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!

2017

***Table of Contents***

[**0. Revision History 0**](#_heading=h.gjdgxs)

[**1**](#_heading=h.30j0zll) **INTRODUCTION AND SCOPE 1**

[1.1](#_heading=h.1fob9te) Introduction 1

[1.2](#_heading=h.3znysh7) Regulatory Compliance 1

[1.3](#_heading=h.2et92p0) Scope of Compliance 1

[**2**](#_heading=h.tyjcwt) **POLICY ROLES AND RESPONSIBILITIES 2**

[2.1](#_heading=h.3dy6vkm) Policy Applicability 2

[2.2](#_heading=h.1t3h5sf) Role of Chief Technical Officer 2

[2.3](#_heading=h.4d34og8) Information Security Team 3

[2.4](#_heading=h.2s8eyo1) System Administrators 4

[2.5](#_heading=h.17dp8vu) Users 5

[2.6](#_heading=h.3rdcrjn) Role Assignment 5

[**3**](#_heading=h.26in1rg) **IT CHANGE CONTROL POLICY 5**

[3.1](#_heading=h.lnxbz9) Policy Applicability 5

[3.2](#_heading=h.35nkun2) Change Request Submittal 6

[3.3](#_heading=h.1ksv4uv) Change Request Approval 6

[3.4](#_heading=h.44sinio) Change Testing 6

[3.5](#_heading=h.2jxsxqh) Change Implementation 7

[**4**](#_heading=h.z337ya) **DATA CLASSIFICATION AND CONTROL POLICY 7**

[4.1](#_heading=h.3j2qqm3) Policy Applicability 7

[4.2](#_heading=h.1y810tw) Data Classification 7

[4.2.1](#_heading=h.4i7ojhp) Introduction 7

[4.2.2](#_heading=h.2xcytpi) %Company% Internal Information Categories 7

[4.3](#_heading=h.1ci93xb) Data Access 8

[4.3.1](#_heading=h.3whwml4) Data Access Request Process 9

[4.4](#_heading=h.2bn6wsx) Physical Security 9

[4.5](#_heading=h.qsh70q) User Authentication 10

[4.5.1](#_heading=h.3as4poj) Users 10

[4.5.2](#_heading=h.1pxezwc) Systems 10

[4.6](#_heading=h.49x2ik5) Account and Access Management 11

[4.6.1](#_heading=h.2p2csry) Information Security Team Responsibilities 11

[4.6.2](#_heading=h.147n2zr) System Administrator Responsibilities 12

[**5**](#_heading=h.3o7alnk) **DATA RETENTION AND DISPOSAL POLICY 13**

[5.1](#_heading=h.23ckvvd) Policy Applicability 13

[5.2](#_heading=h.ihv636) Retention Requirements 14

[5.2.1](#_heading=h.32hioqz) Sample Data Types and Data Retention 14

[5.3](#_heading=h.1hmsyys) Disposal Requirements 15

[5.4](#_heading=h.41mghml) Disposal Process 15

[**6**](#_heading=h.2grqrue) **PAPER AND ELECTRONIC MEDIA POLICIES 16**

[6.1](#_heading=h.vx1227) Policy Applicability 16

[6.2](#_heading=h.3fwokq0) Storage 16

[6.2.1](#_heading=h.1v1yuxt) Physical Security 16

[6.2.2](#_heading=h.4f1mdlm) Hardcopy Media 16

[6.2.3](#_heading=h.2u6wntf) Electronic Media 17

[6.3](#_heading=h.19c6y18) Inventory 17

[6.4](#_heading=h.3tbugp1) Destruction 18

[**7**](#_heading=h.28h4qwu) **FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY 18**

[7.1](#_heading=h.nmf14n) Policy Applicability 18

[7.2](#_heading=h.37m2jsg) Device Management Responsibilities 18

[7.2.1](#_heading=h.1mrcu09) System Administrator 18

[7.2.2](#_heading=h.46r0co2) Network Operations Center 19

[7.2.3](#_heading=h.2lwamvv) Information Security Team 19

[7.3](#_heading=h.111kx3o) Firewall and Router Configuration Changes 19

[7.4](#_heading=h.3l18frh) Allowed Services 20

[7.5](#_heading=h.206ipza) Allowed Network Connection Paths and Configuration Requirements 20

[7.6](#_heading=h.4k668n3) Configuration Review 21

[7.7](#_heading=h.2zbgiuw) Personal Firewalls 21

[**8**](#_heading=h.1egqt2p) **SYSTEM CONFIGURATION POLICY 22**

[8.1](#_heading=h.3ygebqi) Policy Applicability 22

[8.2](#_heading=h.2dlolyb) System Build and Deployment 22

[8.2.1](#_heading=h.sqyw64) System Purpose 22

[8.2.2](#_heading=h.3cqmetx) System Configuration Standards 22

[8.2.3](#_heading=h.1rvwp1q) System Configuration Records 23

[8.2.4](#_heading=h.4bvk7pj) System Configuration Process 23

[8.2.5](#_heading=h.2r0uhxc) Standard Software 23

[8.2.6](#_heading=h.1664s55) Network Time Protocol (NTP) 24

[8.2.7](#_heading=h.3q5sasy) Credit Card Information Processing Application 24

[8.2.8](#_heading=h.25b2l0r) Credit Card Storage Applications 25

[8.2.9](#_heading=h.kgcv8k) Change Detection 25

[8.3](#_heading=h.34g0dwd) Vulnerability Identification and System Updates 26

[8.3.1](#_heading=h.1jlao46) Vulnerability Identification 26

[8.3.2](#_heading=h.43ky6rz) Vulnerability Testing 27

[8.3.3](#_heading=h.2iq8gzs) Security Patch Deployment 28

[**9**](#_heading=h.xvir7l) **ANTI-VIRUS POLICY 28**

[9.1](#_heading=h.3hv69ve) Software Configuration 28

[9.2](#_heading=h.1x0gk37) Signature Updates 29

[9.3](#_heading=h.4h042r0) Software Logging 29

[9.4](#_heading=h.2w5ecyt) Systems not commonly affected by malware 29

[**10**](#_heading=h.1baon6m) **BACKUP POLICY 29**

[10.1](#_heading=h.3vac5uf) Location 29

[10.2](#_heading=h.2afmg28) Transport 30

[10.3](#_heading=h.pkwqa1) Audit 30

[10.4](#_heading=h.39kk8xu) Media Destruction 30

[**11**](#_heading=h.1opuj5n) **ENCRYPTION POLICY 30**

[11.1](#_heading=h.48pi1tg) Policy Applicability 30

[11.2](#_heading=h.2nusc19) Encryption Key Management 31

[11.2.1](#_heading=h.1302m92) Key Access 31

[11.2.2](#_heading=h.3mzq4wv) Split Knowledge and Dual Control 31

[11.2.3](#_heading=h.2250f4o) Key Generation 31

[11.2.4](#_heading=h.haapch) Key Distribution 32

[11.2.5](#_heading=h.319y80a) Key Storage 32

[11.2.6](#_heading=h.1gf8i83) Key Changes and Destruction 32

[11.3](#_heading=h.40ew0vw) Transmission over Un-Trusted Networks 33

[11.3.1](#_heading=h.2fk6b3p) Email Transmission of Confidential Information 33

[11.3.2](#_heading=h.upglbi) Encryption of Wireless Networks 34

[11.4](#_heading=h.3ep43zb) Non-console and Remote Administrative Access 34

[**12**](#_heading=h.1tuee74) **CRITICAL TECHNOLOGIES USAGE POLICY 34**

[12.1](#_heading=h.4du1wux) Policy Applicability 34

[12.2](#_heading=h.2szc72q) Approval 34

[12.3](#_heading=h.184mhaj) Authentication 35

[12.4](#_heading=h.3s49zyc) Device Inventory 35

[12.5](#_heading=h.279ka65) Device Identification 35

[12.6](#_heading=h.meukdy) Acceptable Use 36

[12.7](#_heading=h.36ei31r) Permitted Locations 36

[12.8](#_heading=h.1ljsd9k) Approved Products 36

[12.9](#_heading=h.45jfvxd) Session Disconnect 36

[12.10](#_heading=h.2koq656) Vendor Connections 36

[12.11](#_heading=h.zu0gcz) Credit Card Data Access 37

[**13**](#_heading=h.3jtnz0s) **SOFTWARE DEVELOPMENT POLICY 37**

[13.1](#_heading=h.1yyy98l) Development Environment 37

[13.2](#_heading=h.4iylrwe) Secure Software Development Procedures 38

[13.2.1](#_heading=h.2y3w247) Development Life-Cycle 38

[13.2.2](#_heading=h.1d96cc0) Web-based Applications 39

[13.2.3](#_heading=h.3x8tuzt) Credit Card Informational and Processing Applications 40

[**14**](#_heading=h.2ce457m) **INCIDENT RESPONSE PLAN AND PROCEDURES 40**

[14.1](#_heading=h.rjefff) Incident Identification 40

[14.2](#_heading=h.3bj1y38) Reporting and Incident Declaration Procedures 41

[14.3](#_heading=h.1qoc8b1) Incident Severity Classification 42

[14.4](#_heading=h.4anzqyu) Incident Response 42

[14.4.1](#_heading=h.2pta16n) Typical Response 42

[14.4.1.1](#_heading=h.14ykbeg) Level 1 42

[14.4.1.2](#_heading=h.3oy7u29) Level 2 42

[14.4.1.3](#_heading=h.243i4a2) Level 3 43

[14.4.2](#_heading=h.j8sehv) Credit Card Compromise – Special Response 43

[14.4.3](#_heading=h.338fx5o) Root Cause Analysis and Lessons Learned 44

[14.5](#_heading=h.1idq7dh) Plan Testing and Training 45

[14.6](#_heading=h.42ddq1a) Automated Security System Notifications 45

[**15**](#_heading=h.2hio093) **IDENTIFICATION AND PHYSICAL AUTHENTICATION POLICY 45**

[15.1](#_heading=h.wnyagw) Employee and Visitor Requirements 45

[15.2](#_heading=h.3gnlt4p) Other Authentication Mechanisms Usage 46

[**16**](#_heading=h.1vsw3ci) **LOGGING CONTROLS POLICY 47**

[16.1](#_heading=h.4fsjm0b) Events Logged 47

[16.2](#_heading=h.2uxtw84) Event Log Structure 47

[16.3](#_heading=h.1a346fx) Log Security 47

[**17**](#_heading=h.3u2rp3q) **PROTECTION OF CARD-READING DEVICES AT POINT OF SALE 48**

[17.1](#_heading=h.2981zbj) Training of Sales Clerks 48

[17.2](#_heading=h.odc9jc) Periodic Inspections of Card-Reading Devices 49

[**18**](#_heading=h.38czs75) **RISK-ASSESSMENT PROCESS 49**

[**19**](#_heading=h.1nia2ey) **ADDITIONAL PCI DSS SERVICE PROVIDER RESPONSIBILITIES 49**

[19.1](#_heading=h.47hxl2r) Written Acknowledgment of Responsibility from the Entity 49

[19.2](#_heading=h.2mn7vak) Remote Access to Customers 50

[**20**](#_heading=h.11si5id) **SERVICE PROVIDER MANAGEMENT 50**

[20.1](#_heading=h.3ls5o66) Responsibility Allocation and Compliance Monitoring 50

[20.2](#_heading=h.20xfydz) Written Acknowledgment of Responsibility from the Service Provider 50

[20.3](#_heading=h.4kx3h1s) Service Provider and Entity Engagement and Compliance Monitoring 51

[**21**](#_heading=h.302dr9l) **Inventory of system components 51**

[**22**](#_heading=h.1f7o1he) **Appendix A – Security Awareness and Acceptable Use Policy 52**

[**23**](#_heading=h.3z7bk57) **Appendix B – Authorization Request Form 56**

[**24**](#_heading=h.thw4kt) **Appendix C – Change Request Form 57**

[**25**](#_heading=h.3dhjn8m) **Appendix D – Media Inventory Log 58**

[**26**](#_heading=h.1smtxgf) **Appendix E – Permitted Network Services and Protocols 59**

[**27**](#_heading=h.4cmhg48) **Appendix F – System Configuration Standards 60**

[F.1](#_heading=h.16x20ju) Windows Systems 60

[F.1.1](#_heading=h.3qwpj7n) Windows Installation 60

[F.1.2](#_heading=h.261ztfg) Windows 2000 Server 60

[F.1.3](#_heading=h.l7a3n9) Windows 2000 Professional 60

[F.1.4](#_heading=h.356xmb2) Windows NT 61

[F.1.5](#_heading=h.1kc7wiv) Windows 2003 Server Domain Controller 61

[F.1.6](#_heading=h.44bvf6o) Windows 2003 Server Member Server 61

[F.1.7](#_heading=h.2jh5peh) Windows XP Professional 61

[F.2](#_heading=h.ymfzma) UNIX Systems 61

[F.2.1](#_heading=h.3im3ia3) UNIX Installation 61

[F.2.2](#_heading=h.1xrdshw) HP-UX 62

[F.2.3](#_heading=h.4hr1b5p) Linux 62

[F.2.4](#_heading=h.2wwbldi) FreeBSD 62

[F.2.5](#_heading=h.1c1lvlb) Solaris 62

[F.3](#_heading=h.3w19e94) Network Devices 63

[F.3.1](#_heading=h.2b6jogx) Network Device Installation 63

[F.3.2](#_heading=h.qbtyoq) Cisco IOS 63

[F.3.3](#_heading=h.3abhhcj) Cisco PIX Firewall 63

[F.3.4](#_heading=h.1pgrrkc) Wireless Access Point 63

[F.4](#_heading=h.49gfa85) Server Applications 64

[F.4.1](#_heading=h.2olpkfy) Application Installation 64

[F.4.2](#_heading=h.13qzunr) Oracle Database 64

[F.4.3](#_heading=h.3nqndbk) Apache Web Server 64

[**28**](#_heading=h.22vxnjd) **Appendix G – System Configuration Record 65**

[**29**](#_heading=h.i17xr6) **Appendix H – Backup Media Transfer Log 66**

[**30**](#_heading=h.1h65qms) **Appendix I – Encryption Key Custodianship Form 67**

