

Instant PCI Policy

Table of Contents - Introduction

On January 1, 2014, version 3.0 of the PCI Data Security Standard went into effect. The new standard contains numerous changes from version 2.0, all of which are addressed in our Instant PCI Policy. Our brand-new, fully-updated policy covers all version 3.0 requirements.

What follows is the actual Table of Contents from our new Instant PCI Policy. Please note that, for brevity, the Table of Contents only includes top-level section numbering only. There are numerous, more specific, sections throughout the document.

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	11
1.0 Overview	11
2.0 Purpose	11
3.0 Scope.....	11
4.0 Policies	11
4.1 Network Access.....	11
4.2 Web Browsing and Internet Usage.....	12
4.3 Unacceptable Use	13
4.4 Monitoring and Privacy.....	15
4.5 Responsible Computer and Network Use.....	16
4.6 Reporting of a Security Incident	16
4.7 Applicability of Other Policies.....	17
5.0 Enforcement	17
II. Password Policy.....	18
1.0 Overview	18
2.0 Purpose	18
3.0 Scope.....	18
4.0 Policies	18
4.1 Construction.....	18
4.2 Confidentiality.....	19
4.3 Change Frequency	19
4.4 Incident Reporting	20
4.5 Applicability of Other Policies.....	20
5.0 Enforcement	20
III. Remote Access Policy	21
1.0 Overview	21
2.0 Purpose	21
3.0 Scope.....	21
4.0 Policies	21
4.1 Remote Access Client Software	21

4.2 Remote Network Access	22
4.3 Idle Connections	23
4.4 Prohibited Actions.....	23
4.5 Use of non-company-provided Systems.....	23
4.6 Applicability of Other Policies	24
5.0 Enforcement	24
IV. Confidential Data Policy	25
1.0 Overview	25
2.0 Purpose	25
3.0 Scope.....	25
4.0 Policies	25
4.1 Data Classification.....	25
4.2 Treatment of Confidential Data.....	26
4.3 Examples of Confidential Data.....	28
4.4 Use of Confidential Data.....	29
4.5 Sharing Confidential Data with Third Parties.....	29
4.6 Receiving Confidential Data from Third Parties.....	30
4.7 Security Controls for Confidential Data	30
4.8 Emergency Access to Data	32
4.9 Applicability of Other Policies.....	33
5.0 Enforcement	33
V. Mobile Device Policy	34
1.0 Overview	34
2.0 Purpose	34
3.0 Scope.....	34
4.0 Policies	34
4.1 Physical Security.....	34
4.2 Data Security.....	35
4.3 Connecting Mobile Computers to Unsecured Networks.....	36
4.4 General Guidelines.....	36
4.5 Audits	37
4.6 Applicability of Other Policies.....	37
5.0 Enforcement	37
VI. Retention Policy	38
1.0 Overview	38
2.0 Purpose	38
3.0 Scope.....	38
4.0 Policies	38
4.1 Reasons for Data Retention	38
4.2 Data Duplication	39

4.3 Retention Requirements.....	39
4.4 Retention of Encrypted Data	40
4.5 Data Destruction	40
4.6 Applicability of Other Policies.....	41
5.0 Enforcement	41
VII. Email Policy	42
2.0 Purpose	42
3.0 Scope.....	42
4.0 Policies	42
4.1 Proper Use of Company Email Systems.....	42
4.2 External and/or Personal Email Accounts.....	46
4.3 Confidential Data and Email	47
4.4 Company Administration of Email	47
4.5 Prohibited Actions.....	51
4.6 Applicability of Other Policies.....	52
5.0 Enforcement	53
VIII. Backup Policy	54
1.0 Overview	54
2.0 Purpose	54
3.0 Scope.....	54
4.0 Policies	54
4.1 Identification of Critical Data	54
4.2 Data to be Backed Up	55
4.3 Backup Frequency.....	55
4.4 Off-Site Rotation	55
4.5 Backup Storage	56
4.6 Backup Retention.....	56
4.7 Restoration Procedures & Documentation	57
4.8 Restoration Testing.....	57
4.9 Expiration of Backup Media.....	57
4.10 Applicability of Other Policies.....	57
5.0 Enforcement	57
IX. Network Access and Authentication Policy	59
1.0 Overview	59
2.0 Purpose	59
3.0 Scope.....	59
4.0 Policies	59
4.1 Account Setup.....	59
4.2 Account Access Levels.....	60
4.3 Account Use	61

