
TABLE OF CONTENTS

1.1.1 Requirement

FORMAL PROCESS FOR APPROVING AND TESTING ALL NETWORK CONNECTIONS AND

Changes to Network Configurations

Overview

List of Network Connections Devices

Table 1.1.1.a

Table 1.1.1.b

Table 1.1.1.c

Responsibility for Policy Maintenance

1.1.2 REQUIREMENT

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

Overview

Network Diagram and Topology Documents

Responsibility for Policy Maintenance

1.1.4 REQUIREMENT

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

Overview

Table 1.1.4.a

Table 1.1.4.b

Responsibility for Policy Maintenance

1

1

1

1

2

3

3

4

4

5

5

6

6

6

7

–

1.1.5 REQUIREMENT

Documentation and Business Justification for Use of All Services, Protocols and Ports Allowed

Overview

Table 1.1.5.a: Network Device #1:

Table 1.1.5.b: Network Device #2:

Table 1.1.5.c: Network Device #3:

Table 1.1.5.d

Table 1.1.5.e:

Responsibility for Policy Maintenance

8

8

8

9

9

9

10

10

1.1.6 REQUIREMENT

Requirements to Review Firewall and Router Rule Sets at least Every Six (6) Months

Overview

Policy

Procedure

Table 1.1.6.a

Responsibility for Policy Maintenance

11

11

11

11

11

12

2.2 REQUIREMENT

Configuration Standards for All System Components Policy and Procedures

Overview

13

13

Policy	13
Procedure	14
Table 2.2.a	14
Responsibility for Policy Maintenance	14

3.1 REQUIREMENT

Data Retention and Disposal Policy and Procedures	15
Overview	15
Description of Data and Scope for Cardholder Environment	15
Description of Key Terms and Phrases	15
Types of Data	17
Electronic Media	17
Hardcopy Format	18
Procedure	18
Procedures for Obtaining Data	19
Procedures for Protecting Data	19
Procedures for Accessing, Modifying or Transferring Cardholder Data	19
Provisions and Procedures for Retaining Data	19
Provisions and Procedures for Disposing of and Destroying Data	20
Responsible Parties for Data Retention Activities	20
Responsible Parties for Data Disposal Activities	20
Types of Data and Retention Periods for Legal, Regulatory and Business Requirements	21
Table 3.1.a: Electronic Media Storage of Cardholder Data	21
Table 3.1.b: Hardcopy Format Storage of Cardholder Data	22
Programmatic (Automatic) Removal of Cardholder Data	22
Additional Information	23
Responsibility for Policy Maintenance	23

3.3 REQUIREMENT

Primary Account Number (PAN) Policy and Procedures for Displaying the PAN Digits

Overview	24
Policy	24
Procedure	24
Table 3.3.a	25
Responsibility for Policy Maintenance	25

3.6 REQUIREMENT

Key Management Policy and Procedures

Overview	26
Policy	26
Procedure	27
General Description of System Components that Incorporate Key Management Procedures	27
Generation of Strong Keys	27
Secure Key Storage	28
Periodic Key Changes at least Annually	29
Retirement and Destruction of Old Keys	30
Replacement of Known or Suspected Compromised Keys	30
Table 3.6.a: Key Management Compromise Plan (KMCP): Systems Components Impact	30
Table 3.6.b: Key Management Compromise Plan (KMCP): Personnel	31
Table 3.6.c: Key Management Compromise Plan (KMCP): Notification Process for External Vendor	31
Split Knowledge and dual Control of Keys	31

**Prevention of Unauthorized Substitution of Keys
Key Custodians to Sign Form Specifying that they
Understand and Accept their Key Custodian Responsibilities**

