Your Logo
Will Be
Placed Here

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) CYBERSECURITY POLICY & STANDARDS

ACME Business Consulting, LLC

PCI DSS
Information Security Policy & Standards

Table of Contents

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) Cybersecurity Policy & Standards document provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program for PCI DSS v3.2.1 compliance at ACME Business Consulting, LLC (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every ACME user who interacts with data and information systems. Therefore, it is the responsibility of every user to know this policy and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of cardholder data and information systems. This also includes against accidental loss or destruction.

POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Cybersecurity documentation is comprised of six (6) main parts:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.

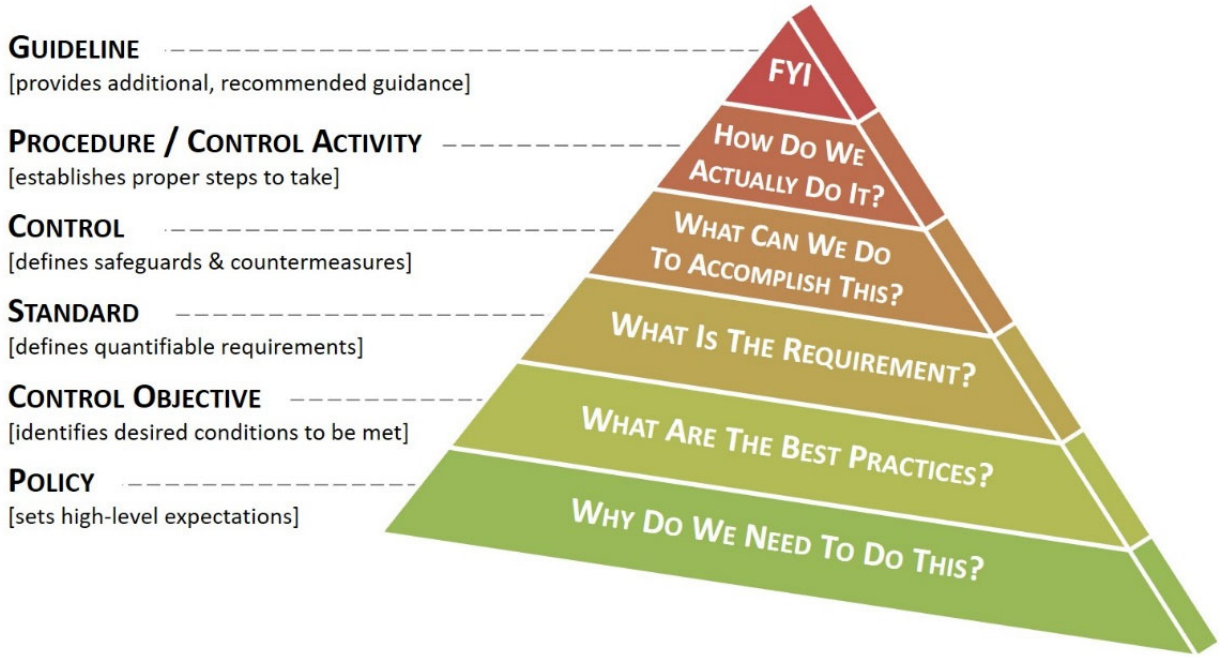

Figure 1: Cybersecurity Documentation Hierarchy

PURPOSE

The purpose of this document is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of ACME's payment card data and related information systems.
- Protecting ACME, its employees, and its clients from illicit use of ACME's information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support ACME's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related Cybersecurity risks.

The formation of the policy is driven by many factors, with the key factor being a risk. This policy sets the ground rules under which ACME shall operate and safeguard its data and information systems to both reduce risk and minimize the effect of potential incidents.

This policy, including related standards and procedures, are necessary to support the management of information risks in daily operations. The development of policy provides due care to ensure ACME users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of ACME data.

Scope & Applicability

This policy and its related standards, procedures, and guidelines apply to all ACME data, information systems, activities, and assets owned, leased, controlled, or used by ACME, its agents, contractors, or other business partners on behalf of ACME that are within scope of the PCI DSS. This policy applies to all ACME employees, contractors, sub-contractors, and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store, or dispose of ACME data.

