Instant PCI Policy
Table of Contents - Introduction

In April 2016, version 3.2 of the PCI Data Security Standard was released. The updated version contains numerous changes from previous versions, all of which are addressed in our Instant PCI Policy. Our brand-new, fully-updated policy covers all version 3.2 requirements.

What follows is the actual Table of Contents from our new Instant PCI Policy. Please note that, for brevity, the Table of Contents includes top-level section numbering only. There are numerous, more specific, sections throughout the document. Also, the actual policy does not include this introduction nor does it include the copyright header. No information within the policy identifies where it was sourced.

Since 2008, InstantSecurityPolicy.com has been happily used by thousands of companies worldwide to meet their IT Security policy needs, and we're confident you will be pleased with our policies as well. Even better, our years of PCI DSS Policy experience will ensure you are satisfied with our Instant PCI Policy.

If you have any questions, please feel free to Contact Us!

Table of Contents

Introduction **9**
- Overview 9
- Scope 9
- Goals 9
- Intent 10
- Implementation 10
- Revision History 10

I. Acceptable Use Policy **12**
- 1.0 Overview 12
- 2.0 Purpose 12
- 3.0 Scope 12
- 4.0 Policies 12
  - 4.1 Network Access 12
  - 4.2 Web Browsing and Internet Usage 13
  - 4.3 Unacceptable Use 14
  - 4.4 Monitoring and Privacy 16
  - 4.5 Responsible Computer and Network Use 17
  - 4.6 Reporting of a Security Incident 17
  - 4.7 Applicability of Other Policies 18
- 5.0 Enforcement 18

II. Password Policy **19**
- 1.0 Overview 19
- 2.0 Purpose 19
- 3.0 Scope 19
- 4.0 Policies 19
  - 4.1 Construction 19
  - 4.2 Confidentiality 20
  - 4.3 Change Frequency 20
  - 4.4 Incident Reporting 21
  - 4.5 Applicability of Other Policies 21
- 5.0 Enforcement 21

III. Remote Access Policy **22**
- 1.0 Overview 22
- 2.0 Purpose 22
- 3.0 Scope 22
- 4.0 Policies 22
  - 4.1 Remote Access Client Software 22

4.2 Remote Network Access 23
4.3 Idle Connections 24
4.4 Prohibited Actions 24
4.5 Use of non-company-provided Systems 25
4.6 Applicability of Other Policies 25
5.0 Enforcement 25
IV. Confidential Data Policy 26
1.0 Overview 26
2.0 Purpose 26
3.0 Scope 26
4.0 Policies 26
4.1 Data Classification 26
4.2 Treatment of Confidential Data 27
4.3 Examples of Confidential Data 29
4.4 Use of Confidential Data 30
4.5 Sharing Confidential Data with Third Parties 30
4.6 Receiving Confidential Data from Third Parties 31
4.7 Security Controls for Confidential Data 31
4.8 Emergency Access to Data 33
4.9 Applicability of Other Policies 34
5.0 Enforcement 34
V. Mobile Device Policy 35
1.0 Overview 35
2.0 Purpose 35
3.0 Scope 35
4.0 Policies 35
4.1 Physical Security 35
4.2 Data Security 36
4.3 Connecting Mobile Computers to Unsecured Networks 37
4.4 General Guidelines 37
4.5 Audits 38
4.6 Applicability of Other Policies 38
5.0 Enforcement 38
VI. Retention Policy 39
1.0 Overview 39
2.0 Purpose 39
3.0 Scope 39
4.0 Policies 39
4.1 Reasons for Data Retention 39
4.2 Data Duplication 40

4.3 Retention Requirements 40
4.4 Retention of Encrypted Data 41
4.5 Data Destruction 41
4.6 Applicability of Other Policies 42
5.0 Enforcement 42
VII. Email Policy 43
2.0 Purpose 43
3.0 Scope 43
4.0 Policies 43
4.1 Proper Use of Company Email Systems 43
4.2 External and/or Personal Email Accounts 47
4.3 Confidential Data and Email 48
4.4 Company Administration of Email 48
4.5 Prohibited Actions 52
4.6 Applicability of Other Policies 53
5.0 Enforcement 54
VIII. Backup Policy 55
1.0 Overview 55
2.0 Purpose 55
3.0 Scope 55
4.0 Policies 55
4.1 Identification of Critical Data 55
4.2 Data to be Backed Up 56
4.3 Backup Frequency 56
4.4 Off-Site Rotation 56
4.5 Backup Storage 57
4.6 Backup Retention 57
4.7 Restoration Procedures & Documentation 58
4.8 Restoration Testing 58
4.9 Expiration of Backup Media 58
4.10 Applicability of Other Policies 58
5.0 Enforcement 58
IX. Network Access and Authentication Policy 60
1.0 Overview 60
2.0 Purpose 60
3.0 Scope 60
4.0 Policies 60
4.1 Account Setup 60
4.2 Account Access Levels 61
4.3 Account Use 62