32

32

Table 3.6.d32

32

Responsibility for Policy Maintenance

33

4.2 REQUIREMENT

Unencrypted Primary Account Numbers (PAN) Policy and Procedures

34

Overview

34

Policy

34

Procedure

34

Table 4.2.a

35

Responsibility for Policy Maintenance

35

5.2 REQUIREMENT

Anti-Virus Policy and Procedures

36

Overview

36

Policy

36

Procedure

37

Table 5.2.a

37

Table 5.2.b

38

Responsibility for Policy Maintenance

38

6.1 REQUIREMENT

Security Patch Management Installation Policy and Procedures	39
Overview	39
Policy	39
Procedure	41
Security Patch Management Program Employee	41
Table 6.1.a: Security Patch Management Program Employee	41
Comprehensive Inventory of all Systems Components	
Directly Associated with the Cardholder Environment	41
Table 6.1.b	42
Comprehensive Inventory of all other I.T. Resources	
Not Directly Associated with the Cardholder Environment	42
Table 6.1.c	43
Industry-Leading Security Sources and Additional Supporting Resources	43
Table 6.1.d: Online Resources for Patch Management,	
Alerts, Security and Support, As Applicable	44
Procedures for Establishing Priorities Regarding	
Security Patch Management	44
Table 6.1.e: Security Patch Management Prioritization Table	45
Database of Remediation Activities that Need to be Applied	45
Table 6.1.f	46
Test Procedures for Testing Patches Regarding Remediation	46
Procedures for Verifying Successful Implementation of Patches and	
other Related Security-Hardening Procedures	47
Responsibility for Policy Maintenance	47

6.3 REQUIREMENT

Software Development Life Cycle Processes	48
Overview	48
Policy	48
Procedure	48
New System/Application and Feature Development	49
Request for New System/Application or Features	49
Feasibility Study	49
Estimate and HW/SW Requirements	49
Management Decision	49
Requirement Analysis	49
Design	50
Implementation	50
Quality Assurance	50
Release for Production	50
Additional Software Development Requirements for PCI DSS	50
Responsibility for Policy Maintenance	51

6.3.7.A REQUIREMENT

Custom Application Code changes for Internal Applications	
Policy and Procedures	52
Overview	52
Policy	52
Procedure	52

Table 6.3.7.a: Custom Application Code Changes for Internal Applications

53

Responsibility for Policy Maintenance

53

6.3.7.B REQUIREMENT

Custom Application Code Changes for Web Applications

Policy and Procedures

54

Overview

54

Policy

54

Procedure

54

Table 6.3.7.b: Custom Application Code Changes for Web Applications

55

Responsibility for Policy Maintenance

55

6.4 REQUIREMENT

Change Control Policy and Procedures

56

Overview

56

Policy

56

Change Control Initiation, Implementation and Authorization

56

Procedure

57

Formally Request a Change

57

Categorize and Prioritize the Change

57

Justification and Analysis of the Change

57

Approving and Scheduling the Change

58

Implementation of the Change

58

Post-Implementation Review for any Changes

58

6.5 REQUIREMENT

Software Development Processes for any Web-Based Applications Policy and Procedures

Overview

Policy

Table 6.5.a

Procedure

Table 6.5.b

Responsibility for Policy Maintenance

7.1 TO 7.2.3 REQUIREMENT

Data Control & Access Control Policy and Procedures

Overview

Policy

Procedure

Restricting Access to Fewest Privileges Necessary
for Job Functions and RBAC Measures

Primary Elements of Role-Based Access Control (RBAC)

Permissions/Operations and objects

Lastly, RBAC Rules Consist of the Following

Authorization Form

Automated Access Control System for All System Components

Table 7.a: Automated Access Controls System and RBAC Architecture

Table 7.b: Automated Access Controls System and RBAC Architecture

Table 7.c: Automated Access Controls System and RBAC Architecture	67
Table 7.d: Automated Access Controls System and RBAC Architecture	68
Table 7.e: Automated Access Controls System and RBAC Architecture	68

Responsibility for Policy Maintenance	69
--	-----------

8.1 TO 8.4 REQUIREMENT

Unique I.D. & Authentication Methods Policy and Procedures	70
Overview	70
Policy	70
Procedure	70
Assignment of Unique I.D. and Password	71
Table 8.a	71
Two-Factor Authentication	71
Table 8.b	72
Transmission and Storage of Passwords	72
Responsibility for Policy Maintenance	72

8.5 TO 8.5.15 REQUIREMENT

Proper Authentication & Password Management Policy and Procedures	73
Overview	73
Policy	73
Procedure	74
Authorization Form	74
Password Resets	75
First-Time Passwords	75
Terminated Employees	75

Inactive Accounts	75
Vendor Accounts	75
Generic User I.D.'s and Shared User I.D.'s and Passwords	76
Password Parameters	76
Familiarity and Acknowledgement of Password Policy and Procedures	76
 Responsibility for Policy Maintenance	 76