Some standards are explicitly stated for persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions shall comply with the standards. ACME departments shall use this policy and its standards or may create a more restrictive set of policies and standards, but not one that is less restrictive, less comprehensive, or less compliant than this policy and its standards.

This policy and its standards do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

Annex 5: Cybersecurity Roles & Responsibilities provides a detailed description of ACME user roles and responsibilities, in regards to cybersecurity.

ACME reserves the right to revoke, change, or supplement this policy and its standards, procedures, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management, unless otherwise stated.

Cardholder Data Security Policy

ACME shall design, implement and maintain a coherent set of standards and procedures to manage risks to cardholder data, in an effort to ensure an acceptable level of cybersecurity risk. Within the scope of the Cardholder Data Environment (CDE), ACME will protect and ensure the Confidentiality, Integrity, and Availability (CIA) of all its information systems and cardholder data, regardless of how it is created, distributed, or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations of Policies, Standards and/or Procedures

Any ACME user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal and / or international law may be reported to the appropriate law enforcement agency for civil and / or criminal prosecution.

Exception To Standards

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. When requesting an exception, users are required to submit a business justification for deviation from the standard in question.

Updates To Policies & Standards

Updates to the PCI DSS Cybersecurity Policy will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, standards, procedures, and guidelines.

REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Firewalls are devices that control computer traffic allowed between ACME's networks and untrusted networks, as well as traffic into and out of more sensitive areas within ACME's internal trusted networks. The Cardholder Data Environment (CDE) is an example of a more sensitive area within ACME's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in PCI DSS Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of PCI DSS Requirement 1.

PCI DSS CONTROL 1.1

Control Objective: The organization establishes firewall and router configuration standards that follow industry-recognized leading practices.

Standard: Asset custodians are required to establish firewall and router configuration processes that include the following: [5]

(a) Asset custodians are required to establish and maintaining a formal process for approving and testing all network connections and changes to both firewall and router configurations; [6]
(b) Asset custodians are required to establish and maintaining detailed network diagrams. Network diagrams must: [7]
(c) Document all connections to cardholder data, including any wireless networks;
(d) Be reviewed annually; and
(e) Be updated as the network changes to reflect the current architecture in place;
(f) Asset custodians are required to establish and maintaining detailed data flow diagrams that show all cardholder data flows across systems and networks; A firewall is required to be installed at each Internet connection and between any Demilitarized Zone (DMZ) and ACME's internal networks; [8]
(g) All network devices must have a documented description of any applicable groups, roles, and responsibilities associated with the device to support configuration management and review processes; [9]
(h) A documented business justification is required for all services, protocols, and ports allowed through the firewall(s), including documentation of security features implemented for those protocols considered to be insecure; [10] and
(i) Firewall and router rule sets must be reviewed at least once every six (6) months and the review must cover: [11]
(j) Validation of Access Control Lists (ACLs); and
(k) Vulnerability management (e.g., validating software and firmware is current).

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Post Office Protocol (POP3)
- Internet Message Access Protocol (IMAP)

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

[5] PCI DSS v3.2 Requirement 1.1
[6] PCI DSS v3.2 Requirement 1.1.1
[7] PCI DSS v3.2 Requirement 1.1.2
[8] PCI DSS v3.2 Requirement 1.1.4
[9] PCI DSS v3.2 Requirement 1.1.5
[10] PCI DSS v3.2 Requirement 1.1.6
[11] PCI DSS v3.2 Requirement 1.1.7

PCI DSS CONTROL 1.2

Control Objective: The organization builds firewall and router configurations that restrict connections between untrusted networks and any system components in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to deploy and configure of firewalls and routers in order to restrict connections between untrusted networks and any system components within the Cardholder Data Environment (CDE) by the following means: [12]

(a) Implementing Access Control Lists (ACLs) and other applicable filters to restrict the inbound and outbound traffic to the CDE to only that which is necessary, as defined by a business justification; [13]
(b) Securing and synchronizing router and firewall configuration files; [14] and
(c) Positioning perimeter firewalls between wireless networks and the CDE.[15]

