.3.1 to 1.3.8 Overview .....	19
1.3.1 to 1.3.8 Policy .....	19
1.3.1 to 1.3.8 Procedure .....	20
1.3.1 to 1.3.8 Additional Supporting Documentation .....	20

Table 1.3.1 to 1.3.8.....	20
Additional Supporting Documentation .....	20
1.3.1 to 1.3.8 Responsibility for Policy Maintenance.....	20
Checklist 1.3.1 to 1.3.8.....	21
DMZ Configuration Checklist .....	21
Requirement 1.4 .....	23
Personal Firewall Software Policy and Procedures .....	23
1.4 Overview.....	23
1.4 Policy.....	23
1.4 Procedure .....	23
Defining Mobile and/or Employee-Owned Computers .....	23
Approved Personal Firewall Software and System Settings .....	24
System Administrative Rights for Personal Firewall Software.....	24
1.4 Additional Supporting Documentation .....	24
1.4 Responsibility for Policy Maintenance .....	24
Requirement 2.1 to 2.1.1.....	25
Changing of Vendor Default Settings Policy and Procedures.....	25
2.1 to 2.1.1 Overview .....	25
2.1. to 2.1.1 Policy .....	25
2.1 to 2.1.1 Procedure.....	25
Changing of Vendor-supplied Defaults for All System Components .....	26
Initiation and Justification of Wireless Environment.....	26
Wireless Infrastructure .....	26
Implementation.....	26
Operations and Maintenance .....	26
Disposition.....	26
2.1 to 2.1.1 Responsibility for Policy Maintenance.....	26
Requirement 2.2 to 2.3.....	27
Configuration Standards for All System Components Policy and Procedures .....	27

2.2 to 2.3 Overview .....	27
2.2 to 2.3 Policy .....	27
2.2 to 2.3 Procedure .....	28
System Configuration Standards.....	28
Table 2.2.a.....	28
Only One Primary Function per Server .....	29
System Configuration and Hardening Procedures.....	29
Non-Console Administrative Access .....	30
2.2 to 2.3 Additional Supporting Documentation .....	30
Table 2.2B .....	30
Additional Supporting Documentation.....	30
2.2 to 2.3 Responsibility for Policy Maintenance .....	31
Requirement 2.1 to 2.3.....	32
Vendor Default Settings and Configuration Standards Checklist .....	32
Requirement 3.1 .....	35
Data Retention and Disposal Policy and Procedures.....	35
3.1 Overview.....	35
3.1. Policy.....	35
Description of Data and Scope for Cardholder Environment .....	35
Description of Key Terms and Phrases .....	35
Types of Data.....	38
Electronic Media .....	38
Hardcopy Format .....	38
3.1 Procedure .....	38
Procedure for Obtaining Data .....	39
Procedure for Protecting Data .....	39
Procedure for Accessing, Modifying or Transferring Cardholder Data.....	39
Provisions and Procedures for Retaining Data.....	40
Provisions and Procedures for Disposing of and Destroying Data.....	40

Responsible Parties for Data Retention Activities .....	40
Responsible Parties for Data Disposal Activities .....	41
Legal and Regulatory Requirements for Retention of Cardholder Data.....	41
Business Justification for Retention of Cardholder Data .....	42
Table 3.1.a.....	42
Electronic Media Storage of Cardholder Data .....	42
Table 3.1.b.....	43
Hardcopy Format Storage of Cardholder Data .....	43
Programmatic (Automatic) Removal of Cardholder Data.....	43
Manual Removal of Cardholder Data.....	44
Additional Information.....	44
3.1 Responsibility for Policy Maintenance .....	44
Requirement 3.2.1 to 3.2.3.....	45
Sensitive Authentication Data Checklist for Network Devices .....	45
Requirement 3.2.1 to 3.2.3.....	50
Sensitive Authentication Data Checklist for Operating Systems.....	50
Requirement 3.2.1 to 3.2.3.....	55
Sensitive Authentication Data Checklist for Applications .....	55
Requirement 3.3 .....	60
Primary Account Number (PAN) Policy and Procedures for Displaying the PAN Digits.....	60
3.3 Overview.....	60
3.3 Policy.....	60
3.3 Procedure .....	60
Table 3.3.a .....	60
3.3 Responsibility for Policy Maintenance .....	61
Requirement 3.4 .....	62
Primary Account Number (PAN) System Protection .....	62
Policy and Procedures.....	62
3.4 Overview.....	62