9.7 TO 9.7.2 REQUIREMENT

Media Distribution and Classification Policy and Procedures	77
Overview	77
Policy	77
Procedures	77
Definition of Media	78
Classification of Media and Information Assets	78
Table 9.7	78
Logging of Media	79
Secure Transport of Media	80
 Responsibility for Policy Maintenance	 80

9.9 REQUIREMENT

Storage and Maintenance of Hardcopy and Electronic Media Policy and Procedures	81
Overview	81
Policy	81
Procedure	81
Protection of all Hardcopy and Electronic Media	82

Storage and Inventory of Media	82
Sending, Retrieving and Receiving Media	82
Responsibility for Policy Maintenance	83

9.10 REQUIREMENT

Periodic Media Destruction Policy and Procedures	84
--	----

10.6 REQUIREMENT

Review of Security Logs Policy and Procedures	85
Overview	85
Policy	85
Procedure	85
Table 10.6	86
Responsibility for Policy Maintenance	86

10.7 REQUIREMENT

Audit Trail History & Log Retention Policy and Procedures	87
Overview	87
Policy	87
Procedure	87
Table 10.7	88
Responsibility for Policy Maintenance	88

12.1 REQUIREMENT

Information Security Policy

89

12.1.2 REQUIREMENT

Annual Formal Risk Assessment Process

90

Overview

90

Policy

90

Procedure

90

The Scope of Risk Assessment System and Technology Risks

90

Table 12.1.2

91

Business Administrative Risks

91

Business Revenue Risks

91

Operational Risks

91

92

Responsibility for Policy Maintenance

92

12.3 REQUIREMENT

Usage Policy and Procedures

93

Overview

93

Policy

94

Procedure

94

Explicit Management Approval to Use the Technologies

95

Table 12.3.a

95

Use of All Technology Resources Must be Authenticated

103

Listing and Labeling of All Devices and Personnel Authorized to Use Them

104

Table 12.3.b	104
Acceptable Use	105
General Guidelines, Responsibilities and Acceptable Use for the Technology	105
Unacceptable Use and Behavior	106
Disciplinary Action	106
Acceptable Network Locations for the Technology	107
List of Company-Approved Products	107
Table 12.3.c	107
Additional Usage Policy Requirements	108

Responsibility for Policy Maintenance	108
--	-----

12.4 TO 12.5.5 REQUIREMENT

Information Security Responsibilities	109
Overview	109
Scope	109
Policy	109
Procedure	110
Information Security Responsibilities for Employees and Contractors	110
Formal Assignment of Information Security	110
Table 12.4.a	111
Table 12.4.b: Information Security Responsibilities Matrix	111
Responsibility for Policy Maintenance	112

12.6 REQUIREMENT

Formal Security Awareness Program	113
Overview	113

Policy	113
Procedure	113
Program Phases	114
Design	114
Identify and Structure Organizational Training Needs	114
Comprehensive Assessment of Needs	115
Table 12.6.a	116
Develop Training Strategy Plan	116
Develop	117
Develop Material and Select Relevant Topics	117
Identify Source Material to be Used	118
Table 12.6.b	119
Refine Material and Develop Model for Training Employees	119
Table 12.6.c	120
Implement	121
Communicate the Plan to All Employees	121
Communicating Security Awareness to Employees	122
Delivering Training to Employees	122
Maintain/Oversight	122
Monitor Adherence to the Program	122
Collect Vital Feedback on the Program	123
Manage Changes as needed for the Program	123
Table 12.6.d	123
Core Components	124
Responsibility for Policy Maintenance	124

12.8 REQUIREMENT

Management of Service Providers Policy and Procedures	125
Overview	125
Policy	125
Procedure	125

Table 12.8: List of Service Providers

126

Responsibility for Policy Maintenance

126

12.9 REQUIREMENT

Incident Response Plan

127

Overview

127

Policy

127

Procedure

127

Preparing for an Incident

128

Table 12.9.a: Description of Incident Response Team

129

Detecting an Incident

130

Table 12.9.b

130

Responding to and Containing an Incident

131

Table 12.9.c: Response Mechanisms for All Critical System Components

131

Table 12.9.d

133

Recovery from an Incident

133

Post-Incident Activities and Awareness

134

Responsibility for Policy Maintenance

134

REFERENCE LIST

135