Supplemental Guidance: Not all firewalls and routers have the functionality for the running configuration to be different that the configuration loaded at startup. However, if the functionality exists, the startup configuration must be synchronized with the correct running configuration so that a reboot of the device will not degrade network security.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 1.3

Control Objective: The organization prohibits direct public access to the Internet and any system component in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to establish and manage firewall and router configuration standards to prohibit direct public access to the Internet and any system component in the Cardholder Data Environment (CDE) that includes, but is not limited to: [16]

(a) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [17]
(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [18]
(c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [19]
(d) Unauthorized outbound traffic from the CDE to the Internet are prohibited; [20]
(e) Stateful inspection (dynamic packet filtering) must be implemented; [21]
(f) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [22] and
(g) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [23]

Supplemental Guidance: A stateful firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and is able to hold significant attributes of each connection in memory. These attributes are collectively known as the state of the connection, and may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated so that filtering decisions would not only be based on administrator-defined rules, but also on the context that has been built by previous connections as well as previous packets belonging to the same connection.

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, or
- Internal use of RFC1918 address space instead of registered addresses.

[12] PCI DSS v3.2 Requirement 1.2
[13] PCI DSS v3.2 Requirement 1.2.1
[14] PCI DSS v3.2 Requirement 1.2.2
[15] PCI DSS v3.2 Requirement 1.2.3
[16] PCI DSS v3.2 Requirement 1.3
[17] PCI DSS v3.2 Requirement 1.3.1
[18] PCI DSS v3.2 Requirement 1.3.2
[19] PCI DSS v3.2 Requirement 1.3.3
[20] PCI DSS v3.2 Requirement 1.3.4
[21] PCI DSS v3.2 Requirement 1.3.5
[22] PCI DSS v3.2 Requirement 1.3.6
[23] PCI DSS v3.2 Requirement 1.3.7

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 1.4

Control Objective: The organization installs personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network.

Standard: Asset custodians are required to install and maintain firewall software or equivalent functionality on any Internet-accessible mobile device or computer which are used to access the Cardholder Data Environment (CDE) that includes, but is not limited to: [24]

(a) Firewall software must be configured by ACME's IT department;
(b) Configuration settings of the firewall software must not be alterable by standard users; and
(c) Firewall configurations must include:
    1. Specific configuration settings are defined for firewall software.
    2. Firewall software is actively running.
    3. Firewall software is not alterable by users of mobile devices and/or computers.

Supplemental Guidance: Examples of mobile devices and computers includes, but are not limited to:

- Laptops
- Tablets
- Smart phones

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 1.5

Control Objective: Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for managing firewalls are kept current and disseminated to all pertinent parties. [25]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

REQUIREMENT #2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS & OTHER SECURITY PARAMETERS

Malicious individuals (external and internal to an organization) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and are easily determined via public information.

PCI DSS CONTROL 2.1

Control Objective: The organization always changes vendor-supplied defaults before installing a system on the network.

Standard: Asset custodians are required to ensure vendor-supplied defaults are changed, prior to the information system being installed on the network. This pre-production hardening process for both wired and wireless information systems must include, but is not limited to: [26]

(a) Changing vendor default credentials: [27]
    1. Passwords;
    2. Simple Network Management Protocol (SNMP) community strings; and
    3. Encryption keys

[24] PCI DSS v3.2 Requirement 1.4
[25] PCI DSS v3.2 Requirement 1.5
[26] PCI DSS v3.2 Requirement 2.1
[27] PCI DSS v3.2 Requirement 2.1.1

(b) Disabling or deleting unnecessary accounts;
(c) Updating firmware on devices; and
(d) Verifying other security-related vendor defaults are changed, if applicable.

Supplemental Guidance: This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.) Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 2.2

Control Objective: The organization develops configuration standards for all system components that are consistent with industry-accepted system hardening standards.