3.4 Policy.....	62
3.4 Procedure .....	62
System used for Protecting the PAN.....	62
Encryption .....	63
Other Means Utilized for Protecting the PAN.....	63
3.4 Responsibility for Policy Maintenance .....	63
Requirement 3.5 .....	64
Protection of Keys used for Encryption of Cardholder Data Policy and Procedures.....	64
3.5 Overview.....	64
3.5 Policy.....	64
3.5 Procedure .....	64
Access to Cryptographic Keys.....	64
Storage and Location of Cryptographic Keys .....	65
3.5 Responsibility for Policy Maintenance .....	65
Requirement 3.6 .....	66
Key Management Policy and Procedures .....	66
3.6 Overview.....	66
3.6 Policy.....	66
3.6 Procedure .....	67
General Description of System Components that Incorporate Key-Management Procedures .....	67
Generation of Strong Keys .....	67
Secure Key Distribution.....	67
Secure Key Storage.....	68
Periodic Key Changes at the end of the Defined Cryptoperiod.....	69
Retirement and Destruction of Old Keys .....	69
Replacement of Known or Suspected Compromised Keys.....	70
Table 3.6.a.....	70
Key Management Compromise Plan (KMCP): Systems Components Impact .....	70
Table 3.6.b.....	71

Key Management Compromise Plan (KMCP): Personnel .....	71
Table 3.6.c .....	71
Key Management Compromise Plan (KMCP): Notification Process for External Vendors	71
Split Knowledge and Dual Control of Keys .....	71
Table 3.6.D .....	72
Prevention of Unauthorized Substitution of Keys .....	72
Key Custodians to Sign Form Confirming Understanding and Acceptance of Key Custodian Responsibilities.....	72
Table 3.6.e.....	73
3.6 Responsibility for Policy Maintenance .....	73
Requirement 4.2 .....	74
Unencrypted Primary Account Numbers (PAN) Policy and Procedures.....	74
4.2 Overview.....	74
4.2 Policy.....	74
4.2 Procedure .....	74
Table 4.2.a .....	74
4.2 Responsibility for Policy Maintenance .....	75
Requirement 5.2 .....	76
Anti-Virus Policy and Procedures.....	76
5.2 Overview.....	76
5.2 Policy.....	76
5.2 Procedure .....	77
Anti-Virus Software Utilized.....	77
Table 5.2.a.....	77
Anti-Virus Attributes for the Cardholder Data Environment.....	77
Table 5.2.b.....	78
Anti-Virus Attributes for Computers Not Directly Related to Cardholder Data Environment.....	78
5.2 Responsibility for Policy Maintenance .....	78
Requirement 6.1 to 6.2.....	79



Security Patch Management Installation Policy and Procedures .....	79
6.1 to 6.2 Overview .....	79
6.1 to 6.2 Policy .....	79
6.1 to 6.2 Procedure .....	80
Security Patch Management Program Employee .....	81
Table 6.1.a.....	81
Security Patch Management Program Employee.....	81
Comprehensive Inventory of All System Components Directly Associated with Cardholder Environment.....	81
Table 6.1.b.....	81
Comprehensive Inventory of all other IT Resources Not Directly Associated with Cardholder Environment.....	82
Table 6.1.c.....	82
Industry-Leading Security Sources and Additional Supporting Resources .....	83
Table 6.1.d.....	83
Online Resources for Patch Management, Alerts, Security and Support, As Applicable ..	83
Risk Ranking for Security Patch Management .....	84
Table 6.1.E.....	85
Risk Ranking Table .....	85
Database of Remediation Activities that Need to be Applied .....	86
Table 6.1.f .....	86
Test Procedures for Testing Patches Regarding Remediation.....	86
Procedures for the Distribution, Deployment and Implementation of Patches and other Related Security-Hardening Procedures .....	87
Procedures for Verifying Successful Implementation of Patches and other Related Security-Hardening Procedures.....	87
6.1 to 6.2 Responsibility for Policy Maintenance .....	87
Requirement 6.3 .....	88
Software Development Life Cycle Processes .....	88
6.3 Overview.....	88