[**31**](#_heading=h.415t9al) **Appendix J – Encryption Key Management Log 68**

[**32**](#_heading=h.2gb3jie) **Appendix K – Critical Technologies Device Inventory 69**

[**33**](#_heading=h.vgdtq7) **Appendix L – Periodic Operational Security Procedures 71**

[**34**](#_heading=h.3fg1ce0) **Appendix M – NEW EMPLOYEE CARD 72**

[**35**](#_heading=h.1ulbmlt) **Appendix N – Inventory of System Components 73**

[**36**](#_heading=h.4ekz59m) **Appendix O – List of Card-Reading Devices at POS 74**

[**37**](#_heading=h.2tq9fhf) **Appendix P – List of Service Providers 74**

[**38**](#_heading=h.18vjpp8) **Appendix Q1 – Role Assignment List 75**

[**39**](#_heading=h.3sv78d1) **Appendix Q2 – Role Specification List 76**

[**40**](#_heading=h.280hiku) **Appendix Q3 – Role Specification for PAN Visibility 76**

# 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 – |  |  |

# INTRODUCTION AND SCOPE

## 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.

## 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.

## 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.)

# POLICY ROLES AND RESPONSIBILITIES

## Policy Applicability

All employees, contractors, vendors and third-parties that use, maintain or handle

%Company% information assets must follow this policy.

## 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.)

## 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.).

## 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.

## Users

Each user of %Company% computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all %Company% information system users:

* Understand what the consequences of their actions are with regard to computing security practices and act accordingly. Embrace the “Security is everyone’s responsibility” philosophy to assist %Company% in meeting its business goals.
* Maintain awareness of the contents of the information security policies.
* Read and sign at least annually the %Company% Security Awareness and Acceptable Use Policy (Appendix A)
* Classify confidential and sensitive information that is received unclassified. Limit the distribution of this information accordingly.

**PCI Requirements Reference:**

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

**12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

## Role Assignment

%Company% uses role-based access control (RBAC) to restrict data resource access to unauthorized subjects. All personnel are assigned appropriate roles before they can exercise permissions and access data resources. Each role is connected to data resource access needs and a level of privilege as defined in Appendix Q2.

Roles are based on individual personnel’s job classification and function. All privileged user IDs are granted the least privilege necessary to perform job responsibilities. The security team is responsible for assigning roles with corresponding level of privilege and provides documented approval for each role in appendix Q1.

**PCI Requirements Reference:**

**7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access.

**7.1.1** Define access needs for each role, including:

System components and data resources that each role needs to access for their job function

Level of privilege required (for example, user, administrator, etc.) for accessing resources

**7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

**7.1.3** Assign access based on individual personnel’s job classification and function.

**7.1.4** Require documented approval by authorized parties specifying required privileges.

# IT CHANGE CONTROL POLICY

## Policy Applicability

All proposed changes to %Company% network devices, systems and application configurations must follow this policy.

## Change Request Submittal

The responsible party that will be implementing the change must complete and submit a Change Request Form to the COO. A model form is shown in Appendix C illustrating the minimum data to be captured electronically or on hard copy. This form will not be reviewed without the following information completed, at a minimum:

* Resources Affected by Change (customers) – If a change could impact the functionality of customers, internal or external, this item must be completed. This documentation must include changes to features, applications and procedures that will be different from the existing system. Included in this documentation are any upgrades that the customer needs to perform to the operating system or other required 3rd party software or hardware.
* Back out Procedures – If the change does not go as intended a plan must be in place that describes the process of reverting the environment to its original configuration.
* Test Plan - A set of planned tests must be developed to verify that the change accomplished what it was supposed to do, and does not adversely affect other system components or create a weakness in the security posture of the environment. This plan may be specific to each change.

Completion of the relevant details in the %Company% issue tracking system is equivalent to completion of the change request form.

**PCI Requirements Reference:**

**Audit Procedure 6.4.5.1** Verify that documentation of customer impact is included in the change control documentation for each sampled change

**6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system.

**Audit Procedure 6.4.5.4** Verify that back-out procedures are prepared for each sampled change.

## Change Request Approval

After all planning and documentation is complete all management and concerned parties must sign off on the Change Request Form. This can be achieved verbally in the weekly IT Development meeting.

**PCI Requirements Reference:**

**Audit Procedure 6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change.

## Change Testing

Prior to introduction into the production network or systems all changes must first be tested on a QA or test network isolated from the production environment.

The documented test plan must be followed to ensure no adverse effects on the network, systems or applications. Any discrepancies should be documented and a new Change Request Form generated once all issues have been resolved. All relevant PCI DSS requirements are implemented on all new or changed systems and networks, and documentation updated as applicable.

**PCI Requirements Reference:**

**6.4.6** Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

**6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following:

* Change control procedures related to implementing security patches and software modifications are documented.

**6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system

**6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls.

## Change Implementation

All changes must be implemented according to the documented change procedures that were tested successfully. Any discrepancies between expected results and actual results that impact the network, systems, applications, business requirements or support procedures must result in the immediate invocation of the documented back out procedures.

# DATA CLASSIFICATION AND CONTROL POLICY

## Policy Applicability

All data stored and accessed on %Company% information systems, whether managed by employees or by a third party, must follow this policy. Policy exemptions will be permitted only if approved in advance and in writing by the COO.

## Data Classification

### Introduction

All data stored on %Company% computing resources must be assigned a classification level by the information owner or creator. This level is used to determine which users are permitted to access the data.

### %Company% Internal Information Categories

**Confidential** - applies to the most sensitive business information which is intended strictly for use within %Company%. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, and/or its customers.

Confidential information includes:

* Passwords
* Encryption keys
* Cardholder information
* Bank account information
* Intellectual property

**Sensitive** - Applies to less sensitive business information, which is intended for use within %Company%. Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers.

Sensitive information includes:

* Internal market research
* Audit reports, etc.

**Private** - Applies to personal information, which is intended for use within %Company%.

* Unauthorized disclosure could adversely impact the company and/or its employees.
* Examples of Private information include: policies and procedures, procedure metrics, human resources information, etc.

**Public** - Applies to all other information which does not clearly fit into any of the above three classifications. Unauthorized disclosure isn’t expected to seriously or adversely impact the company. Any release of this information must be authorized by the COO or CEO. Public information includes:

**PCI Data** – The class of credit card and transaction data identified for protection under the Payment Card Industry (PCI) Data Security Standard (DSS). Two types of data are defined: Cardholder Data which may be stored after transaction authorization and Sensitive Authentication Data which may **not** be stored after transaction authorization.

* **Card Holder Data** – Applies to credit card data taken as payment for services. Data elements as specified in the PCI DSS version 3.2 are
  + Primary Account Number (PAN)
  + Card holder Name
  + Service Code
  + Expiration Date
* **Sensitive Authentication Data** – Applies to credit card data required for authentication and processing of credit card transactions as specified in the PCI DSS version 3.2 are
  + Full Track Data
  + CAV2/CVC2/CVV2/CID
  + PIN/PIN Block

## Data Access

All confidential or sensitive data must be protected via access controls to ensure that data is not improperly disclosed, modified, deleted or rendered unavailable. The access controls must track all access to such data and identify who and when the data was accessed (See Section 16 Logging Controls Policy for more details). All access to systems must be configured to deny-all but what information a particular user needs to access per their business role.

Access to systems or applications handling confidential, sensitive or private information must follow the data access request process. All requests require approval by the Information Security Team and a valid Authorization Request Form (Appendix B - A model form is shown illustrating the minimum data to be captured electronically or on hard copy. Access to data exceeding the employee’s authorized role must also follow the data access request process and must include documented limits around such access (e.g. access source, access time limits, etc.).

### Data Access Request Process

The following generally describes the workflow used by %Company% for requesting new access:

1. The user’s manager will request or grant (as appropriate) authorization for access to confidential data via the New Employee Card (Appendix P).
2. The user’s manager must approve the request for access based on the employee’s role, identify any additional access requirements and submit the request to a member of the Information Security Team for approval.
3. If the access requested requires privileges above the employee’s role a member of the Information Security Team will engage additional system owners or management to confirm.
4. The Information Security Team will forward the approved request to the System Administrator for account creation.
5. The System Administrator will create the user account(s) requested. Once the accounts have been created, the System Administrator must forward the request form to the COO for inclusion in the Users employee records and notify the Information Security Team that the request has been completed.

Requests for change of access must be submitted by the user’s manager utilizing the last version of the New Employee Card (Appendix M). Business units are expected to capture this data in such a form that a clear audit trail is available for review at all times on file and the workflow shall be the same as above. Direction regarding removal of an employee’s access shall follow the same workflow above. When an employee leaves the business a note will be added to their New Employee Card to confirm that access has been removed.

## Physical Security

Hard copy materials and electronic media containing sensitive or confidential information must be protected by appropriate physical access controls.

* Cameras must be used to monitor server closets and data centers where systems reside that store sensitive, confidential, and cardholder data. The data collected must be stored for at least 3 months unless otherwise restricted by law.
* Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential or sensitive data.
* Visitor logs and physical audit trails of access to these systems must be collected and kept at least 3 months unless otherwise restricted by law.
* Physical access must be restricted to publicly accessible network jacks, wireless access points and handheld devices.

**PCI Requirements Reference:**

**9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

**9.1.1** Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

**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.

**9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.

## User Authentication

### Users

Each user’s access privileges shall be authorized according to business need. User access authority to computer resources shall be provided only when necessary to perform tasks related to %Company% business.

The use of non-authenticated (e.g., no password) User IDs or User IDs not associated with a single identified user are prohibited. Shared or group user IDs are never permitted for user-level access. Every user must use a unique user account and a personal secret password for access to %Company% information systems and networks. Systems and applications must authenticate using a password or token entry.

All users must acknowledge understanding of the %Company% Information Security Policies by reading and signing the %Company% Security Acknowledgment and Acceptable Use Policy (Appendix A) prior to being allowed to access %Company% information systems and networks.

**PCI Requirements Reference:**

**7.2** Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. This access control system(s) must include the following:

**7.2.2** Assignment of privileges to individuals based on job classification and function.

**8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.

**8.4** Document and communicate authentication policies and procedures to all users including:

* + Guidance on selecting strong authentication credentials
  + Guidance for how users should protect their authentication credentials
  + Instructions not to reuse previously used passwords
  + Instructions to change passwords if there is any suspicion the password could be compromised.

**8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

**8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

* + All user access to, user queries of, and user actions on databases are through programmatic methods.
  + Only database administrators have the ability to directly access or query databases.
  + Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

**10.1** Implement audit trails to link all access to system components to each individual user.

### Systems

Each computer system shall have an automated or procedural access control process. The process requires the following:

* Generic user IDs or passwords are disabled or removed.
* User ID’s shall consist of at least 7 characters.
* User ID’s will be unique for each user.
* Authenticate every system account and application account with a password.
* Require all passwords/passphrases to be at least 7 characters in length.
* Require complex passwords, consisting of both numeric and alphabetic characters.
* Require that new passwords cannot be the same as the four previously used passwords.
* Lock out user ID after not more than six invalid logon attempts.
* Require that once a user ID is locked out, it remains locked for at least 30 minutes or until the System Administrator enables the user ID.
* Require system/session idle time out of 15 minutes.
* Require passwords to be reset at least every ninety (90) days.
* Remove/disable inactive user accounts at least every ninety (90) days.

The requirements above are for authenticating all system users.

**PCI Requirements Reference:**

**8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data.

**8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:

* + Something you know, such as a password or passphrase
  + Something you have, such as a token device or smart card
  + Something you are, such as a biometric.

**8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

**8.1.4** Remove/disable inactive user accounts at least every 90 days.

**8.2.4** Change user passwords/passphrases at least once every 90 days.

**8.2.3** Passwords/passphrases must meet the following:

* + Require a minimum length of at least seven characters.
  + Contain both numeric and alphabetic characters.

Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above

**8.2.5** Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.

**8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts.

**8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

**8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

## Account and Access Management

### Information Security Team Responsibilities

The Information Security Team will approve access authorization according to the role and responsibilities of information system users. Each request for access must contain written and/or electronic evidence of approval by the Information Security Team.

Information Security, in conjunction with business unit management, will determine the default access levels that will be granted per a user’s role (see section 2.6). The Information Security Team will perform a bi-annual audit of computer resource authorizations to confirm that access privileges are appropriate. The audit will consist of validating access rights for sample user populations.