Standard: Asset custodians are required to develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to: [28]

(a) Verifying that system configuration standards are:
    1. Updated as new vulnerability issues are identified;
    2. Applied when new systems are configured;
    3. Consistent with industry-accepted hardening standards;
(b) Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers); [29]
(c) Enforcing least functionality, which includes but is not limited to:
    1. Allowing only necessary and secure services, protocols, and daemons; [30]
    2. Removing all unnecessary functionality, which includes but is not limited to: [31]
        i. Scripts;
        ii. Drivers;
        iii. Features;
        iv. Subsystems;
        v. File systems; and
        vi. Unnecessary web servers
(d) Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS), or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP; [32]
(e) Verifying system security parameters are configured to prevent misuse; [33] and
(f) Documenting the functionality present on information systems.

Supplemental Guidance: *Annex 8: System Hardening* contains the approved baseline configurations. Baseline configurations should be based on industry-recognized leading practices. Sources of approved baseline configurations are:

- Microsoft Security Configuration Wizard
- Center for Internet Security (CIS)
- Defense Cybersecurity Agency (DISA) Security Technical Implementation Guides (STIGs) [34]

If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 2.3

Control Objective: The organization encrypts all non-console administrative access using strong cryptography.

[28] PCI DSS v3.2 Requirement 2.2
[29] PCI DSS v3.2 Requirement 2.2.1
[30] PCI DSS v3.2 Requirement 2.2.2
[31] PCI DSS v3.2 Requirement 2.2.5
[32] PCI DSS v3.2 Requirement 2.2.3
[33] PCI DSS v3.2 Requirement 2.2.4
[34] DISA STIGs official site: http://iase.disa.mil/stigs/index.html

REQUIREMENT #10: TRACK & MONITOR ALL ACCESS TO NETWORK RESOURCES & CARDHOLDER DATA

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS CONTROL 10.1

Control Objective: The organization implements audit trails for linking access to system components to individual users.

Standard: Asset custodians and data owners are required to implement auditing of systems and applications that allow access to system components to be linked to individual users. [169]

Supplemental Guidance: It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 10.2

Control Objective: The organization utilizes automated audit trails for system components to reconstruct events.

Standard: Asset custodians and data owners are required to implement automated audit trails for all system components to reconstruct the following events: [170]

(a) All individual user accesses to cardholder data; [171]
(b) All actions taken by any individual with root or administrative privileges; [172]
(c) Access to all audit trails; [173]
(d) Invalid logical access attempts; [174]
(e) Use of and changes to identification and authentication mechanisms, including but not limited to: [175]
    1. creation of new accounts and elevation of privileges; and
    2. all changes, additions, or deletions to accounts with root or administrative privileges;
(f) Initialization, stopping, or pausing of the audit logs; [176] and
(g) Creation and deletion of system-level objects. [177]

Supplemental Guidance: Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

[169] PCI DSS v3.2 Requirement 10.1
[170] PCI DSS v3.2 Requirement 10.2
[171] PCI DSS v3.2 Requirement 10.2.1
[172] PCI DSS v3.2 Requirement 10.2.2
[173] PCI DSS v3.2 Requirement 10.2.3
[174] PCI DSS v3.2 Requirement 10.2.4
[175] PCI DSS v3.2 Requirement 10.2.5
[176] PCI DSS v3.2 Requirement 10.2.6
[177] PCI DSS v3.2 Requirement 10.2.7

PCI DSS CONTROL 10.3

Control Objective: The organization follows best practices for logging audit trail entries.

Standard: Asset custodians and data owners are required to configure systems to record at least the following audit trail entries for all system components for each event: [178]

(a) User identification; [179]
(b) Type of event; [180]
(c) Date and time; [181]
(d) Success or failure indication; [182]
(e) Origination of event; [183] and
(f) Identity or name of affected data, system component, or resource. [184]

Supplemental Guidance: By recording these details for the auditable events at PCI DSS requirement 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

PCI DSS CONTROL 10.4

Control Objective: The organization utilizes time-synchronization technology to synchronize all critical system clocks.

