



IT Policy Template for any company aiming to reach PCI DSS certification or that already has the certification, but wants to revise, update or improve their current IT policy!

For an editable copy, please contact 24 Solutions at: info@24solutions.com

2017

Table of Contents

0.	Revision History.....	0
1	INTRODUCTION AND SCOPE	1
1.1	Introduction	1
1.2	Regulatory Compliance.....	1
1.3	Scope of Compliance	1
2	POLICY ROLES AND RESPONSIBILITIES.....	2
2.1	Policy Applicability	2
2.2	Role of Chief Technical Officer	2
2.3	Information Security Team.....	3
2.4	System Administrators	4
2.5	Users.....	5
2.6	Role Assignment	5
3	IT CHANGE CONTROL POLICY.....	5
3.1	Policy Applicability	5
3.2	Change Request Submittal.....	6
3.3	Change Request Approval.....	6
3.4	Change Testing.....	6
3.5	Change Implementation	7
4	DATA CLASSIFICATION AND CONTROL POLICY	7
4.1	Policy Applicability	7
4.2	Data Classification	7
4.2.1	Introduction	7
4.2.2	%Company% Internal Information Categories	7
4.3	Data Access.....	8
4.3.1	Data Access Request Process	9
4.4	Physical Security	9
4.5	User Authentication	10
4.5.1	Users.....	10
4.5.2	Systems.....	10
4.6	Account and Access Management	11
4.6.1	Information Security Team Responsibilities.....	11
4.6.2	System Administrator Responsibilities	12
5	DATA RETENTION AND DISPOSAL POLICY.....	13
5.1	Policy Applicability	13
5.2	Retention Requirements.....	14

5.2.1	Sample Data Types and Data Retention.....	14
5.3	Disposal Requirements.....	15
5.4	Disposal Process.....	15
6	PAPER AND ELECTRONIC MEDIA POLICIES	16
6.1	Policy Applicability	16
6.2	Storage.....	16
6.2.1	Physical Security	16
6.2.2	Hardcopy Media.....	16
6.2.3	Electronic Media	17
6.3	Inventory	17
6.4	Destruction.....	18
7	FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY	18
7.1	Policy Applicability	18
7.2	Device Management Responsibilities.....	18
7.2.1	System Administrator	18
7.2.2	Network Operations Center	19
7.2.3	Information Security Team.....	19
7.3	Firewall and Router Configuration Changes.....	19
7.4	Allowed Services	20
7.5	Allowed Network Connection Paths and Configuration Requirements	20
7.6	Configuration Review	21
7.7	Personal Firewalls	21
8	SYSTEM CONFIGURATION POLICY	22
8.1	Policy Applicability	22
8.2	System Build and Deployment	22
8.2.1	System Purpose.....	22
8.2.2	System Configuration Standards.....	22
8.2.3	System Configuration Records	23
8.2.4	System Configuration Process	23
8.2.5	Standard Software.....	23
8.2.6	Network Time Protocol (NTP).....	24
8.2.7	Credit Card Information Processing Application.....	24
8.2.8	Credit Card Storage Applications	25
8.2.9	Change Detection	25
8.3	Vulnerability Identification and System Updates.....	26
8.3.1	Vulnerability Identification	26
8.3.2	Vulnerability Testing.....	27
8.3.3	Security Patch Deployment	28

9	ANTI-VIRUS POLICY.....	28
9.1	Software Configuration.....	28
9.2	Signature Updates.....	29
9.3	Software Logging	29
9.4	Systems not commonly affected by malware	29
10	BACKUP POLICY.....	29
10.1	Location.....	29
10.2	Transport.....	30
10.3	Audit.....	30
10.4	Media Destruction	30
11	ENCRYPTION POLICY	30
11.1	Policy Applicability	30
11.2	Encryption Key Management	31
11.2.1	Key Access	31
11.2.2	Split Knowledge and Dual Control	31
11.2.3	Key Generation.....	31
11.2.4	Key Distribution.....	32
11.2.5	Key Storage.....	32
11.2.6	Key Changes and Destruction.....	32
11.3	Transmission over Un-Trusted Networks.....	33
11.3.1	Email Transmission of Confidential Information.....	33
11.3.2	Encryption of Wireless Networks	34
11.4	Non-console and Remote Administrative Access	34
12	CRITICAL TECHNOLOGIES USAGE POLICY.....	34
12.1	Policy Applicability	34
12.2	Approval	34
12.3	Authentication.....	35
12.4	Device Inventory	35
12.5	Device Identification.....	35
12.6	Acceptable Use	36
12.7	Permitted Locations.....	36
12.8	Approved Products.....	36
12.9	Session Disconnect.....	36
12.10	Vendor Connections.....	36
12.11	Credit Card Data Access.....	37
13	SOFTWARE DEVELOPMENT POLICY.....	37
13.1	Development Environment	37