The Information Security Team must collect additional approvals for all access that is not associated with a defined access role. Extension authorizations for contractor accounts must go through the Information Security Team to provide an audit trail. An Emergency ID will be established when access is needed to diagnose and/or correct a problem.

* The request to create the Emergency ID must be made via the Information Security Team, which will notify the appropriate system administration team.
* The requestor must inform the Information Security Team upon completion of the work so that the ID can be disabled.
* The Information Security Team will ensure that the Emergency ID Request Form is completed as soon as practical (the completion of this form should NOT delay providing access). The completed form must be filed by the Information Security Team

### System Administrator Responsibilities

Account creation requests must specify access either explicitly or via a “role” that has been mapped to the required access. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights. If a user requests a password reset via phone, email, web or other non-face-to-face method, that user’s identity must be verified before the password is reset.

Access should be removed immediately upon notification that access is no longer required. Written procedures must be in place to ensure that access privileges of terminated or transferred users are revoked as soon as possible. Whenever possible users who are on leave-of-absence or extended disability should be suspended from the system.

User IDs shall be disabled after sixty (60) days of inactivity. After an additional thirty (30) days, disabled user IDs must be purged. These requirements may not apply to certain specialized accounts (e.g., NT Admin, root). In those instances, the System Administrator must provide a written waiver to the Information Security Team and document the compensating controls around access to the accounts.

All computer resources capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

* System Administrators must enable audit logs to record user and administrative activities. Audit logs must be archived for a minimum of one year with (90) days available for on-line viewing.
* Passwords set by System Administrators must be changed by the user immediately upon the user’s next login. System Administrators must set initial passwords that are unique and compliant with the password rules.
* System Administrators must validate the identity of the user before performing a password reset. Business units must create local policies for positively validating user identities.
* Contractor accounts must have Information Security Team approval and must automatically expire at the end of the contract date. Extensions must be requested through the Information Security Team. System Administrators must monitor these accounts carefully while they are in use.
* Access must be immediately revoked for terminated users and for user access that is no longer required.
* Vendor accounts used for remote maintenance must only be enabled during the time that access is needed.
* Ensure that all systems and especially access to any databases containing cardholder information is authenticated (e.g., users, applications, administrators, etc.).

**PCI Requirements Reference:**

**8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects

**8.1.3** Immediately revoke access for any terminated users.

**8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

**Audit Procedure 8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use.

**8.1.4** Remove/disable inactive user accounts at least every 90 days

**8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:**

* Enabled only during the time period needed and disabled when not in use.
* Monitored when in use

**8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

**8.2.4** Change user passwords at least once every 90 days.

**8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

* + All user access to, user queries of, and user actions on databases are through programmatic methods.
  + Only database administrators have the ability to directly access or query databases.
  + Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

**10.1** Implement audit trails to link all access to system components to each individual user.

# DATA RETENTION AND DISPOSAL POLICY

## Policy Applicability

All data deemed sensitive or confidential by the Information Security Team, which is stored on %Company% networks and systems must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

## Retention Requirements

All sensitive and confidential data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements. The specific retention length will be established by the Data Owner under advisement form the General Counsel.

### Sample Data Types and Data Retention

|  |  |
| --- | --- |
| **Data Type** | **Data Retention Period** |
| Confidential | 10 years |
| Sensitive | 7 years |
| Private | 5 years |
| Public | 3 years |
| PCI Data (Card Holder Data) | 18 months |
| PCI Data (Sensitive Authentication Data)\* | Never stored beyond authorization of  payment transaction |

\*As a special case, cardholder data used for single transactions may be kept for up to 120 days. Cardholder data utilized for recurring transactions will be retained for the lifetime of the customer’s account with %Company%. Once a customer’s account is disabled or terminated, all of the cardholder data for that merchant must be purged within 120 days of the termination using an approved destruction method. Sensitive Authentication Data, including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. Storage of cardholder authorization data post-authorization is forbidden. Business units will create local policies for retention of all other company information. All system and network audit logs must be retained for one year with 90 days minimum kept available for online use.

**PCI Requirements Reference:**

**3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

* + Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
  + Specific retention requirements for cardholder data
  + Processes for secure deletion of data when no longer needed
  + A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

**3.2** Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

**3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

**3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

**3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.

**10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

## Disposal Requirements

All confidential or sensitive electronic data, when no longer needed for legal, regulatory or business requirements must be removed from %Company% systems using an approved method documented in this policy. This requirement includes all data stored in systems, temporary files or contained on storage media.

**PCI Requirements Reference:**

**9.8** Destroy media when it is no longer needed for business or legal reasons as follows:

## Disposal Process

A programmatic (automatic) process will be executed on cardholder information systems nightly to remove all sensitive and confidential data that exceeds business retention requirements. Other applicable data stored in files and directories where the containing media will be reused must be deleted securely by a “wiping” utility approved by the Information Security Department.

Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:

* Hard disks: sanitize (7-pass binary wipe), degauss or shred platter.
* Floppy disks: disintegrate, incinerate, pulverize, shred or melt.
* Tape media: degauss, shred, incinerate, pulverize or melt.
* USB “thumb” drives, smart cards, and digital media: incinerate, pulverize or melt.
* Optical disks (CDs and DVDs): destroy optical surface, incinerate, pulverize, shred or melt.
* RSA Encryption Keys: keys must be revoked and the revoked key published to any online key repositories where the previously valid key is stored.
* Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all confidential or sensitive information must be destroyed or concealed according to the approved methods in this policy.
* Removable computer storage media such as floppy, optical disks or magnetic tapes may not be donated to charity or otherwise recycled.
* Outsourced destruction of media containing confidential or sensitive information must use a bonded Disposal Vendor that provides a “Certificate of Destruction”.
* Storage containers used for materials that are to be destroyed must be secured. For example, “to-be-shredded” containers could have a lock preventing access to their content, or physically prevent access to the inside of the container by following the measures in section 6.2.

**PCI Requirements Reference:**

**3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

* + Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
  + Specific retention requirements for cardholder data
  + Processes for secure deletion of data when no longer needed
  + A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

**9.8** Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:

**9.8.1** Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

**9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

# PAPER AND ELECTRONIC MEDIA POLICIES

## Policy Applicability

All employees handling hardcopy or electronic media must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Operating Officer.

## Storage

### Physical Security

Hard copy materials and electronic media containing sensitive or confidential information must be protected by appropriate physical access controls.

* Camera must be used to monitor sensitive areas. The data collected must be stored for at least 3 months unless otherwise restricted by law.
* Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential or sensitive data.
* Visitor logs and physical audit trails of access to these systems must be collected and kept at least 3 months unless otherwise restricted by law.

**PCI Requirements Reference:**

**9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

**9.1.1** Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

**9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.

**Audit procedure 9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

**9.7** Maintain strict control over the storage and accessibility of media.

### Hardcopy Media

Hard copy materials containing sensitive or confidential information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

* At no time are printed reports containing confidential or sensitive information to be removed from any %Company% secure office environment.
* At no time is printed material containing confidential or sensitive information to be removed from any %Company% data center or computer room without prior authorization from the Information Security Team.
* Printed reports containing consumer confidential or sensitive data are to be physically retained, stored or archived only within secure %Company% office environments, and only for the minimum time deemed necessary for their use.
* All hardcopy material containing confidential or sensitive information should be clearly labeled as such.
* All confidential or sensitive hardcopy media must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin) which has been approved by the Information Security Team.
* Confidential or sensitive hardcopy material is never to be stored in unlocked or insecure containers or open workspaces.

### Electronic Media

Electronic media containing sensitive or confidential information (e.g., CD, DVD, floppy disk, hard disk, tape, etc.) is subject to the following storage guidelines:

* Confidential or sensitive information must never be copied onto removable media without authorization from the Information Security Team.
* At no time is electronic media containing confidential or sensitive information to be removed from any %Company% secure office environment with the exception of computer system backups.
* At no time is electronic media containing confidential or sensitive information to be removed from any %Company% data center or computer room without prior authorization from the Information Security Team.
* Electronic media containing consumer confidential or sensitive data are to be physically retained, stored or archived only within secure %Company% office environments, and only for the minimum time deemed necessary for their use.
* All electronic media containing confidential or sensitive information should be clearly labeled as such.
* All removable, confidential or sensitive electronic media must be stored securely.
* All media must be sent or delivered by a secured courier or other delivery methods that that can be accurately tracked and that have been approved by the Information Security Team.

**PCI Requirements Reference:**

**9.5** Physically secure all media.

**9.6** Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:

**9.6.1** Classify the media so it can be identified as confidential.

**9.6.2** Send the media by secured courier or other delivery methods that that can be accurately tracked

**9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).

## Inventory

A Media Inventory Log (Appendix D A model form is shown illustrating the minimum data to be captured electronically or on hard copy). All stored electronic and hardcopy media containing confidential or sensitive information must be inventoried at least annually by the Information Security Team. At this time, the security controls on the storage mechanism will be checked. Upon completion of the inventory the log will be updated.

**PCI Requirements Reference:**

**9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually

## Destruction

All hardcopy shred bins must remain locked at all times (until shredding). Employees should make every effort to immediately cross-cut shred any printed material containing confidential or sensitive information.

Electronic media must be destroyed as outlined in the Data Retention and Disposal Policy.

**PCI Requirements Reference:**

**9.8** Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:

**9.8.1** Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

**Audit procedure 9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).

# FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY

## Policy Applicability

All firewalls and routers on %Company% networks, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

## Device Management Responsibilities

Management of all %Company% firewalls and routers shall be a combined effort of the System Administrator, the Network Operations Center and the Information Security Team. The following subsections detail the responsibilities for these groups.

### System Administrator

* Assure that changes to firewall hardware or software or security rules are approved by the Information Security Team and follow all change control policies and procedures.
* Document all firewall security rule changes utilizing Appendix E, Permitted Network Services and Protocols (A model form is shown illustrating the minimum data to be captured electronically or on hard copy).
* Following every change, review and update network diagrams to assure they accurately describe all connections to confidential or sensitive information and critical network protection mechanisms (e.g., firewalls, IDS/IPS, Anti-virus systems, access control systems, etc.).
* Enable appropriate logging on all security systems and perform active daily monitoring of the logs that report security events.
* Provide the Network Operations Center with read-only access to logs related to the critical systems health and performance.
* Provide the Network Operations Center and Information Security Team with read-only access to security event logs.
* Report network security incidents to the Information Security Team immediately upon discovery.
* Coordinate an appropriate response with the Information Security Team to mitigate security events.
* Ensure that router configuration files are secures and synchronized properly.

### Network Operations Center

* Monitor system and application specific alerts on critical systems (e.g., interface up/down, firewall daemon failing, system reboots, etc.)
* Notify the appropriate parties in the event of a security system failure or security event.

### Information Security Team

* Assure that security rules applied to the firewalls are sufficient to protect %Company% networks and corporate assets from external attacks and unauthorized access.
* Assure that security rules applied to the firewalls are sufficient to prevent internal security events from leaving the %Company% network.
* Review all firewall and router security rule change requests for policy compliance prior to submission through the change management process.
* Ensure that all protocols/services allowed through the firewalls are properly documented
* Ensure risky protocols have undergone a risk assessment and have a current documented business need.
* Actively monitor firewall security events to identify internal or external security incidents.
* Coordinate an appropriate response with the System Administrator to mitigate security events.

**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**.**

**1.1.5a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.

**1.2.2** Secure and synchronize router configuration files.

## Firewall and Router Configuration Changes

Because firewalls and routers support critical %Company% information systems activities they are considered to be production systems.

All firewall and router changes must be approved by the Information Security Team and must be adequately tested following production standards as defined in the Change Control Policy. These changes include, but are not limited to:

* Rule additions, deletions, and modifications.
* Software or system modifications.
* Software or system upgrades, patches, or hot-fixes.

**PCI Requirements Reference:**

**1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations.

## Allowed Services

Every port, protocol and service that is not specifically permitted by this policy, with supporting documents issued by the Information Security Team, must be blocked by %Company% firewalls. The list of currently approved ports, protocols and services, with justifications, is listed in Appendix E, Permitted Network Services and Protocols.

For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (e.g., NIST, ENISA, OWASP, etc.).

**PCI Requirements Reference:**

**1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

**1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

## Allowed Network Connection Paths and Configuration Requirements

All Internet-based inbound traffic is only permitted into a firewall segmented demilitarized zone (DMZ) network. In all cases, this traffic should be limited to only ports necessary for %Company%’s business requirements. Perimeter routers should not be configured with a route to internal address space with the exception of the DMZ. Internal IP addresses must be hidden utilizing Network Address Translation (NAT) or Port Address Translation (PAT). Anti-spoofing technologies must be configured on perimeter devices, denying or rejecting all traffic with a:

* Source IP address matching internally allocated or %Company% owned address space.
* Source IP address matching RFC 1918 address space.
* Destination IP address matching RFC 1918 address space.

Outbound traffic from internal production systems must only be allowed to the %Company% DMZ network. Additionally, this traffic should be restricted to only required protocols and services.