4.4 Account Termination	62
4.5 Network Authentication Requests.....	62
4.6 Database Authentication Requests	63
4.7 Use of Passwords	63
4.8 Screensaver Passwords.....	63
4.9 Minimum Configuration for Access	63
4.10 Encryption of Login Credentials	64
4.11 Failed Login Attempts	64
4.12 Alternate Authentication Mechanisms.....	64
4.13 Applicability of Other Policies.....	65
5.0 Enforcement	65
X. Incident Response Policy	66
1.0 Overview	66
2.0 Purpose	66
3.0 Scope.....	66
4.0 Policies	66
4.1 Types of Incidents	66
4.2 Preparation	67
4.3 Confidentiality.....	68
4.4 Electronic Incidents.....	68
4.5 Physical Incidents.....	69
4.6 Hybrid Incidents	71
4.7 Notification	72
4.8 Managing Risk.....	72
4.9 Business Recovery and Continuity Planning.....	74
4.10 Applicability of Other Policies.....	76
5.0 Enforcement	76
XI. External Connection Policy	77
1.0 Overview	77
2.0 Purpose	77
3.0 Scope.....	77
4.0 Policies	78
4.1 Encryption	78
4.2 Authentication	78
4.3 Implementation	78
4.4 Management.....	78
4.5 Logging and Monitoring.....	79
4.6 Encryption Keys.....	79
4.7 Managing Risk.....	79
4.8 Restricting Third Party Access.....	79

4.9 Applicability of Other Policies	80
5.0 Enforcement	80
XII. Guest Access Policy.....	81
1.0 Overview	81
2.0 Purpose	81
3.0 Scope.....	81
4.0 Policies	81
4.1 Granting Guest Access	81
4.2 Guest Access Infrastructure Requirements	83
4.3 Restrictions on Guest Access	83
4.4 Monitoring of Guest Access	83
4.5 Applicability of Other Policies.....	83
5.0 Enforcement	83
XIII. Wireless Access Policy	84
1.0 Overview	84
2.0 Purpose	84
3.0 Scope.....	84
4.0 Policies	84
4.1 Physical Guidelines.....	84
4.2 Configuration and Installation	85
4.3 Accessing Confidential Data.....	86
4.4 Inactivity.....	86
4.5 Wireless Scans.....	87
4.6 Audits	87
4.7 Wireless Access Point Inventory	87
4.8 Applicability of Other Policies	88
5.0 Enforcement	88
XIV. Network Security Policy.....	89
1.0 Overview	89
2.0 Purpose	89
3.0 Scope.....	89
4.0 Policies	89
4.1 Network Device Authentication	89
4.2 Logging	92
4.3 Audit Trails	93
4.4 Firewalls	95
4.5 Networking Hardware.....	97
4.6 Network Servers.....	98
4.7 Intrusion Detection/Intrusion Prevention	100
4.8 File Integrity Monitoring.....	100

4.9 Security Testing.....	100
4.10 Disposal of Information Technology Assets.....	103
4.11 Network Compartmentalization.....	104
4.12 Network Documentation.....	105
4.13 Antivirus/Anti-Malware.....	106
4.14 Software Use Policy.....	107
4.15 Software/Application Development Policy.....	108
4.16 Maintenance Windows and Scheduled Downtime.....	109
4.17 Change Management.....	110
4.18 Suspected Security Incidents.....	110
4.19 Redundancy.....	110
4.20 Manufacturer Support Contracts.....	111
4.21 Security Policy Management.....	111
4.22 Applicability of Other Policies.....	113
5.0 Enforcement.....	113
XV. Encryption Policy.....	114
1.0 Overview.....	114
2.0 Purpose.....	114
3.0 Scope.....	114
4.0 Policies.....	114
4.1 Applicability of Encryption.....	114
4.2 Encryption Key Management.....	116
4.3 Acceptable Encryption Algorithms.....	117
4.4 Legal Use.....	118
4.5 Applicability of Other Policies.....	118
5.0 Enforcement.....	118
XVI. Outsourcing Policy.....	119
1.0 Overview.....	119
2.0 Purpose.....	119
3.0 Scope.....	119
4.0 Policies.....	119
4.1 Deciding to Outsource.....	119
4.2 Outsourcing Core Functions.....	120
4.3 Evaluating a Provider.....	120
4.4 Security Controls.....	120
4.5 Outsourcing Contracts.....	121
4.6 Access to Information.....	121
4.7 List of Providers.....	121
4.8 Applicability of Other Policies.....	122
5.0 Enforcement.....	122

XVII. Physical Security Policy.....	123
1.0 Overview	123
2.0 Purpose	123
3.0 Scope.....	123
4.0 Policies	123
4.1 Choosing a Site.....	123
4.2 Security Zones.....	124
4.3 Access Controls	125
4.4 Physical Data Security	126
4.5 Physical System Security.....	127
4.6 Fire Prevention.....	129
4.7 Entry Security.....	129
4.8 Applicability of Other Policies.....	131
5.0 Enforcement	131
Appendix A: Policy Acceptance Form	132
Appendix B: Definitions	133