13.2	Secure Software Development Procedures.....	38
13.2.1	Development Life-Cycle.....	38
13.2.2	Web-based Applications	39
13.2.3	Credit Card Informational and Processing Applications	40
14	INCIDENT RESPONSE PLAN AND PROCEDURES	40
14.1	Incident Identification	40
14.2	Reporting and Incident Declaration Procedures	41
14.3	Incident Severity Classification	42
14.4	Incident Response.....	42
14.4.1	Typical Response.....	42
14.4.1.1	Level 1.....	42
14.4.1.2	Level 2	42
14.4.1.3	Level 3	43
14.4.2	Credit Card Compromise – Special Response.....	43
14.4.3	Root Cause Analysis and Lessons Learned	44
14.5	Plan Testing and Training.....	45
14.6	Automated Security System Notifications.....	45
15	IDENTIFICATION AND PHYSICAL AUTHENTICATION POLICY	45
15.1	Employee and Visitor Requirements.....	45
15.2	Other Authentication Mechanisms Usage.....	46
16	LOGGING CONTROLS POLICY.....	47
16.1	Events Logged	47
16.2	Event Log Structure	47
16.3	Log Security.....	47
17	PROTECTION OF CARD-READING DEVICES AT POINT OF SALE	48
17.1	Training of Sales Clerks	48
17.2	Periodic Inspections of Card-Reading Devices	49
18	RISK-ASSESSMENT PROCESS	49
19	ADDITIONAL PCI DSS SERVICE PROVIDER RESPONSIBILITIES.....	49
19.1	Written Acknowledgment of Responsibility from the Entity	49
19.2	Remote Access to Customers	50
20	SERVICE PROVIDER MANAGEMENT.....	50
20.1	Responsibility Allocation and Compliance Monitoring	50
20.2	Written Acknowledgment of Responsibility from the Service Provider.....	50
20.3	Service Provider and Entity Engagement and Compliance Monitoring.....	51
21	Inventory of system components.....	51

22	Appendix A – Security Awareness and Acceptable Use Policy	52
23	Appendix B – Authorization Request Form	56
24	Appendix C – Change Request Form	57
25	Appendix D – Media Inventory Log	58
26	Appendix E – Permitted Network Services and Protocols	59
27	Appendix F – System Configuration Standards	60
F.1	Windows Systems	60
F.1.1	Windows Installation	60
F.1.2	Windows 2000 Server	60
F.1.3	Windows 2000 Professional.....	60
F.1.4	Windows NT.....	61
F.1.5	Windows 2003 Server Domain Controller.....	61
F.1.6	Windows 2003 Server Member Server	61
F.1.7	Windows XP Professional.....	61
F.2	UNIX Systems	61
F.2.1	UNIX Installation	61
F.2.2	HP-UX.....	62
F.2.3	Linux.....	62
F.2.4	FreeBSD	62
F.2.5	Solaris.....	62
F.3	Network Devices	63
F.3.1	Network Device Installation	63
F.3.2	Cisco IOS	63
F.3.3	Cisco PIX Firewall.....	63
F.3.4	Wireless Access Point.....	63
F.4	Server Applications	64
F.4.1	Application Installation	64
F.4.2	Oracle Database	64
F.4.3	Apache Web Server	64
28	Appendix G – System Configuration Record	65
29	Appendix H – Backup Media Transfer Log	66
30	Appendix I – Encryption Key Custodianship Form	67
31	Appendix J – Encryption Key Management Log	68
32	Appendix K – Critical Technologies Device Inventory	69
33	Appendix L – Periodic Operational Security Procedures	71

34	Appendix M – NEW EMPLOYEE CARD	72
35	Appendix N – Inventory of System Components.....	73
36	Appendix O – List of Card-Reading Devices at POS.....	74
37	Appendix P – List of Service Providers	74
38	Appendix Q1 – Role Assignment List	75
39	Appendix Q2 – Role Specification List	76
40	Appendix Q3 – Role Specification for PAN Visibility	76

o. Revision History

Changes	By	Date
1.5 – ...		
1.6 – Updated in preparation for PCI DSS Audit		
1.7 – Updates following PCI DSS Audit		
1.8 – Additional further updates		
1.9 – Minor updates to make policy wording more appropriate		
2.0 –		

1 INTRODUCTION AND SCOPE

1.1 Introduction

This document explains %Company%'s information security requirements for all employees. %Company%'s management has committed to these policies to protect information utilized by %Company% in attaining its business goals. All employees are required to adhere to the policies described within this document.

1.2 Regulatory Compliance

The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding credit cardholder information for all credit card brands.

In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 1.1 of the PCI standard.

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, and retail POS systems that process credit cards over the internet.

During normal course of compliance and reporting activities %Company% will ensure that proper scoping of compliant PCI operations and reporting are in effect.