Databases must be located on an internal network, which is segmented from the %Company% DMZ network. Inbound connections to internal production payment systems, and originating from %Company% wireless networks, are not permitted. The use of a stateful packet inspection firewall must be utilized for Internet and wireless segmentation to only allow established connections into or out of each particular network segment. VLAN's with compliant ACL’s may be used for cardholder environment segmentation so long as the VLAN switch is compliant with PCI and hardened to prevent all currently identified switch exploits (e.g. ARP cache flood). If VLAN’s are used for segmenting all requirements for firewalls apply (e.g. deny all but business necessary traffic, change control, etc).

**PCI Requirements Reference:**

**1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment.

**1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

**1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ.

**1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

**1.3.5** Permit only “established” connections into the network**. (***Implementing stateful packet inspection, also known as dynamic packet filtering*)

**1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

**1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

**1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

**1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

**1.3.7** Do not disclose private IP addresses and routing information to unauthorized parties.

*Note: Methods to obscure IP addressing may include, but are not limited to:*

* + *Network Address Translation (NAT)*
  + *Placing servers containing cardholder data behind proxy servers/firewalls,*
  + *Removal or filtering of route advertisements for private networks that employ registered addressing,*
  + *Internal use of RFC1918 address space instead of registered addresses.*

## Configuration Review

At least every six months, the Information Security Team must thoroughly review each firewall rule set and record results of the review. The review must include the removal, when merited, of unused or unnecessary access paths. All proposed changes identified as a result of this review must go through the current change control process prior to implementation.

**PCI Requirements Reference:**

**1.1.7** Requirement to review firewall and router rule sets at least every six months.

## Personal Firewalls

All mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees) that are used to access the %Company% network must have personal firewall software (or equivalent functionality) installed and activated. All such software must be configured to actively run and have a non-user alterable configuration as dictated by the Information Security Team.

**PCI Requirements Reference:**

**1.4** Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:

* Specific configuration settings are defined
* Personal firewall (or equivalent functionality) is actively running.
* Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

# SYSTEM CONFIGURATION POLICY

## Policy Applicability

All servers and network devices on %Company% networks, whether managed by employees or by third parties, must be built and deployed in accordance with this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

## System Build and Deployment

### System Purpose

All computing systems should be designated for a single primary purpose where possible (e.g., web servers, database servers, and DNS should be implemented on separate servers). No multi-purpose systems may, under any circumstances, store, transmit, or process confidential or sensitive data unless required by vendor documentation (e.g., SAP, Peoplesoft, ipAngel, Cisco Pix with add-ons, etc).

**PCI Requirements Reference:**

**2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

### System Configuration Standards

All systems, prior to deployment in the production environment must conform to the

System Configuration Standards (Appendix G- a model form is shown illustrating the minimum data to be captured electronically or on hard copy). A valid business justification and risk assessment must exist for all deviations from %Company% published configuration standards. Deviations require written approval by the Information Security Team and must be noted on the System Configuration Record for the system.

### System Configuration Records

A System Configuration Record (Appendix G - a model form is shown illustrating the minimum data to be captured electronically or on hard copy. This form must be updated with any future modifications to system configurations.

### System Configuration Process

All new system deployments will follow the following high level procedure:

1. Install operating system.
2. Update all operating system software per vendor recommendations.
3. Configure operating system parameters and secure the system according to the system configuration build documentation described in Appendix F (A model form is shown illustrating the minimum data to be captured electronically or on hard copy. Install applications and software:
   1. Install system specific applications and software according to System Configuration Record (if this is a replacement for an existing system).
   2. Install applications and software necessary for the systems purpose.
   3. Configure Network Time Protocol (NTP).
4. Update all application software per vendor recommendations.
5. Configure application parameters according to build document (application hardening).
6. Enable logging per Logging Controls (Section 16).
7. For systems containing confidential or sensitive information deploy file integrity monitoring (FIM) software to alert personnel to unauthorized modification of critical system or content files. Configure FIM to perform critical file comparisons at least weekly.
8. Complete system specific System Configuration Record and maintain on file.

**PCI Requirements Reference:**

**2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

**2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.

**2.2.4** Configure system security parameters to prevent misuse.

**Audit Procedure 2.2.4.b** Examine the system configuration standards to verify that common security parameter settings are included.

**2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

**11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

### Standard Software

The following list must be considered standard installed software on all applicable systems. A valid business justification and risk assessment must exist for all deviations from %Company% published configuration standards. Any such deviations require written approval by the Information Security Team, and noted on the System Configuration Record for the system (see below).

* File servers, mail servers, and Windows-based systems
* Anti-Virus software
* Critical production systems
* File Integrity software
* Notebooks/Laptops
* Personal Firewall software
* VPN Client software
* PGP Desktop with Whole Disk Encryption enabled

**PCI Requirements Reference:**

**1.4** Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.

**5.1**Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

### Network Time Protocol (NTP)

With the exception of the internal %Company% NTP server(s), all %Company% production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment. The internal %Company% NTP server(s) will be configured to request time updates from the Internet site time.nist.gov. Client systems able to retrieve time settings from the NTP server will be limited through Access Control Lists (ACL). Access to time data is restricted to only personnel with a business need to access the data. The NTP system will at all times be running the latest available version of the software. Changes to time settings are logged, monitored, and reviewed.

**PCI Requirements Reference:**

**10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

*Note: One example of time synchronization technology is Network Time Protocol (NTP).*

**Audit Procedures 10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.

**10.4.1** Critical systems have the correct and consistent time**.**

**10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:

* Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.
* Where there is more than one designated time server, the time servers peer with one another to keep accurate time.
* Systems receive time information only from designated central time server(s).

**10.4.2** Time data is protected**.**

**10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.

**10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.

### Credit Card Information Processing Application

All %Company% applications, dealing with the processing or retrieval of cardholder information, must be configured in a manner which masks or truncates displayed PAN so that the first six and last four digits are the maximum number of digits to be displayed. If the application is designed for a specific purpose in which the full PAN must be displayed, approval must be given by the Information Security Team during the Requirements Phase as described in Section 13 Software Development Policy. In all cases displaying full or masked PANs must be limited to the fewest number of users possible and only personnel with a legitimate business need can see more than first six/last four digits of the PAN.

**PCI Requirements Reference:**

**3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN.

### Credit Card Storage Applications

All %Company% applications, dealing with the storage of cardholder information, must be configured in a manner which does not retain prohibited cardholder data, such as full track data, card-validation codes, card not present values, pins or pin blocks. Storage devices on a network must be on an internal network segregated from the DMZ. All access to networked storage devices must have its authentication and communication encrypted. The PAN must be rendered unreadable through one of the following:

* Strong one-way hash functions (hashed indexes) with salts
* Truncation
* Index tokens and pads (pads must be securely stored)
* Strong cryptography with associated key management processes and procedures

**PCI Requirements Reference:**

**1.3.6** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

**3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

*Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:*

* *The cardholder’s name*
* *Primary account number (PAN)*
* *Expiration date*
* *Service code*

*To minimize risk, store only these data elements as needed for business.*

**3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

**3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.

**3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

* + One-way hashes based on strong cryptography, (hash must be of the entire PAN)
  + Truncation (hashing cannot be used to replace the truncated segment of PAN)
  + Index tokens and pads (pads must be securely stored)
  + Strong cryptography with associated key-management processes and procedures.

**8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

### Change Detection

Change-detection solutions such as file-integrity monitoring (FIM) software are installed on all critical systems that contain sensitive data. The Change-detection solution must monitor all user activity on critical systems. Reporting and alerting tools are enabled in order to automatically alert key personnel when changes to critical files have been made (ex. System executables, application executables, configuration files, content files, log and audit files). The software is configured to perform critical file comparisons at least weekly. Alarms from the Change-detection solution are continuously reviewed to determine if incident response actions need to be taken. If unauthorized changes have been done to systems containing confidential or sensitive information, the security team is immediately notified and the incident response measures in section 14 are performed.

**PCI Requirements Reference:**

**11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

**11.5.1** Implement a process to respond to any alerts generated by the change-detection solution.

## Vulnerability Identification and System Updates

### Vulnerability Identification

Members of the Information Security Team must be informed of information security issues and vulnerabilities applicable to %Company’s% computing systems. When security issues are identified, the Information Security Team is responsible for notifying appropriate personnel, including system and network administrators and assigning a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

The primary method for identifying new threats as they arise will be through vendor and security specific Internet mailing lists. Although not complete, the following lists should be subscribed to as well as other vendor lists applicable to %Company% specific software packages and systems:

* CERT
* NT BUGTRAQ
* SANS

%Company% System Configuration Standards (Appendix F - a model form is shown illustrating the minimum data to be captured electronically or on hard copy) must be updated to reflect measures required for protection from any newly discovered vulnerability.

**PCI Requirements Reference:**

**2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to:

* Center for Internet Security (CIS)
* International Organization for Standardization (ISO)
* SysAdmin Audit Network Security (SANS) Institute
* National Institute of Standards Technology (NIST).

**6.1** Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

### Vulnerability Testing

The Information Security Team is responsible for conducting internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). This process includes identifying any unauthorized wireless devices on the network. Internal vulnerability scans are performed by qualified personnel. Additional external vulnerability scans must be performed at least quarterly by a scan vendor qualified by the payment card industry.

Internal and external penetration tests at both the application and network layer must be performed annually or after any significant change in the network. %Company% ‘s penetration tests are based on industry-accepted penetration testing approaches (for example, NIST SP800-115) and Includes coverage for the entire CDE perimeter and critical systems. Application layer penetration tests must cover all the vulnerabilities in section 13.2.2. Any segmentation controls and scope reduction controls must be tested to ensure that the CDE is isolated from the rest of the network. A penetration test always follows any changes to segmentation controls/methods isolating the CDE, otherwise it is done annually. A review and special consideration will be taken for vulnerabilities and threats experienced in the last 12 months. All potential vulnerabilities identified through vulnerability scans and penetration tests will be communicated to appropriate personnel within %Company% for assessment and remediation. All high-risk vulnerabilities must be corrected utilizing the Change Control %Company% Policy. Follow up scans must be performed to verify all “high-risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per PCI DSS Requirement 6.1)

The Chief Technical Officer must coordinate an annual formal risk assessment process that identifies any existing or new threats and vulnerabilities to ensure %Company’s% assets are adequately protected.

**PCI Requirements Reference:**

**11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

**11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

**11.2.1** Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high-risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.

**11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

**11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.

**11.3.1** Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

**11.3.2** Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

**11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

**11.3** Implement a methodology for penetration testing that includes at least the following:

* + Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115).
  + Includes coverage for the entire CDE perimeter and critical systems.
  + Includes testing from both inside and outside of the network.
  + Includes testing to validate any segmentation and scope reduction controls.
  + Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.
  + Defines network-layer penetration tests to include components that support network functions as well as operating systems.
  + Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.
  + Specifies retention of penetration testing results and remediation activities results.

**11.3.4** If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

**11.4** Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

**12.2** Implement a risk assessment process, that: Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), Identifies critical assets, threats, and vulnerabilities, and Results in a formal, documented analysis of risk.

### Security Patch Deployment

All security patches, hot-fixes and service packs identified by the Information Security

Team or system administrators must be applied to applicable systems within (30) days of vendor release. As with any change to the environment the change management process must be followed.

**PCI Requirements Reference:**

**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

# ANTI-VIRUS POLICY

## Software Configuration

All applicable systems must be configured with Information Security Team approved anti-virus/anti-spyware/anti-adware software. The software must be configured to be actively running, perform periodic scans, log anti-virus events with routing to a central logging solution, and end users must not be able to configure or disable the software.

**PCI Requirements Reference:**

**5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

**5.2** Ensure that all anti-virus mechanisms are maintained as follows:

* Are kept current.
* Perform periodic scans.
* Generate audit logs which are retained per PCI DSS Requirement 10.7.

**5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

**5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

## Signature Updates

All systems with anti-virus software must be configured to update virus signatures on at least a daily basis.

**PCI Requirements Reference:**

**5.2** Ensure that all anti-virus mechanisms are maintained as follows:

* Are kept current.
* Perform periodic scans.
* Generate audit logs which are retained per PCI DSS Requirement 10.7.

**5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are configured to perform automatic updates and configured to perform periodic scans.

## Software Logging

Anti-virus software must alert the Information Security Team in real-time of the detection of a virus. The Information Security Team will determine what steps to take based on the Incident Response Policy. Retention of Anti-Virus software logs will be in accordance with the Data Retention and Disposal Policy.

**PCI Requirements Reference:**

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

## Systems not commonly affected by malware

All %Company’s% systems that is not commonly targeted by malware (ex. mainframes, mid-range computers (such as AS/400) and similar systems) are annually evaluated to confirm if any anti-virus software implementation is necessary. This is done by monitoring vendor security notices and anti-virus news groups (for example) to learn about evolving malware that is relevant to %Company’s% systems.

**PCI Requirements Reference:**

**5.1.2** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

# BACKUP POLICY

## Location

The backup media for each system is relocated to a secure off-site storage area.

The off-site storage location must be visited annually by management or a member of the Information Security Team to confirm that it is physically secure and fireproof.

**PCI Requirements Reference:**

**9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually.

## Transport

Offline storage media utilized for archival or back-up purposes must be handled and retained in a secured environment such that only %Company% personnel and contracted storage facility personnel have access to the archival media. All media couriers and transport mechanisms must be certified by the Information Security Team.