4.4 Account Termination 63
4.5 Network Authentication Requests 63
4.6 Database Authentication Requests 64
4.7 Use of Passwords 64
4.8 Screensaver Passwords 64
4.9 Minimum Configuration for Access 64
4.10 Encryption of Login Credentials 65
4.11 Failed Login Attempts 65
4.12 Alternate Authentication Mechanisms 65
4.13 Applicability of Other Policies 66
5.0 Enforcement 66
X. Incident Response Policy 67
1.0 Overview 67
2.0 Purpose 67
3.0 Scope 67
4.0 Policies 67
4.1 Types of Incidents 67
4.2 Preparation 68
4.3 Confidentiality 69
4.4 Electronic Incidents 69
4.5 Physical Incidents 70
4.6 Hybrid Incidents 72
4.7 Notification 73
4.8 Managing Risk 73
4.9 Business Recovery and Continuity Planning 75
4.10 Applicability of Other Policies 77
5.0 Enforcement 77
XI. External Connection Policy 78
1.0 Overview 78
2.0 Purpose 78
3.0 Scope 78
4.0 Policies 79
4.1 Encryption 79
4.2 Authentication 79
4.3 Implementation 79
4.4 Management 79
4.5 Logging and Monitoring 80
4.6 Encryption Keys 80
4.7 Managing Risk 80
4.8 Restricting Third Party Access 80

4.9 Applicability of Other Policies 81
5.0 Enforcement 81
XII. Guest Access Policy 82
1.0 Overview 82
2.0 Purpose 82
3.0 Scope 82
4.0 Policies 82
4.1 Granting Guest Access 82
4.2 Guest Access Infrastructure Requirements 84
4.3 Restrictions on Guest Access 84
4.4 Monitoring of Guest Access 84
4.5 Applicability of Other Policies 84
5.0 Enforcement 84
XIII. Wireless Access Policy 85
1.0 Overview 85
2.0 Purpose 85
3.0 Scope 85
4.0 Policies 85
4.1 Physical Guidelines 85
4.2 Configuration and Installation 86
4.3 Accessing Confidential Data 87
4.4 Inactivity 87
4.5 Wireless Scans 88
4.6 Audits 88
4.7 Wireless Access Point Inventory 88
4.8 Applicability of Other Policies 89
5.0 Enforcement 89
XIV. Network Security Policy 90
1.0 Overview 90
2.0 Purpose 90
3.0 Scope 90
4.0 Policies 90
4.1 Network Device Authentication 90
4.2 Logging 93
4.3 Audit Trails 94
4.4 Firewalls 96
4.5 Networking Hardware 98
4.6 Network Servers 99
4.7 Intrusion Detection/Intrusion Prevention 101
4.8 File Integrity Monitoring 101

4.9 Security Control Monitoring 101
4.10 Security Testing 102
4.11 Disposal of Information Technology Assets 105
4.12 Network Compartmentalization 106
4.13 Network Documentation 107
4.14 Antivirus/Anti-Malware 108
4.15 Software Use Policy 109
4.16 Software/Application Development Policy 110
4.17 Maintenance Windows and Scheduled Downtime 112
4.18 Change Management 112
4.19 Suspected Security Incidents 113
4.20 Redundancy 113
4.21 Manufacturer Support Contracts 113
4.22 Security Policy Management 114
4.23 Applicability of Other Policies 116
5.0 Enforcement 116
XV. Encryption Policy 117
1.0 Overview 117
2.0 Purpose 117
3.0 Scope 117
4.0 Policies 117
4.1 Applicability of Encryption 117
4.2 Encryption Key Management 119
4.3 Acceptable Encryption Algorithms 121
4.4 Legal Use 121
4.5 Applicability of Other Policies 121
5.0 Enforcement 121
XVI. Outsourcing Policy 122
1.0 Overview 122
2.0 Purpose 122
3.0 Scope 122
4.0 Policies 122
4.1 Deciding to Outsource 122
4.2 Outsourcing Core Functions 123
4.3 Evaluating a Provider 123
4.4 Security Controls 124
4.5 Outsourcing Contracts 124
4.6 Access to Information 124
4.7 List of Providers 124
4.8 Applicability of Other Policies 125

5.0 Enforcement 125
XVII. Physical Security Policy 126
1.0 Overview 126
2.0 Purpose 126
3.0 Scope 126
4.0 Policies 126
4.1 Choosing a Site 126
4.2 Security Zones 127
4.3 Access Controls 128
4.4 Physical Data Security 129
4.5 Physical System Security 130
4.6 Fire Prevention 132
4.7 Entry Security 132
4.8 Applicability of Other Policies 134
5.0 Enforcement 134
Appendix A: Policy Acceptance Form 135
Appendix B: Definitions 136