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

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:
  - All security events
  - Logs of all system components that store, process, or transmit CHD and/or SAD
  - Logs of all critical system components
  - 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.