Positive log-out and log-in of archive media will take place during all archive media transfers. All media that is transferred from one location to another should be logged as being transferred, by whom, where, and was it properly received, with signature from management. The Backup Media Transfer Log is located in Appendix H (A model form is shown illustrating the minimum data to be captured electronically or on hard copy. All media containing confidential or sensitive data must be classified and identifiable as such prior to transfer as detailed in the Data Classification and Control Policy.

**PCI Requirements Reference:**

**9.6.1** Classify media so the sensitivity of the data can be determined.

**9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked.

**9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).

## Audit

All media used will be classified as confidential or sensitive and assigned a unique tracking number or similar feature that uniquely identifies the media. All media must be registered with the Information Security Team for tracking prior to use. Quarterly inventories of all stored media will take place. The Information Security Team will compare their list of in-use media with records at the storage facility using the Media Inventory Log (Appendix D A model form is shown illustrating the minimum data to be captured electronically or on hard copy.

## Media Destruction

All media that is no longer needed or has reached end-of-life must be destroyed or rendered unreadable so that no data may be extracted. Information on acceptable destruction techniques is detailed in the Data Retention and Disposal policy.

# ENCRYPTION POLICY

## Policy Applicability

This policy documents encryption standards that must be applied to all applicable mechanisms and systems on %Company% networks, whether managed by employees or by third parties. This policy also applies to the management of encryption keys, which may be shared with customers to exchange confidential information. Documentation provided to customers who have a need to exchange encryption keys with %Company% must include these guidelines. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

## Encryption Key Management

Keys must be generated, accessed, distributed and stored in a controlled and secured manner.

### Key Access

Access to encryption key components will only be granted to those custodians specifically requiring access due to job function. All access may only be granted by the Chief Technical Officer and those requiring access must have so noted on their Authorization Request Form (Appendix B - A model form is shown illustrating the minimum data to be captured electronically or on hard copy. Additionally, these users must sign the Encryption Key Custodianship Form (Appendix I) A model form is shown illustrating the minimum data to be captured electronically or on hard copy. These forms will be held in the employee’s Human Resources file.

**PCI Requirements Reference:**

**3.5.2** Restrict access to keys to the fewest number of custodians necessary.

**Audit Procedure 3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

### Split Knowledge and Dual Control

Two custodians authorized by the Information Security Team, are required to collaborate to perform any symmetric key action (such as key generation or loading the key). Additionally, no single custodian may know or have access to all pieces of a symmetric data encryption key. The separation of public and private encryption keys satisfies the concept of split knowledge and dual control.

**PCI Requirements Reference:**

**3**.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.

### Key Generation

* Only strong encryption keys are to be used. Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm.

Generating encryption keys must be accomplished by two custodians authorized by the Information Security Team. Each custodian will generate one clear text piece that will be used to create the encryption key. To prevent unauthorized substitution of keys physical and logical access to the key generating procedures and mechanisms must be secured.

**PCI Requirements Reference:**

**3.6.1** Generation of strong cryptographic keys.

**3.6.7** Prevention of unauthorized substitution of keys.

### Key Distribution

Only custodians authorized by the Information Security Team are allowed to retrieve key components from secure storage or distribute keys. Custodians must document all such actions in the Encryption Key Management Log (Appendix J) A model form is shown illustrating the minimum data to be captured electronically or on hard copy. The encryption keys must be placed in secure packaging prior to being returned to storage.

**PCI Requirements Reference:**

**3.6.2** Secure cryptographic key distribution.

### Key Storage

All secret and private keys used to encrypt/decrypt cardholder data must be stored encrypted and in the fewest possible locations. Secret and private keys must be stored in one (or more) of the following three ways:

1. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key within applicable applications.
2. Within a secure cryptographic device such as a HSM.
3. As at least two full-length key components or key shares, in accordance with an industry-accepted method.

Clear-text backups of encryption key components must be stored separately in tamper-evident packaging in a secure location.

**PCI Requirements Reference:**

**3.5.3** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times**:**

* + Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.
  + Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device).
  + As at least two full-length key components or key shares, in accordance with an industry-accepted method.

*Note: It is not required that public keys be stored in one of these forms.*

**3.6.3** Secure cryptographic key storage.

**3.5.4** Store cryptographic keys in the fewest possible locations.

### Key Changes and Destruction

An encryption key change is the process of generating a new key, decrypting the current production data and re-encrypting the confidential data with the new key. All data encryption keys must be changed after reaching the end of their cryptoperiod or when circumstances dictate a change to maintain encryption or key integrity. The following dictates when a key change is required:

* End of cryptoperiod: Keys must be changed after having reached the end of their respective cryptoperiod. Considerations for defining the cryptoperiod include the strength of the underlying algorithm, size or length of the key, risk of key compromise, sensitivity of the data being encrypted and industry best practices and guidelines (for example, NIST Special Publication 800-57).
* Suspicious Activity: This change is driven by any activity related to the key process, which raises concern regarding the security of the existing key.
* Resource Change: Keys must be changed if a resource with knowledge of the keys terminates employment or assumes a new job role that no longer requires access to an encryption process.
* Technical Requirement: Keys must be changed if the key in place has become questionable due to a technical issue such as corruption or instability.
* Encryption keys no longer in service are to be disposed of in accordance with the process outlined in the Data Retention and Disposal Policy.

**PCI Requirements Reference:**

**3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 80057).

**3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.

## Transmission over Un-Trusted Networks

Confidential and sensitive information must be encrypted during transmission over networks in which is it easy and common for the data to be intercepted, modified or diverted. Examples of strong encryption that is acceptable are:

* Transport Layer Security (TLS version 1.2)
* Internet Protocol Security (IPSec)

*Examples of insecure protocols are FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.*

Where SSL and early TLS (version 1.0 and sometimes 1.1, depending on use and implementation) is used, %Company% will need to comply with the additional requirements in Appendix A2 in the PCI DSS.

**PCI Requirements Reference:**

**4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

* Only trusted keys and certificates are accepted.
* The protocol in use only supports secure versions or configurations.
* The encryption strength is appropriate for the encryption methodology in use

*Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*

### Email Transmission of Confidential Information

Confidential and sensitive information is never to be sent unencrypted through email. Employees, with a valid business justification, must be issued email encryption software by the Information Security Team.

**PCI Requirements Reference:**

**4.2** Never send unprotected PANs by end-user messaging technologies (for example, email, instant messaging, SMS, chat, etc.).

### Encryption of Wireless Networks

All wireless networks in use at %Company% facilities must be protected through secure data encryption by industry best practice; minimum standards are WPA or WPA2. Wired Equivalent Privacy (WEP) is expressly prohibited. Under no circumstances should the encryption strength be configured to be less than 128 bits. Wireless encryption keys will be changed every ninety (90) days or whenever an administrator with knowledge of the keys is terminated.

**PCI Requirements Reference:**

**4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

## Non-console and Remote Administrative Access

All non-console (including remote) administrative access is encrypted using strong cryptography as referred to in the PCI DSS, using industry-recognized protocols with appropriate key strengths and key management (clarified in section 11.3). Clear-text protocols such as HTTP and Telnet are not permitted to be used when encrypting non-console access. The system is configured to invoke strong cryptography before any administrator’s password is requested.

**PCI Requirements Reference**:

**2.3** Encrypt all non-console administrative access using strong cryptography.

# CRITICAL TECHNOLOGIES USAGE POLICY

## Policy Applicability

All users of critical technologies deployed on %Company% networks, whether employees or contractors, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer. Currently, “critical technologies” include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, and Internet usage within the %Company% computing environment. This policy will be modified in the future to include any new “critical technologies” used.

**PCI Requirements Reference:**

**12.3** Develop usage policies for critical technologies and define proper use of these technologies.

## Approval

The Information Security Team must explicitly approve any use or deployment of critical technologies by job function role or on an individual basis. For general user application, this includes: dial-in modem access, personal modem deployment, and wireless network access. These approvals must be documented on the user’s Authorization Request Form (Appendix B - A model form is shown illustrating the minimum data to be captured electronically or on hard copy.

**PCI Requirements Reference:**

**12.3.1** Explicit approval by authorized parties

## Authentication

User authentication mechanisms, where possible, must be integrated into the current %Company% authentication systems. All device use must be authenticated at minimum with username and password or other authentication item (for example, token). Under no circumstances may the user authentication requirements be less strict than currently defined policies and procedures (e.g., complex passwords, password change interval, etc.).

All remote access (including general users, administrators, and vendors (for support or maintenance)) to the %Company% network using these technologies must be authenticated via a strong multi-factor authentication scheme approved by the Information Security Team.

All non-console and remote administrative access to the %Company% CDE must be authenticated via a strong multi-factor authentication scheme approved by the Information Security Team.

**PCI Requirements Reference:**

**8.3** Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

**8.3.2** Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity’s network.

## Device Inventory

All approved user devices (personal modems and wireless network interfaces) must be noted on the Critical Technologies Device Inventory (Appendix K A model form is shown illustrating the minimum data to be captured electronically or on hard copy. All approved users of these technologies must be noted on the Critical Technologies User List (Appendix L A model form is shown illustrating the minimum data to be captured electronically or on hard copy. Users that must be documented include:

* Wireless network users
* Personal modem possessors
* Employees with dial-in access
* Vendors with dial-in access

**PCI Requirements Reference:**

**12.3.3** A list of all devices and personnel authorized to use the devices.

**11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification.

## Device Identification

All personal modems and wireless access points must be labeled with the device owner, contact information and device purpose.

**PCI Requirements Reference:**

**12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)

## Acceptable Use

Acceptable use of %Company% critical technologies are subject to the same guidelines and restrictions put forth in the Security Awareness and Acceptable Use Policy (Appendix A).

**PCI Requirements Reference:**

**12.3.5** Acceptable uses for the technology.

## Permitted Locations

The Information Security Team must authorize the placement of any wireless access points and dial-in modems. Dial-in modems are typically limited to the data center. Wireless access points are normally placed in the ceiling plenum. The use of these devices must be logged according to the Critical Technologies Device Inventory (Appendix K A model form is shown illustrating the minimum data to be captured electronically or on hard copy) and Critical Technologies User List (Appendix L A model form is shown illustrating the minimum data to be captured electronically or on hard copy.

**PCI Requirements Reference:**

**12.3.6** Acceptable network locations for the technologies

## Approved Products

Only Information Security Team approved devices may be deployed into the %Company% network. The use of these devices must be logged according to the Critical Technologies Device Inventory (Appendix K) and Critical Technologies User List (Appendix L A model form is shown illustrating the minimum data to be captured electronically or on hard copy)

**PCI Requirements Reference:**

**12.3.7** A list of company-approved products.

## **Session Disconnect**

All remote-access technologies must be configured to automatically disconnect sessions after thirty (30) minutes of inactivity.

**PCI Requirements Reference:**

**12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity

## Vendor Connections

Dial-in modems, systems and accounts used solely for the purpose of vendor maintenance and support must remain disconnected and/or disabled until required. Activating these remotes access paths requires approval from the Information Security Team or established problem management procedures and they must be disabled immediately after use.

**PCI Requirements Reference:**

**12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use

## Credit Card Data Access

If any credit card data is available through remote dial-in modem connections special precautions must be taken. The following are prohibited:

* Storage of the company information onto local hard drives, floppy disks, and other media is prohibited.
* Cut, paste, and print functions of remote PCs is prohibited for the duration of the connection.

**PCI Requirements Reference:**

**12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

# SOFTWARE DEVELOPMENT POLICY

## Development Environment

A test/development environment, **separate from the production environment**, must be used to test all new software. If the network has network connectivity with the production %Company% network, access controls must be in place to enforce the separation.

Production cardholder data will not be used for testing and development purposes without being sanitized. Test personnel should make every effort to use mock data only for testing on non-production systems and software. If it is determined that production card holder data must be used in testing, the Security Council must review and approve the business justification, the testing window will have as short a duration as possible, all PCI controls must be enforced on the systems under test, and the Security Council must be notified of test results, and verification that production data has been scrubbed after close of testing window.

All test data, custom application accounts, usernames and passwords must be removed at the conclusion of testing, and in all cases before software becomes active. All code promotion to the production environment will be accomplished by the System Administrators. Under no circumstances will the Development Department have full time read/write access to production applications or data. Under emergency situations developers may assist in troubleshooting utilizing an Emergency ID described in section *2.3 Information Security Team Responsibilities.*

**PCI Requirements Reference:**

**6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers

**6.4** **Audit procedure:** Examine policies and procedures to verify the following are defined:

* + Development/test environments are separate from production environments with access control in place to enforce separation.
  + A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.
  + Production data (live PANs) are not used for testing or development.
  + Test data and accounts are removed before a production system becomes active.
  + Change control procedures related to implementing security patches and software modifications are documented.

## Secure Software Development Procedures

### Development Life-Cycle

Internal and 3rd party development of proprietary software must utilize industry recognized best practices for software development such as described at [http://cwe.mitre.org/top25/](http://cwe.mitre.org/top25/%20) . Security checks and control measures must be considered throughout the development life-cycle.