6.3 Policy.....	88
6.3 Procedure .....	88
New System/Application and Feature Development .....	88
Request for New System/Application or Features.....	89
Feasibility Study.....	89
Estimate and HW/SW Requirements .....	89
Management Decision .....	89
Requirement Analysis.....	89
Design.....	89
Implementation.....	90
Quality Assurance and Testing.....	90
Release for Production.....	90
6.3 Additional Software Development Requirements for PCI DSS .....	90
6.3 Additional Supporting Documentation .....	91
Table 6.3.....	91
Additional Supporting Documentation .....	91
6.3 Responsibility for Policy Maintenance .....	91
Requirement 6.3.2 .....	93
Custom Application Code Change Reviews Policy and Procedures .....	93
6.3.2 Overview.....	93
6.3.2 Policy.....	93
6.3.2 Procedure .....	93
Table 6.3.7.a.....	94
Custom Application Code Changes for Internally-Developed Applications.....	94
6.3.2 Additional Supporting Documentation .....	95
Table 6.3.7.A.....	95
Additional Supporting Documentation for Code Reviews.....	95
6.3.2 Responsibility for Policy Maintenance .....	96
Requirement 6.4 .....	97

Change Control Policy and Procedures.....	97
6.4 Overview.....	97
6.4 Policy.....	97
6.4 Procedure .....	98
Change Control Initiation, Implementation and Authorization Directives.....	98
Change Control Lifecycle.....	98
Formally Request a Change .....	98
Categorize and Prioritize the Change .....	98
Justification and Analysis of the Change .....	98
Approving and Scheduling the Change.....	99
Implementation of the Change.....	99
Post-Implementation Review for any Changes .....	99
Minimum Reporting Criteria for Change Control Documentation .....	99
Separation of Duties between Different Environments .....	100
Production Data and Test Data Requirements .....	100
6.4 Additional Supporting Documentation .....	100
Table 6.4.A.....	100
Additional Supporting Documentation .....	100
6.4 Responsibility for Policy Maintenance .....	101
Requirement 6.5 to 6.59.....	102
Software Development Secure Coding Guidelines and Training Policy and Procedures.....	102
6.5 to 6.5.9 Overview .....	102
6.5 to 6.5.9 Policy .....	102
6.5 to 6.5.9 Procedure.....	103
Initiatives for Secure Coding Techniques.....	103
Developing Secure Applications to Thwart Common Threats.....	103
6.5 to 6.5.9 Additional Supporting Documentation .....	104
Table 6.5 to 6.5.9 (A).....	104
Additional Supporting Documentation .....	104

6.5 to 6.5.9 Responsibility for Policy Maintenance .....	105
Requirement 6.5.a and 6.5.b .....	106
Secure Coding Training Checklist .....	106
Required Training Procedures for Secure Coding for OWASP-Recognized Vulnerabilities. .	106
Adherence to OWASP-Recognized Vulnerabilities .....	107
Required Training Procedures for Secure Coding for CWE/SANS Top 25 Software Errors .	108
Secure Code Training Procedures for Specific Languages .....	112
Requirement 7.1 to 7.2.3 .....	113
Data Control & Access Control Policies and Procedures .....	113
7.1 to 7.2.3 Overview .....	113
7.1 to 7.2.3 Policy .....	113
7.1 to 7.2.3 Procedure .....	113
Restricting Access to Fewest Privileges Necessary for Job Functions and RBAC Measures	113
Primary Elements of Role-Based Access Control (RBAC) .....	114
Permissions/Operations and Objects.....	114
Lastly, RBAC Primary Rules Consist of the Following.....	114
Authorization Form .....	115
Automated Access Control System for All System Components.....	115
Table 7.a.....	116
Automated Access Controls System and RBAC Architecture: Network Devices .....	116
Table 7.b.....	117
Automated Access Controls System and RBAC Architecture: Operating Systems.....	117
Table 7.c.....	117
Automated Access Controls System and RBAC Architecture: Applications .....	118
Table 7.d.....	118
Automated Access Controls System and RBAC Architecture: Databases.....	118
Table 7.e.....	119
7.1 to 7.2.3 Responsibility for Policy Maintenance .....	119
Requirement 8.1 to 8.4.....	120

Unique ID & Authentication Methods Policy and Procedures .....	120
8.1 to 8.4 Overview .....	120
8.1 to 8.4 Policy .....	120
8.1 to 8.4 Procedure .....	120
Authentication Methods used for all System Components.....	121
Assignment of Unique ID and Password .....	122
Two-Factor Authentication .....	122
Transmission and Storage of Passwords.....	122
8.1 to 8.4 Additional Supporting Documentation .....	122
Additional Supporting Documentation .....	122
8.1 to 8.4 Responsibility for Policy Maintenance .....	123
Requirement 8.5 to 8.5.15.....	124
Proper Authentication & Password Management .....	124
Policy and Procedures.....	124
8.5 to 8.5.15 Overview .....	124
8.5 to 8.5.15 Policy .....	124
8.5 to 8.5.15 Procedure .....	125
Authorization Form .....	125
Password Resets.....	126
First-Time Passwords .....	126
Terminated Employees .....	126
Inactive Accounts .....	126
Vendor Accounts .....	127
Generic User IDs and Shared User IDs and Passwords .....	127
Password Parameters.....	127
Familiarity and Acknowledgement of Password Policy and Procedures.....	127
8.5 to 8.5.15 Responsibility for Policy Maintenance .....	127
Requirement 8.5.1 .....	128
Authorization Form for User Access .....	128