Standard: Network Time Protocol (NTP) is ACME's official method of synchronizing all system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time:[185]

(a) Asset custodians are responsible for configuring ACME's NTP servers so that they are receiving time from industry-accepted time sources; [186] and
(b) Asset owners must ensure NTP on their systems is configured properly and validate the following:
    1. Systems are configured to synchronize time with ACME's NTP servers;
    2. Information systems have the correct and consistent time; [187] and
    3. Time data is protected from unauthorized modification. [188]

Supplemental Guidance: Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[189] Official NIST or USNO Internet Time Service (ITS) that can to be used for system time synchronization include, but are not limited to:

- time.nist.gov 192.43.244.18 [primary]; and
- time-nw.nist.gov 131.107.13.100 [alternate]

Procedures: [insert a description of the actual procedures that you follow to meet this requirement]

[178] PCI DSS v3.2 Requirement 10.3
[179] PCI DSS v3.2 Requirement 10.3.1
[180] PCI DSS v3.2 Requirement 10.3.2
[181] PCI DSS v3.2 Requirement 10.3.3
[182] PCI DSS v3.2 Requirement 10.3.4
[183] PCI DSS v3.2 Requirement 10.3.5
[184] PCI DSS v3.2 Requirement 10.3.6
[185] PCI DSS v3.2 Requirement 10.4
[186] PCI DSS v3.2 Requirement 10.4.3
[187] PCI DSS v3.2 Requirement 10.4.1
[188] PCI DSS v3.2 Requirement 10.4.2
[189] http://tycho.usno.navy.mil/ntp.html

- SUPPLEMENTAL DOCUMENTATION -

PCI DSS POLICY & STANDARD SUPPLEMENTAL

ANNEXES, TEMPLATES & REFERENCES

Version 2020.1

PCI DSS
Information Security Policy & Standards

TABLE OF CONTENTS

ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include negatively affecting [Company Name]'s competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by [Company Name]
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include negatively affecting [Company Name]'s competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by [Company Name], or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to [Company Name].
		· Impact would not be damaging or a risk to business operations.

LABELING

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed**. Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.
- **Displayed**. Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

GENERAL ASSUMPTIONS

- Any information created or received by [Company Name] employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

PERSONAL DATA (PD)

PD is any information about an individual maintained by [Company Name] including any information that:

- Can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive PD (sPD) is always PD, but PD is not always sPD. Examples of PD include, but are not limited to:

- Name
  - Full name;
  - Maiden name;
  - Mother's maiden name; and
  - Alias(es);
- Personal Identification Numbers
  - Social Security Number (SSN);
  - Passport number;
  - Driver's license number;
  - Taxpayer Identification Number (TIN), and
  - Financial account or credit card number;
- Address Information
  - Home address; and
  - Personal email address;
- Personal Characteristics
  - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
  - Fingerprints;
  - Handwriting, and

DATA HANDLING GUIDELINES

HANDLING CONTROLS	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-[Company Name] employees.	▪ NDA is recommended prior to access by non-[Company Name] employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*

ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Confidential	Restricted
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Controlled Unclassified Information (CUI)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	

ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL).*

DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

SAFETY & CRITICALITY

The Safety & Criticality (SC) rating reflects two aspects of the "importance" of the asset or process:

- On one hand, SC simply represents the importance of the asset relative to the achievement of the company's goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to [Company Name], its clients, its partners, or the general public.

The three (3) SC ratings are:

- SC-1: Mission Critical. This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of [Company Name]:
  - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
  - Any business interruption would have a significant impact on [Company Name]'s mission.
    - Cannot go down without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of [Company Name]'s business operations:
  - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on [Company Name]'s mission.
    - Loss of availability is difficult to deal with and can only be tolerated for a short time.
    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
    - The consequences of loss of integrity are unacceptable.
  - *Requires protection measures equal to or beyond leading practices* to ensure adequate security.
  - Safety aspects of SC-2 systems could lead to:
    - Loss of privacy; and/or
    - Unwanted harassment.
- SC-3: Non-Critical. This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
  - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
    - The consequences could include the delay or degradation of services or routine activities.
  - *Requires protection measures that are commensurate with leading practices* to ensure adequate security.
  - Safety aspects of SC-3 systems could lead to:
    - Inconvenience;
    - Frustration; and/or
    - Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

Basic Assurance Requirements

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

Enhanced Assurance Requirements

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to [Company Name].