The high level overview of the security measures taking place within each phase of the %Company% development process are as follows:

* Requirements Analysis – developers should determine whether application requirements are inherently insecure.
* Design – application components must be planned in a manner consistent with data and network security.
* Development – developers must consider all application vulnerabilities (i.e.: memory bound issues, privilege and access bypass, etc.).
* QA Implementation - implementation must not compromise security controls already in place, or introduce new vulnerabilities.
* QA Testing - in addition to functional and efficiency testing, all security features of the application must be tested.
* Documentation – all application feature and implementation documentation must include direction on proper security configurations.
* Production Implementation – implementation must not compromise security controls already in place, or introduce new vulnerabilities.
* Production Testing – in addition to functional and efficiency testing, all security features of the application must be tested.
* Maintenance – all future application maintenance should not compromise security controls already in place, or introduce new vulnerabilities.
* Code changes – all future code changes must be reviewed by individuals other than the originating author. The reviewer must have adequate knowledge about code-review techniques and secure coding practices.

**PCI Requirements Reference:**

**6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:

* + In accordance with PCI DSS (for example, secure authentication and logging)
  + Based on industry standards and/or best practices.
  + Incorporating information security throughout the software-development life cycle

**6.3.2** Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:

* + Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.
  + Code reviews ensure code is developed according to secure coding guidelines
  + Appropriate corrections are implemented prior to release.
  + Code-review results are reviewed and approved by management prior to release.

### Web-based Applications

In addition to the Development Life-Cycle security measures that take place throughout the application development life-cycle, special care should be given to %Company%’s applications that are web-based. All %Company%’s developers will receive training on secure coding practices at least annually. All development must be done taking the OWASP guidelines into account, located at <http://www.owasp.org>. Specifically, the following vulnerabilities must be considered and checked for during the Code Review and Testing phases:

* Unvalidated Input
* Malicious Use of User IDs
* Malicious Use of Account Credentials and Session Cookies
* Broken authentication and session management
* Cross-Site Request Forgery (CSRF)
* Cross-Site Scripting
* Buffer Overflows
* SQL Injection and other Command Injection Flaws
* Error Handling Flaws
* Insecure cryptographic storage
* Denial of Service
* Insecure Configuration Management
* Insecure Direct Object references
* All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).

Annually, and whenever significant modifications have taken place, all web-based applications will be put through an application-specific penetration test. All custom code is to be reviewed by an organization that specializes in application security or an application layer firewall in front of web-facing applications.

**PCI Requirements Reference:**

**6.5** Address common coding vulnerabilities in software-development processes as follows:

* + Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
  + Develop applications based on secure coding guidelines.

**6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

**6.5.2** Buffer overflows

**6.5.3** Insecure cryptographic storage

**6.5.4** Insecure communications

**6.5.5** Improper error handling

**6.5.6** All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).

**6.5.7** Cross-site scripting (XSS)

**6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).

**6.5.9** Cross-site request forgery (CSRF)

**6.5.10** Broken authentication and session management.

**6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

* Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
* Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

### Credit Card Informational and Processing Applications

All %Company% proprietary or custom applications dealing with the processing or retrieval of cardholder information must be configured in a manner, which masks or truncates the displayed PAN. If the PAN is to be masked only the first 6 and last 4 digits may remain displayed. If the application is designed for a specific purpose in which the full PAN must be displayed, approval must be given by the Information Security Team. All the roles defined in Appendix Q2, that need access to displays of more than the first 6 and last 4 digits (includes full PAN), are listed in Appendix Q3 together with a business justification. All roles not specifically authorized in Appendix Q3 may only see masked PANs.

**PCI Requirements Reference:**

**Audit Procedure 3.3.a** Examine written policies and procedures for masking the display of PANs to verify:

* + A list of roles that need access to displays of more than the first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access.
  + PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.
  + All roles not specifically authorized to see the full PAN must only see masked PANs

# INCIDENT RESPONSE PLAN AND PROCEDURES

## Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day-to-day activities include, but are not limited to:

* Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
* Fraud – Inaccurate information within databases, logs, files or paper records
* Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals)
* Security event notifications (e.g., file integrity alerts, intrusion detection alarms, physical security alarms such as fire alarms, environmental alarms, natural disaster alerts)
* Addition of unauthorized devices (such as skimming devices, unauthorized wireless access points, unknown “free” USB-sticks)

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations. In all cases, every employee should report incidents per the instructions under 14.2 Incident Reporting unless they are assigned other activities within the incident response plan.

## Reporting and Incident Declaration Procedures

The Information Security Team should be notified immediately of any suspected or real security incidents involving %Company% computing assets, particularly any critical system. If it is unclear as to whether a situation should be considered a security incident, the Information Security Team should be contacted to evaluate the situation. With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by Information Security Team personnel or under the oversight of Information Security Team personnel, to assure the integrity of the incident investigation and recovery process. When faced with a potential situation you should do the following:

* If the incident involves a compromised computer system.
* Do not alter the state of the computer system.
* The computer system should remain on and all currently running computer programs left as is. Do not shutdown the computer or restart the computer.
* Immediately disconnect the computer from the network by removing the network cable from the back of the computer.
* Reporting the security incident.
* Contact the Information Security Team to report any suspected or actual incidents.
* No one should communicate with anyone outside of their supervisor(s) or the
* Information Security Team about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Information Security Team.
* Document any information you know while waiting for the Information Security Team to respond to the incident. This must include date, time, and the nature of the incident, if known. Any information you can provide will aid in responding in an appropriate manner.

**PCI Requirements Reference:**

**12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

* + Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
  + Specific incident response procedures
  + Business recovery and continuity procedures
  + Data backup processes
  + Analysis of legal requirements for reporting compromises
  + Coverage and responses of all critical system components
  + Reference or inclusion of incident response procedures from the payment brands.

**11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected.

## Incident Severity Classification

The Information Security Team will first attempt to determine if the security incident justifies a formal incident response.

In cases where a security incident does not require an incident response the situation will be forwarded to the appropriate area of IT to ensure that all technology support services required are rendered. The following descriptions should be used to determine what response the Information Security Department will take.

* Level 1 - One instance of potentially unfriendly activity (e.g., finger, unauthorized telnet, port scan, corrected virus detection, unexpected performance peak, etc.).
* Level 2 - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second Level 1 attack.
* Level 3 - Serious attempt or actual breach of security (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful buffer/stack overflow, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.) or a second Level 2 attack.
* Any Level 1 type incident occurring against systems storing sensitive or confidential data or originating from unauthorized internal systems is classified as a Level 2.

## Incident Response

### Typical Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls. The following actions should be taken by the Information Security Department once an incident has been identified and classified.

#### Level 1

Contain and Monitor

1. If possible, record the user, IP address and domain of intruder.
2. Utilize approved technology controls to temporarily or permanently block the intruder’s access.
3. Maintain vigilance for future break-in attempts from this user or IP address.

#### Level 2

Contain, Monitor and Warn

1. Collect and protect information associated with the intrusion.
2. Utilize approved technology controls to temporarily or permanently block the intruder’s access.
3. Research the origin of the connection.
4. Contact ISP and ask for more information regarding the attempt and intruder.
5. Research potential risks related to intrusion method attempted and re-evaluate for higher classification and incident containment, eradication, and recovery as described for Level 3 incident classifications.
6. Upon identification, inform malicious user of our knowledge of their actions and warn of future recriminations if attempt is repeated. If an employee is the malicious user management should work with Human Resources to address the Acceptable Use violation appropriately.

#### Level 3

Contain, Eradicate, Recover and perform Root Cause Analysis

1. If the incident involved credit card systems, the Acquirer and applicable card associations must be notified. See section 14.4.2 for more details.
2. Contain the intrusion and decide what action to take. Consider unplugging the network cables, applying highly restrictive ACL’s, deactivating or isolating the switch port, deactivating the user ID, terminating the user’s session/change password etc.
3. Collect and protect information associated with the intrusion via offline methods. In the event that forensic investigation is required the Information Security Team will work with legal and management to identify appropriate forensic specialists.
4. Notify management of the situation and maintain notification of progress at each following step.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research the origin of the connection.
7. Contact ISP and ask for more information regarding attempt and intruder, reminding them of their responsibility to assist in this regard.
8. Research potential risks related to or damage caused by intrusion method used.

### Credit Card Compromise – Special Response

For any incidents involving potential compromises of credit card information, the Information Security Team will use the following procedure:

1. Contain and limit the exposure. Conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
   1. Log all actions taken (e.g., bound notebook, video camera, etc).
   2. Utilize chain of custody techniques during all transfers of equipment and information related to the incident.
   3. Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
   4. Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the network cable, deactivate switch port, isolate to contained environment e.g. isolated VLAN). Utilize Disaster Recovery / Business continuity procedures to recover business processes.
   5. Preserve logs and electronic evidence.
   6. If using a wireless network, change SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised).
   7. Be on high alert and monitor all cardholder information systems.
2. Alert all necessary parties. Be sure to notify:
   1. Internal or External Incident Response or Forensics Team, if they are not already involved
   2. Merchant bank
   3. U.S. Secret Service (if PCI payment data is compromised)
3. Follow appropriate procedures for each card association which %Company% utilizes for credit card services.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact (650) 432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa’s “What to do if Compromised” documentation for additional activities that must be performed. That documentation can be found at <https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf>

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999\_MERC-Entire\_Manual.pdf.

American Express

Contact your relationship manager or call the support line at 1-800-528-4800 for further guidance.

Discover Card

Contact your relationship manager or call the support line at 1-800-347-3083 for further guidance.

JCB

Contact your relationship manager or call the support line at 1-213-896-3718 for further guidance.

**PCI Requirements Reference:**

**12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

* + Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
  + Specific incident response procedures
  + Business recovery and continuity procedures
  + Data backup processes
  + Analysis of legal requirements for reporting compromises
  + Coverage and responses of all critical system components
  + Reference or inclusion of incident response procedures from the payment brands.

### Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Information Security Team and all affected parties will meet to review the results of the investigation conducted under step 1, Section 14.4.3 of this document to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

**PCI Requirements Reference:**

**12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments

## Plan Testing and Training

At least once a year, a mock-incident will be initiated to facilitate testing of the current plan. The exact incident to be tested will be at the discretion of the Information Security Team. Once complete, a follow-up session, as detailed above, will be held. All %Company% employees that could have an active role within incident response will be part of the test process. Training regarding incident response responsibilities should be performed regularly to ensure employee’s readiness for test and actual incidents.

**PCI Requirements Reference:**

**12.10.2** Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.

**12.10.4** Provide appropriate training to staff with security breach response responsibilities

## Automated Security System Notifications

All automated intrusion detection systems within the %Company% environment, including intrusion detection sensors and file integrity checking systems, will be configured to automatically notify the Information Security Team of any potential compromises or attacks. An engineer with the Information Security Team must be available on a 24/7 basis to initiate the incident response plan if warranted.

**PCI Requirements Reference:**

**Audit Procedure 12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

**Audit Procedure 12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the incident response plan.

# IDENTIFICATION AND PHYSICAL AUTHENTICATION POLICY

## Employee and Visitor Requirements

All visitors are authorized before entering the office facility and provided with an ID badge that is clearly distinguishable from employee badges. Visitors to %Company%’s shared office facility must, at all times, clearly display their ID badges. It is every employee’s responsibility to keep watch for unknown persons or employees not displaying badges. Employees must escort visitors at all times within the office facility. A visitor log is maintained to record visitor activity within the different facilities and this log is retained for at least 3 months. Visitors are asked to surrender ID badges before leaving the facility. Onsite personnel’s ID badges and access mechanisms to the facility will be revoked immediately upon termination.

**PCI Requirements Reference:**

**9.2** Develop procedures to easily distinguish between onsite personnel and visitors, to include:

* + Identifying onsite personnel and visitors (for example, assigning badges)
  + Changes to access requirements
  + Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

**9.3** Control physical access for onsite personnel to sensitive areas as follows:

* + Access must be authorized and based on individual job function.
  + Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled

**9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained

**9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel

**9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration

**9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.

## Other Authentication Mechanisms Usage

A case when an entity uses smart card authentication for physical access:

%Company% uses smart cards to gain authorized physical access to the company’s premises. Each smart card is connected to individual accounts and never shared amongst multiple accounts. Employees must define their own four-digit string PIN-code when a smart card is issued to them the first time. The smart card does not gain access without the input of a PIN-code. Generic PIN-codes like 1111 and 1234 are not permitted. Some smart cards will gain employees access to all of the company’s premises, other smart cards cannot gain access to sensitive areas. This separation of access scope is determined by the employee’s role. All employees will have their smart cards either removed or disabled immediately following termination.

**PCI Requirements Reference:**

**8.6** Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.

Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

**7.1.3** Assign access based on individual personnel’s job classification and function.

**9.3** Control physical access for onsite personnel to sensitive areas as follows:

Access must be authorized and based on individual job function.

Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled

# LOGGING CONTROLS POLICY

## Events Logged

Automated audit trails must be implemented for all system components to reconstruct the following events:

* All user access to company information.
* All administrative actions utilizing userID’s with significant privileges above a general user (e.g. root, userID’s with Administrator group privilege, oracle, etc)
* Access, initialization, stopping, or pausing of audit log files
* Any user or administrator authentication attempts (both valid and invalid)
* Creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
* Creation or deletion of system-level objects
* Invalid logical access attempts

**PCI Requirements Reference:**

**10.2.1** All individual user accesses to cardholder data

**10.2.2** All actions taken by any individual with root or administrative privileges

**10.2.3** Access to all audit trails

**10.2.4** Invalid logical access attempts

**10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges

**10.2.6** Initialization, stopping, or pausing of the audit logs

**10.2.7** Creation and deletion of system-level objects.

## Event Log Structure

All system access event logs must contain at least the following information.