Requirement 8.5.16 .....	132
Database Authentication and Configuration .....	132
Policy and Procedures.....	132
8.5.16 Overview.....	132
8.5.16 Policy.....	132
8.15.16 Procedures.....	132
Database Authentication Procedures .....	132
Table 8.15.16.a.....	133
Database Authentication Methods.....	133
Database Access Rights and Stored Procedures .....	133
Table 8.15.16.b .....	134
Database Access Rights and Stored Procedures.....	134
Database Administrators.....	134
Database Applications and Related Application IDs .....	135
Database Tools .....	135
Table 8.15.16.c.....	135
Database Tools and Uses .....	135
8.5.16 Responsibility for Policy Maintenance .....	135
Requirement 9.1 .....	136
Physical Security Controls Checklist.....	136
Requirement 9.2 to 9.4.....	141
Personnel and Visitor Access Checklist.....	141
Requirement 9.7 to 9.7.2 .....	146
Media Distribution and Classification.....	146
Policy and Procedures.....	146
9.7 to 9.7.2 Overview .....	146
9.7 to 9.7.2 Policy .....	146
9.7 to 9.7.2 Procedure .....	146
Definition of Media .....	146

Media in hardcopy format .....	146
Media in electronic format .....	147
Classification of Media and Information Assets.....	147
Table 9.7.....	147
Logging of Media .....	149
Secure Transport of Media.....	149
9.7 to 9.7.2 Responsibility for Policy Maintenance.....	149
Requirement 9.9 .....	150
Storage and Maintenance of Hardcopy and Electronic Media Policy and Procedures.....	150
9.9 Overview.....	150
9.9 Policy.....	150
9.9 Procedure .....	150
Protection of All Hardcopy and Electronic Media.....	151
Storage and Inventory of Media .....	151
Sending, Retrieving and Receiving Media.....	151
9.9 Responsibility for Policy Maintenance .....	152
Requirement 9.10 .....	153
Periodic Media Destruction Policy and Procedures .....	153
9.10 Overview.....	153
9.10 Policy.....	153
9.10 Procedure .....	153
Destruction of Hardcopy Materials.....	153
Destruction of Electronic Media .....	154
9.10 Responsibility for Policy Maintenance .....	154
Requirement 10.1 to 10.3.6.....	155
Audit Trails Checklist.....	155
Requirement 10.4 .....	164
Time-Synchronization Technology.....	164
Policy and Procedures.....	164

10.4 Overview.....	164
10.4 Policy.....	164
10.4 Procedures.....	164
Time-Synchronization Security Requirements.....	165
Correct and Consistent Time.....	165
Time-Synchronization Environment.....	165
Protection of Time.....	166
Time-Synchronization Personnel .....	166
10.4 Responsibility for Policy Maintenance .....	166
Requirement 10.5 .....	167
Securing of Audit Trails Policy and Procedures .....	167
10.5 Overview.....	167
10.5 Policy.....	167
10.5 Procedures.....	167
Viewing of Audit Trail Files.....	167
Table 10.5.A .....	168
Personnel Allowed to View Audit Trails.....	168
Protection of Audit Trail Files.....	168
Table 10.5.B .....	168
Procedures for Protection of Audit Trail Files .....	168
Centralized Log Server Environment.....	168
Table 10.5.C.....	169
Centralized Log Server Environment .....	169
Logs for External-Facing Technologies.....	169
Table 10.5.D .....	169
External Facing Technologies and Log Requirements .....	169
File Integrity Monitoring .....	169
Table 10.5.E.....	170
File Integrity Monitoring .....	170



10.5 Responsibility for Policy Maintenance .....	170
Requirement 10.6 .....	171
Review of Security Logs Policy and Procedures.....	171
10.6 Overview.....	171
10.6 Policy.....	171
10.6 Procedure .....	171
10.6 Responsibility for Policy Maintenance .....	171
Checklist 10.6 .....	172
Review of Security Logs Checklist .....	172
Requirement 10.7 .....	174
Audit Trail History & Log Retention Policy and Procedures .....	174
10.7 Overview.....	174
10.7 Policy.....	174
10.7 Procedure .....	174
Table 10.7.....	174
10.7 Responsibility for Policy Maintenance .....	175
Requirement 11.1 .....	176
Wireless Access Points Checklist .....	176
Requirement 12.1 .....	177
Information Security Policy.....	177
Requirement 12.1.2 .....	178
Annual Formal Risk Assessment Process .....	178
12.1.2 Overview.....	178
12.1.2 Policy.....	178
12.1.2 Procedure .....	178
The Scope of Risk Assessment .....	178
System and Technology Risks.....	178
Table 12.1.2.....	179
Business Administrative Risks .....	179

Business Revenue Risks .....	179
Operational Risks.....	180
12.1.2 Responsibility for Policy Maintenance .....	180
Requirement 12.3 .....	181
Usage Policies and Procedures .....	181
12.3 Overview.....	181
12.3 Policy.....	181
12.3 Procedure .....	182
Explicit Management Approval to Use the Technologies .....	182
Table 12.3.a.....	182
Use of All Technology Resources Must be Authenticated.....	197
Listing and Labeling of All Devices and Personnel Authorized to Use Them.....	198
Table 12.3.b.....	198
Acceptable Use.....	199
General Guidelines, Responsibilities and Acceptable Use for the Technology .....	199
Unacceptable Use and Behavior .....	200
Disciplinary Action.....	200
Acceptable Network Locations for the Technology.....	200
List of Company-Approved Products .....	200
Table 12.3.c.....	200
Additional Usage Policy Requirements .....	201
12.3 Responsibility for Policy Maintenance .....	202
Requirement 12.4 to 12.5.5.....	203
Information Security Responsibilities.....	203
12.4 to 12.5.5 Overview .....	203
12.4 to 12.5.5 Policy .....	203
12.4 to 12.5.5 Procedure.....	203
Information Security Responsibilities for Employees and Contractors .....	204
Formal Assignment of Information Security .....	204

Table 12.4.a.....	204
Table 12.4.b.....	205
Information Security Responsibilities Matrix .....	205
12.4 to 12.5.5 Responsibility for Policy Maintenance.....	206
Requirement 12.6 .....	207
Formal Security Awareness Program.....	207
12.6 Overview.....	207
12.6 Policy.....	207
12.6 Procedure .....	207
Program Phases.....	207
Design.....	208
Identify and Structure Organizational Training Needs .....	208
Centralized Mode.....	208
Moderately Decentralized Model.....	208
Entirely Decentralized Model .....	209
Comprehensive Assessment of Needs.....	209
Table 12.6.a.....	209
Develop Training Strategy Plan .....	210
Develop .....	210
Develop Material and Select Relevant Topics.....	211
Identify Source Material to be Used .....	212
Table 12.6.b.....	212
Refine Material and Develop Model for Training Employees.....	212
Table 12.6.c.....	213
Implement.....	215
Communicate the Plan to All Employees.....	215
Communicating Security Awareness to Employees.....	215
Delivering Training to Employees .....	215
Maintain/Oversight .....	216

Monitor Adherence to the Program .....	216
Collect Vital Feedback on the Program.....	216
Manage Changes as Needed for the Program .....	216
Table 12.6.d.....	216
Core Components.....	217
12.6 Responsibility for Policy Maintenance .....	217
Requirement 12.8 .....	218
Management of Service Providers Policy and Procedures.....	218
12.8 Overview.....	218
12.8 Policy.....	218
12.8 Procedure .....	218
Table 12.8.....	218
List of Service Providers .....	218
12.8 Responsibility for Policy Maintenance .....	219
Requirement 12.9 .....	220
Incident Response Plan.....	220
12.9 Overview.....	220
12.9 Policy.....	220
12.9 Procedure .....	221
Preparing for an Incident .....	221
Table 12.9.a.....	222
Description of Incident Response Team .....	222
Detecting an Incident.....	223
Table 12.9.b.....	223
Responding to and Containing an Incident.....	224
Table 12.9.c.....	224
Response Mechanisms for All Critical System Components and All Other IT Resources Deemed Critical by <i>[company name]</i> .....	224
Table 12.9.d.....	226
Recovery from an Incident.....	227

Post-Incident Activities and Awareness .....	227
12.9 Responsibility for Policy Maintenance .....	228
Reference List.....	229

[Return to Top](#)