1.3 Scope of Compliance

This Information Security Policy applies to all “system components.” System components are defined as any network component, server, or application that is included in or connected to the company’s information environment. The company information environment is that part of the network that possesses company information. For example, the following types of systems would be in scope for compliance within any environment:

- Systems storing company information (e.g. databases, PC’s used by accounting for generating reports)
- Systems processing company information (e.g. web servers, application servers, etc.)
- Network devices transporting or directing company information traffic (e.g. border router, DMZ firewall, intranet firewall, etc.)

- Devices that create media containing company information (e.g. fax machine, printer, backup tape silo)
- Support systems (e.g. Active Directory, PC's performing support functions such as system administration, etc.)

2 POLICY ROLES AND RESPONSIBILITIES

2.1 Policy Applicability

All employees, contractors, vendors and third-parties that use, maintain or handle %Company% information assets must follow this policy.

2.2 Role of Chief Technical Officer

The Chief Technical Officer is responsible for coordinating and overseeing %Company%'s compliance with policies and procedures regarding the confidentiality, integrity and security of its information assets.

The Chief Technical Officer will work closely with the other %Company% managers and staff involved in securing the company's information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed. Specific responsibilities of the Chief Technical Officer include:

- Make high-level decisions pertaining to the information security policies and their content. Approve exceptions to these policies in advance on a case-by-case basis.
- On an annual basis, coordinate a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- At least annually review the Information Security policies and procedures to maintain adequacy in light of emergent business requirements or security threats.
- Make sure that third parties, with whom company information is shared, are contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the company information which they process.
- Assure that connections to third parties are managed per PCI requirements via the relationship procedures described in Management of Connected Entities (Appendix O)
- Complete tasks as required by the Periodic Operational Security Procedures (Appendix N).
- Disseminating %Company% information security policies and acceptable use guidance, and other user policies to all relevant system users, including vendors, contractors and business partners.
- Ensure background checks are carried out on potential employees who will have access to systems, networks, or data, for example background, pre-employment, criminal, or reference checks.
- Work with the Information Security Team on disseminating security awareness information to system users.
- Work with the Information Security Team to administer sanctions and disciplinary action relative to violations of Information Security Policy.

- Notify Access Management personnel when any employee is terminated Maintain all Security Awareness and Acceptable Use (Appendix A) and Authorization Request Forms (Appendix B) in employee files.

PCI Requirements Reference:

2.6 Hosting providers must protect each entity’s hosted environment and data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers*.

12.1.1 Review the security policy at least annually and update the policy when the environment changes.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

Audit Procedure 12.5 Examine information security policies and procedures to verify:

- The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management.
- The following information security responsibilities are specifically and formally assigned:

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 Maintain a list of service providers including a description of the service provided.

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

12.8.4 Maintain a program to monitor service providers’ PCI DSS compliance status at least annually

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

8.1.3 Immediately revoke access for any terminated users

Audit Procedure 12.5.1 Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned.

12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions).

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)

2.3 Information Security Team

Successfully securing %Company% information systems requires that the various individuals and groups consistently adhere to a shared vision for security. The Information Security Team works with system managers, administrators and users to develop security policies, standards and procedures to help protect the assets of %Company%.

The Information Security Team is dedicated to security planning, education and awareness. Specific responsibilities of the Information Security Team:

- Create new information security policies and procedures when needs arise. Maintain and update existing information security policies and procedures. Review the policy on an annual basis and assist management with the approval process.
- Act as a central coordinating department for implementation of the Information Security Policies.

- Maintain and distribute incident response and escalation procedures.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.
- Review logs daily. Follow up on any exceptions identified.
- Restrict and monitor access to sensitive areas. Ensure appropriate physical controls are in place where sensitive cardholder information is present.
- Complete tasks as required by the Periodic Operational Security Procedures (Appendix L).

PCI Requirements Reference:

12.1 Establish, publish, maintain, and disseminate a security policy.

12.1.1 Review the security policy at least annually and update the policy when the environment changes

12.5 Assign to an individual or team the following information security management responsibilities:

12.5.1 Establish, document, and distribute security policies and procedures

12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.

12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

12.5.5 Monitor and control all access to data.

10.6.1 Review the following at least daily:

- o All security events
- o Logs of all system components that store, process, or transmit CHD and/or SAD
- o Logs of all critical system components
- o Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

2.4 System Administrators

%Company% System Administrators are the direct link between information security policies and the network, systems and data. System Administrator responsibilities include:

- Applying %Company% information security policies and procedures as applicable to all information assets.
- Administering user account and authentication management.
- Assisting the Information Security Team with monitoring and controlling all access to %Company% data.
- Maintain an up to date network diagram including wireless networks.
- Restrict physical access to publicly accessible network jacks, wireless access points, gateways and hand held devices.
- Completing tasks as required by the Periodic Operational Security Procedures (Appendix L).

PCI Requirements Reference:

1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

12.5.4 Administer user accounts, including additions, deletions, and modifications.

12.5.5 Monitor and control all access to data

9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.