* User Identification
* Type of event
* Date and time of event
* Result of the event
* Originating location of the event
* The name of the affected data, system component or resource

**PCI Requirements Reference:**

**10.3** Record at least the following audit trail entries for all system components for each event:

**10.3.1** User identification

**10.3.2** Type of event

**10.3.3** Date and time

**10.3.4** Success or failure indication

**10.3.5** Origination of event

**10.3.6** Identity or name of affected data, system component, or resource.

## Log Security

All event logs must be collected in a centralized location or media that is difficult to alter and protected from unauthorized access. The viewing of such logs is to occur on a need only basis. The logs will be further protected by a file integrity monitoring system that alerts the Information Security Team upon unauthorized access.

**PCI Requirements Reference:**

**10.5** Secure audit trails so they cannot be altered.

**10.5.1** Limit viewing of audit trails to those with a job-related need

**10.5.2** Protect audit trail files from unauthorized modifications

**10.5.3** Promptly back-up audit trail files to a centralized log server or media that is difficult to alter

**10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

**10.5.5** Use file-integrity monitoring and change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

*The following section 17 only applies to entities that use card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale.*

# Protection of card-reading devices at point of sale

The company trains newly employed sales clerks to protect and inspect all card-reading devices. Sales clerks are asked to be on the lookout for suspicious behavior near point of sale terminals and report such behavior to management that will in turn contact the information security team. Inspections are made on a monthly basis or after any report of suspicious behavior.

**PCI Requirements Reference:**

**9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

## Training of Sales Clerks

Newly hired sales clerks are trained by senior sales clerks during the first 5 days of hire. The training contains the following:

* **Be on the look-out for any suspicious behavior around card-reading devices.** Suspicious behavior includes, but not limited to, unknown persons trying to open, attach devices or unplug card-reading devices.
* **Report any suspicious behavior to management**, that will in turn report to the security team.
* **Verify the identity of any third-party persons claiming to be repair or maintenance personnel**, prior to granting them access to modify or troubleshoot devices. The verification includes asking the person for job credentials and asking management for any scheduled maintenance. Calling the POS company is necessary if the two former actions did not provide adequate result.
* **How to inspect card reading devices**, which is defined in Section 17.2.
* **Not to install, replace or return devices** without verification from the security team.

**PCI Requirements Reference:**

**9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:

* Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
* Do not install, replace, or return devices without verification.
* Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
* Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

## Periodic Inspections of Card-Reading Devices

Card-reading devices should be periodically inspected by sales clerks once every 30 days or immediately after any report of suspicious behavior (The frequency of inspections will depend on factors such as location of the devices and whether the devices are attended or unattended). The inspection contains the following steps:

* The card-reading devices are compared to the list of point of sale devices in Appendix S, comparing the serial number of each device to make sure the device has not been stolen or substituted.
* The card-reading devices are also checked to see if the outer casing has been opened by checking if any of the stickers on the device openings have been broken.
* The devices are inspected to see if any attached components are present, like skimming devices.

**PCI Requirements Reference:**

**9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

# Risk-assessment process

A risk-assessment is performed annually or after any significant changes to the organizations environment. The Chief Technical Officer is responsible for the risk-assessment process and uses the ISO 27005 risk assessment methodology (other examples of risk-assessment methodologies include but are not limited to OCTAVE and NIST SP 800-30).

**PCI Requirements Reference:**

**12.2** Implement a risk-assessment process that:

* Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
* Identifies critical assets, threats, and vulnerabilities, and
* Results in a formal, documented analysis of risk.

*The following section 19 only applies to entities that are categorized as service providers. See PCI Security Standards Council (SSC) definition of a service provider and if it relates to the* *entity at* ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)).

# Additional PCI DSS service provider responsibilities

## Written Acknowledgment of Responsibility from the Entity

The %Company% (being a service provider) must acknowledge in writing that they are responsible for the security of cardholder data that they store, process or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.

**PCI Requirements Reference:**

**12.9** Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.

## Remote Access to Customers

Remote access to customer premises is authenticated using unique passwords for each customer. The passwords follow the same standard as defined in section 4.5.

**PCI Requirements Reference:**

**8.5.1** Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

*Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*

*The following section 20 applies only to entities who make use of external service providers.*

# Service Provider management

## Responsibility Allocation and Compliance Monitoring

%Company% withholds documented information about which requirements are management by the entity and which requirements are managed by external service providers. (24 Solutions provides a matrix for this purpose). The entity must also monitor the PCI DSS compliance status of the service provider at least annually and will document the current status in Appendix T – List of Service Providers.

**PCI Requirements Reference:**

**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.

## Written Acknowledgment of Responsibility from the Service Provider

A written acknowledgement must exist between the entity and the service provider that states the responsibilities of the service provider. The service provider is responsible for all the requirements defined in the section above, as well as the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the entity, or to the extent that they could impact the security of the entities’ CDE.

**PCI Requirements Reference:**

**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.

## Service Provider and Entity Engagement and Compliance Monitoring

The entity must establish a process prior to engaging with a service provider and must perform due diligence in this process, meaning that the entity has exercised an appropriate level of caution or investigation prior to acting or making the decision to engage with a service provider. The process should first include a risk analysis from the Chief Technical Officer. Examples of considerations that the entity should investigate include the provider’s reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their PCI DSS compliance and what evidence they provide, etc.

**PCI Requirements Reference:**

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

# Inventory of system components

%Company% maintains an inventory of system components in scope for PCI DSS. Any network component, server, or application included in or connected to the cardholder data environment is listed in Appendix R.

**PCI Requirements Reference:**

**2.4** Maintain an inventory of system components that are in scope for PCI DSS.

# Appendix A – Security Awareness and Acceptable Use Policy

**%Company% Security Awareness and Acceptable Use Policy**

**Overview**

The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity. %Company% is committed to protecting all employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of %Company%. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every %Company% employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

**Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at %Company%. These rules are in place to protect the employees and %Company%. Inappropriate use exposes %Company% to risks including virus attacks, compromise of network systems and services, and legal issues.

**Scope**

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at %Company%, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by %Company%.

**Policy**

**General Use and Ownership**

1. While network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of %Company%. Because of the need to protect the network, management cannot guarantee the confidentiality of employee’s personal information stored on any network device belonging to %Company%.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within %Company% may monitor equipment, systems and network traffic at any time.
5. %Company% reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

**Security and Proprietary Information**

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: credit card information, company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed every 90 days.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or lock (control-alt-delete for Windows users) when the host will be unattended.
5. Use encryption of information in compliance with Information Technologies' Security Policies.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the corporate security standards, including personal firewalls.
7. Postings by employees from a %Company% email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of %Company%, unless posting is in the course of business duties.
8. All hosts used by the employee that are connected to the %Company% Internet/Intranet/Extranet, whether owned by the employee or %Company%, shall be continually executing approved virus-scanning software with a current virus database.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

**Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of %Company% authorized to engage in any activity that is illegal under local, national or international law while utilizing %Company%-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

**System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by %Company%.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which %Company% or the end user does not have an active license is strictly prohibited. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all %Company% properties is prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a %Company% computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any %Company% account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, %Company% employees to parties outside %Company%.

**Email and Communications Activities**

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within %Company%'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by %Company% or connected via %Company%'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Definitions**

*Spam* Unauthorized and/or unsolicited electronic mass mailings.



Employee/Contractor/Third Party Signature Date



Printed Name Date of Security Awareness Training

# Appendix B – Authorization Request Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART I (To be filled out by the Requestor or Requestor’s Supervisor)** | | | | | |
| 1. Type of Request:  □ Initial □ Modification □Deletion | | | 2. Office: | | |
| 3. Name (*Last, First, MI*): | | | 4. Title: | | |
| 5. Organization: | 6. Phone Number: | | 7. Start Date: | | 8. Stop Date: |
| 9. Requestor’s Signature: | | | | | 10. Date: |
| **PART II (To be filled out by the Requestor's Supervisor)** | | | | | |
| 11. Profile (Check the appropriate standard profile(s)):  □ Basic User □ System Engineer □ Security Engineer □ Key Custodian □ Network Engineer □ Software Engineer  □ Security Manager □ Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 12. ID Badge:  □ Visitor □Building □ Internal Doors □ Data Center | | | 13. System Type:  □ Windows □ Unix □Wireless Use  □ Modem Use □ Modem Possession | | |
| 14. Justification for Accesses: | | | | | |
| 15. Supervising Official Certification:  Name Phone Signature Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| **PART III (To be completed by the Chief Technical Officer)** | | | | | |
| 16. Background Check Completed:  □ Yes □ No | | 17. Performed By: | | 18. Date Granted: | |
| 19. Security Officer Official Certification:  Name Phone Signature Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| **PART IV (To be completed by System Administrator)** | | | | | |
| 20. User ID: | | 21. Date User Notified: | | 22. Date Deleted: | |
| 23. System Engineer Official Certification:  Name Phone Signature Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |

# Appendix C – Change Request Form

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PART I (To be filled out by the Lead Requestor)** | | | | | |
| 1. Type of Request:  □ Initial Request □ Updated Request | | | 2. Office: | | |
| 3. Name (Last*, First, MI*): | | | 4. Phone Number: | | 5. Date: |
| 6. Type of Change:  □ New Implementation □ Repair □ Removal □ Emergency □ Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 7. Description of Change: | | | | | |
| 8. Recurring Change:  □ Yes, add to calendar □ No | | | 9. Requested Implementation Window: | | |
| 10. Systems Affected by Change: | | 11: Users Affected by Change: | | 12. Documentation Attached:  □ Test Plan  □ Back out Plan | |
| 13. Resources That May be Affected by Change:  □ Customer(s) □ Internal Dept. □ Other  Explain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | 14. Criticality of Change:  □ High □Medium □ Low  Explain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| **PART II (To be completed by Management)** | | | | | |
| 15.Review Date: | 16. Review Participants: | | | | |
| 17. Test Plan Review:  □ Acceptable □ Further Action is Required | | | 18. Back Out Plan Review:  □ Acceptable □ Further Action is Required | | |
| 19. Resource Review:  □ Acceptable □ Further Action is Required | | | 20. Schedule Review:  □ Acceptable □ Further Action is Required | | |
| 21. Comments: | | | | | |
| **PART III (To be completed by Management after approval)** | | | | | |
| 22. Approval Date: | | | 23. Approved Implementation Date: | | |
| 24. Supervising Official Certification:  Name Phone Signature Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |

# Appendix D – Media Inventory Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Location** | **Name** | **Signature** | **Acceptable** |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |
|  |  |  |  | □ Yes □ No |

# Appendix E – Permitted Network Services and Protocols

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Firewall** | **Source** | **Destination** | **Ports** | **Protocols** | **Business Justification** |
| *Internet* | *Internet* | *Web Farm* | *80* | *HTTP* | *Public access to DMZ web servers* |
| *Internet* | *Internet* | *Web Farm* | *443* | *HTTPS* | *Secure member and payment access to DMZ web servers* |
| *Internet* | *Internet* | *VPN Concentrator* | *500* | *IPSEC* | *Remote user VPN* |
| *Internal* | *VPN Concentrator* | *File Servers* | *135*  *137*  *139* | *MS* | *Remote user file access* |
| *Internal* | *Web Farm* | *Database Cluster* | *1433* | *SQL* | *Data population from web* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Appendix F – System Configuration Standards

**PCI Requirements Reference:**

**2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

**2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to:

* + Center for Internet Security (CIS)
  + International Organization for Standardization (ISO)
  + SysAdmin Audit Network Security (SANS) Institute
  + National Institute of Standards Technology (NIST).

**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release

## F.1 Windows Systems

### F.1.1 Windows Installation

The following general install procedures will be followed for all %Company% Microsoft Windows-based system deployments:

1. Install operating system.
2. Update all operating system software per vendor recommendations.
3. Configure operating system parameters according to build document (OS hardening).
4. Install system specific applications and software according to a System Configuration Record, if one exists. Otherwise, install necessary software.
5. Update all application software per vendor recommendations.
6. Configure application parameters according to build document (application hardening).
7. Complete system specific System Configuration Record and maintain on file.

### F.1.2 Windows 2000 Server

The system hardening document located at the following link will be used as the basis for all %Company% Windows 2000 Server network system deployments:

Windows 2000 Server Benchmark Level-2 version 2.2.1

<http://www.cisecurity.org/tools2/win2000/W2K-Srv-v2.2.1.pdf>

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.1.3 Windows 2000 Professional

The system hardening document located at the following link will be used as the basis for all %Company% Windows 2000 Professional network system deployments:

Windows 2000 Professional Benchmark Level-2 version 2.2.1

<http://www.cisecurity.org/tools2/win2000/W2K-Pro-v2.2.1.pdf>

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.1.4 Windows NT

The system hardening document located at the following link will be used as the basis for all %Company% Windows NT network system deployments:

Windows NT Level 1 Benchmark version 1.0.5

http://www.cisecurity.org/tools2/win2000/CIS-WinNT-v1.0.5.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.1.5 Windows 2003 Server Domain Controller

The system hardening document located at the following link will be used as the basis for all %Company% Windows 2003 Server Domain Controller network system deployments:

Windows 2003 Server Domain Controller Benchmark version 1.2

http://www.cisecurity.org/tools2/win2000/CIS\_Win2003\_DC\_Benchmark\_v1.2.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.1.6 Windows 2003 Server Member Server

The system hardening document located at the following link will be used as the basis for all %Company% Windows 2003 Server Member Server network system deployments:

Windows 2003 Server Member Server Benchmark version 1.2

http://www.cisecurity.org/tools2/win2000/CIS\_Win2003\_MS\_Benchmark\_v1.2.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.1.7 Windows XP Professional

The system hardening document located at the following link will be used as the basis for all %Company% Windows XP Professional network system deployments:

Windows XP Professional Benchmark version 2.01

http://www.cisecurity.org/tools2/win2000/CIS\_WindowsXP\_Benchmark\_v2.01.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

## F.2 UNIX Systems

### F.2.1 UNIX Installation

The following general install procedures will be followed for all %Company% UNIX-based system deployments:

1. Install operating system.
2. Update all operating system software per vendor recommendations.
3. Configure operating system parameters according to build document (OS hardening).
4. Install system specific applications and software according to a System Configuration Record, if one exists. Otherwise, install necessary software.
5. Update all application software per vendor recommendations.
6. Configure application parameters according to build document (application hardening).
7. Complete system specific System Configuration Record and maintain on file.

### F.2.2 HP-UX

The system hardening document located at the following link will be used as the basis for all %Company% HP-UX network system deployments:

HP-UX Benchmark version 1.3.1

http://www.cisecurity.org/tools2/hpux/CIS\_HPUX\_Benchmark\_v1.3.1.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.2.3 Linux

The system hardening document located at the following link will be used as the basis for all %Company% Linux network system deployments:

Red Hat Enterprise Linux Benchmark version 1.0.4

<http://www.cisecurity.org/tools2/linux/CIS_RHLinux_Benchmark_v1.0.5.zip>

SuSE Linux Benchmark version 1.0

<http://www.cisecurity.org/tools2/linux/CIS_SUSE_Linux_Benchmark_v1.0.pdf>

Slackware Linux Benchmark version 1.1

http://www.cisecurity.org/tools2/linux/CIS\_Slackware\_Linux\_Benchmark\_v1.1.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.2.4 FreeBSD

The system hardening document located at the following link will be used as the basis for all %Company% FreeBSD network system deployments:

FreeBSD Benchmark version 1.0.5

http://www.cisecurity.org/tools2/freebsd/CIS\_FreeBSD\_Benchmark\_v1.0.5.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.2.5 Solaris

The system hardening document located at the following link will be used as the basis for all %Company% Solaris network system deployments:

Solaris Benchmark (for Solaris 2.5.1 and later releases) version 1.3.0

<http://www.cisecurity.org/tools2/solaris/CIS_Solaris_Benchmark_v1.3.pdf>

Solaris Benchmark (for Solaris 10) version 2.1.1 and do-backup.sh script

http://www.cisecurity.org/tools2/solaris/CIS\_Solaris10\_Benchmark\_v2.1.1.tar.gz

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

## F.3 Network Devices

### F.3.1 Network Device Installation

The following general install procedures will be followed for all %Company% network device deployments:

1. Update all operating system or firmware software per vendor recommendations.
2. Configure device parameters according to build document (device hardening).
3. Disable unencrypted management interfaces (e.g. telnet) and enable encrypted management interfaces (SSH)
4. Complete system specific System Configuration Record and maintain on file.

### F.3.2 Cisco IOS

The system hardening document located at the following link will be used as the basis for all %Company% Cisco IOS-based network system deployments:

Cisco IOS Benchmark version 2.1

<http://www.cisecurity.org/tools2/cisco/cisco-ios-router-benchmark.pdf>

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.3.3 Cisco PIX Firewall

The system hardening document located at the following link will be used as the basis for all %Company% Cisco PIX network system deployments:

Cisco PIX Benchmark version 1.0

<http://www.cisecurity.org/tools2/cisco/cisco-pix-benchmark.pdf>

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.3.4 Wireless Access Point

The following configuration steps are to be used as the basis for all %Company% Wireless Access Point (WAP) system deployments:

1. Change the default SSID (Service Set ID or network name).
2. Disable the SSID broadcast.
3. Change the default password for the WAP’s Administrator account.
4. Enable MAC Address Filtering.
5. Limit the number of allowed connections to the minimum needed.
6. Disable DHCP.
7. Enable the highest encryption possible: WEP 128-bit (802.11b) or WPA with TKIP or AES (802.11g).
8. Disable mixed "b" and "g" environment.
9. Change the default IP address.
10. Enable the WAP's firewall.
11. Disable the ‘DMZ’ feature.
12. Disable the Remote Management feature.
13. Disable Universal Plug 'n' Play (UPnP) feature.
14. Place the WAP near the center of buildings and avoid placing near exterior walls.

While configuring the system, all exceptions to this standard must be noted on the completed System Configuration Record.

### F.4 Server Applications

### F.4.1 Application Installation

The following general install procedures will be followed for all %Company% server application deployments:

1. Install necessary software.
2. Update application software per vendor recommendations.
3. Configure application parameters according to build document (application hardening).
4. Update system specific System Configuration Record and maintain on file.

### F.4.2 Oracle Database

The system hardening document located at the following link will be used as the basis for all %Company% Oracle database deployments:

Oracle Benchmark (for Oracle version 8i) version 1.2

<http://www.cisecurity.org/tools2/oracle/CIS_Oracle_Benchmark_v1.2.pdf>

Oracle Benchmark (for Oracle version 9i/10g) version 2.0

http://www.cisecurity.org/tools2/oracle/CIS\_Oracle\_Benchmark\_v2.0.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

### F.4.3 Apache Web Server

The system hardening document located at the following link will be used as the basis for all %Company% Apache web server deployments:

Apache Web Server Benchmark version 1.0

<http://www.cisecurity.org/tools2/apache/CIS_Apache_Benchmark_v1.0.pdf>

While configuring the system, all exceptions to this hardening standard must be noted on the completed System Configuration Record.

# Appendix G – System Configuration Record

|  |  |  |  |
| --- | --- | --- | --- |
| **General System Information** | | | |
| 1. System Name: | 2. System Purpose: | | 3. Build Date: |
| 4. Build Engineer: | | 5. Comments: | |
| **IP Information** | | | |
| 6. IP Address: | 7. Subnet Mask: | | 8. Default Gateway: |
| 9. DNS/WINS Entries: | 10. Domain: | | 11. Other Settings: |
| **Operating System** | | | |
| 12. Operating System: | | 13. Version: | |
| 14. Date Patched to: | | 15. Patch Exceptions: | |
| 16. System Hardened:  □ Yes □ No | | 17. Hardened by Which Standard: | |
| 18. Hardening Exceptions:  Document Number Reason for Exception  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| **Application (Attach additional Sheets for Other Entries)** | | | |
| 19. Operating System: | | 20. Version: | |
| 21. Date Patched to: | | 22: Patch Exceptions: | |
| 23. System Hardened:  □ Yes □ No | | 24. Hardened by Which Standard: | |
| 25. Hardening Exceptions:  Document Number and Reason for Exception  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| **Notes** | | | |
| 26. Additional Comments / Notes: | | | |

# Appendix H – Backup Media Transfer Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Container #** | **Courier Signature** | **Management Signature** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix I – Encryption Key Custodianship Form

Encryption key custodians are those person(s) delegated the responsibility of managing, handling and protecting access to %Company% encryption keys. Custodians are responsible for the safety and integrity of keys in their custody. The custodian has responsibility to:

* Implement all encryption key controls as specified by the Information Security Department and documented in information security policies and procedures. Provide safeguards for encryption keys during generation, loading and storage.
* Administer access to the encryption keys and make provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to these keys.
* Control access and secrecy of the combination of the safe containing the clear-text encryption keys.
* Appropriate and complete the Encryption Key Management Log for any activity involving cryptographic keys.
* Participation in the encryption key generation, distribution, change, and destruction processes.



Key Custodian Signature Date



Printed Name

# Appendix J – Encryption Key Management Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Time** | **Key** | **Custodian and Witness** | **Reason** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix K – Critical Technologies Device Inventory

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Device Name** | **Location** | **Owner / Administrator** |
| *Personal Modem* | *N/A* | *Call Center PC (IBM\_PCJSMITH)* | *John Smith* |
| *Dial-in Modem* | *RAS1* | *Datacenter – RAS Server* | *Administrator Doug* |
| *Dial-in Modem* | *RAS2* | *Datacenter – RAS Server* | *Administrator Doug* |
| *Dial-in Modem* | *PBX* | *Datacenter – PBX Switch* | *Vendor* |
| *Wireless Router* | *WAP1* | *Call Center* | *Administrator Suzy* |
| *Wireless Interface* | *N/A* | *Call Center PC (IBM\_PCJSMITH)* | *John Smith* |
| *Wireless Interface* | *N/A* | *Call Center PC (IBM\_PCJDOE)* | *Jane Doe* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Device** | **User** | **Justification / restrictions** |
| *Call Center PC Modem* | *John Smith* | *Back-up for network outage* |
| *RAS1* | *Jimmy John* | *Employee Remote Access* |
| *RAS1* | *Jack Jackson* | *Employee Remote Access* |
| *RAS1* | *Janis Jameson* | *Employee Remote Access* |
| *RAS2* | *Christopher Caine* | *Employee Remote Access* |
| *RAS2* | *Lambert Lake* | *Employee Remote Access* |
| *PBX* | *Technotronic Systems* | *Vendor support – 8-5 Only Connect only when needed* |
| *WAP1* | *John Smith* | *Network Access* |
| *WAP1* | *Mary Samsonite* | *Network Access* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix L – Periodic Operational Security Procedures

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Task** | **Daily** | | **Weekly** | **Monthly** | **Quarterly** | **Annually** | **As Required** |
| **Security Policy** | | | | | | | |
| Enterprise Risk Analysis | |  |  |  |  | X |  |
| Policy/standards review | |  |  |  |  | X |  |
| Security awareness orientation | |  |  |  | X |  |  |
| **Organizational Security** | | | | | | | |
| Distribute Security Alerts | |  |  |  |  |  | X |
| Review security policy exceptions compliance | |  |  |  | X |  |  |
| **Asset Classification and Control** | | | | | | | |
| Review system access controls | |  |  |  | X |  |  |
| Review access request approvals & audit trail | |  |  |  | X |  |  |
| Audit disposal of data and media | |  |  |  | X |  |  |
| **Personnel Security** | | | | | | | |
| New employee security orientation | |  |  |  |  | X | X |
| Process employee data access requests | |  |  |  |  |  | X |
| Audit terminated employee samples for system, network, application access | |  |  |  | X |  |  |
| Incident response team meeting | |  |  | X |  |  |  |
| **Physical and Environmental Security** | | | | | | | |
| Physical walkthrough of facility, work areas and data center | |  | X |  |  |  |  |
| Review compliance of data center access & visitor logs | |  |  |  | X |  |  |
| **System Security** | | | | | | | |
| Review intrusion detection (IDS/IPS) logs | | X |  |  |  |  |  |
| File Integrity Scans | | X |  |  |  |  |  |
| Scan desktops for vulnerabilities and security compliance | |  |  |  | X |  |  |
| Scan servers and network for vulnerabilities and security compliance | |  |  |  | X |  |  |
| External application scans | |  |  |  | X |  |  |
| Use a Wireless Analyzer to detect wireless devices in use | |  |  |  | X |  |  |
| Review all security and event logs | | X |  |  |  |  |  |
| Perform network-layer and application-layer penetration testing | |  |  |  |  | X |  |

# Appendix M – NEW EMPLOYEE CARD

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job Classification: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Start Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Systems Access: □ Office Systems – level \_\_\_\_\_\_\_\_\_\_\_\_\_\_

□ VPN Access

□ %Company% Application Access – level \_\_\_\_\_\_\_\_\_\_\_\_\_\_

□ Database Access – level \_\_\_\_\_\_\_\_\_\_\_\_\_\_

□ Server Access – level \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Management Approval (signature): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Management Approval (name and title): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix N – Inventory of System Components

|  |  |  |  |
| --- | --- | --- | --- |
| Component ID # | Component Name | Component Type | Function Description |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*The following Appendix O only applies to entities that use card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale.*

# Appendix O – List of Card-Reading Devices at POS

|  |  |  |  |
| --- | --- | --- | --- |
| Model | Location(address) | Date Acquired | Serial #/Unique Identifier |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**PCI Requirements Reference:**

9.9.1 Maintain an up-to-date list of devices. The list should include the following:

* Make, model of device
* Location of device (for example, the address of the site or facility where the device is located)
* Device serial number or other method of unique identification.

# Appendix P – List of Service Providers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service Provider Name | Service Description | PCI DSS Compliance Status | Service Provider Contact Information | Date of Last Update |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**PCI Requirements Reference:**

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

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

# Appendix Q1 – Role Assignment List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | User ID | Job Classification | Role Assigned | Signature from Security Team |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix Q2 – Role Specification List

|  |  |  |
| --- | --- | --- |
| Role | Data Resource Access Needs | Level of Privilege |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix Q3 – Role Specification for PAN Visibility

|  |  |  |
| --- | --- | --- |
| Role | More than 6 first/last 4 Digit PAN Visibility Access (Y/N) | Business Justification |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |