Your Logo
Will Be
Placed Here

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

ACME Business Consulting, Inc.

PCI DSS
Information Security Policies & Standards
PCI DSS v3

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 compliance at ACME Business Consulting, Inc. (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.

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.

Appendix D: 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.

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

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.

EXCEPTIONS

While every exception to a policy or standard potentially weakens protection mechanisms for ACME information systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available in Appendix E: Cybersecurity Exception Request Procedures.

UPDATES

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.

KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Cybersecurity Terms*, is the primary reference document that ACME uses to define common cybersecurity terms. [1] Key terminology to be aware of includes:

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

[1] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

CYBERSECURITY CONSIDERATIONS FOR PROTECTING SYSTEMS

Appendix F: Type of Security Controls provides a detailed description of cybersecurity considerations in protecting information systems, based on the importance of the system and the sensitivity of the data processed or stored by the system.

POLICIES, CONTROL OBJECTIVES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

In order to reduce possible confusion, VENDOR must be aware of and abide by ACME's use of terminology for cybersecurity documentation:

(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.

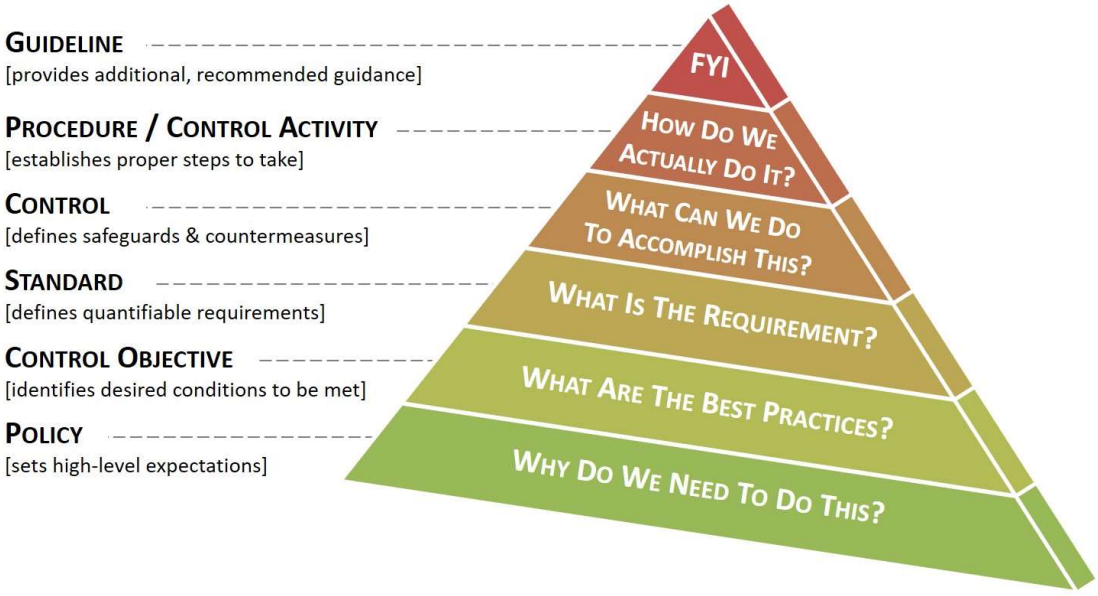

Figure 1: Cybersecurity Documentation Hierarchy

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: [3]

(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; [4]
(b) Asset custodians are required to establish and maintaining detailed network diagrams. Network diagrams must: [5]
(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; [6]
(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; [7]
(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; [8] and
(i) Firewall and router rule sets must be reviewed at least once every six (6) months and the review must cover: [9]
(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]

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

(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; [11]
(b) Securing and synchronizing router and firewall configuration files; [12] and
(c) Positioning perimeter firewalls between wireless networks and the CDE.[13]

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: [14]

(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; [15]
(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [16]
(c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [17]
(d) Unauthorized outbound traffic from the CDE to the Internet are prohibited; [18]
(e) Stateful inspection (dynamic packet filtering) must be implemented; [19]
(f) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [20] and
(g) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [21]

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.

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

REQUIREMENT #7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on the need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS CONTROL 7.1

Control Objective: The organization limits access to system components and cardholder data to only those individuals whose job requires such access.

Standard: Asset custodians and data owners are required to implement administrative and technical measures to limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations include the following: [104]

(a) Defining access needs for each role, including: [105]
    1. System components and data resources that each role needs to access for their job function; and
    2. Level of privilege required (e.g., user, administrator, etc.) for accessing resources;
(b) Restricting access to privileged user IDs to least privileges necessary to perform job responsibilities; [106]
(c) Assigning access based on individual personnel's job classification and function; [107] and
(d) Requiring documented approval by authorized parties specifying required privileges. [108]

Supplemental Guidance: The implement of an automated access control system can be a combination of technology, since all modern computers, payment application, and Point of Sale (POS) software already have built-in systems for user accounts and privilege controls. Microsoft's PCI DSS Compliance Planning Guide should be referenced for using Active Directory as an automated access control system. [109]

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

PCI DSS CONTROL 7.2

Control Objective: The organization implements an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all," unless specifically allowed.

Standard: Asset custodians and data owners are required to ensure systems components are configured to restrict access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following: [110]

(a) Coverage of all system components; [111]
(b) Assignment of privileges to individuals based on job classification and function (RBAC); [112] and
(c) Default "deny-all" setting. [113]

Supplemental Guidance: Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. An access control system automates the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access.

Vendor manuals should be used to validate setting, since some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.

[104] PCI DSS v3.2 Requirement 7.1
[105] PCI DSS v3.2 Requirement 7.1.1
[106] PCI DSS v3.2 Requirement 7.1.2
[107] PCI DSS v3.2 Requirement 7.1.3
[108] PCI DSS v3.2 Requirement 7.1.4
[109] Microsoft's Payment Card Industry Data Security Standard Compliance Planning Guide http://www.microsoft.com/en-us/download/details.aspx?id=18015
[110] PCI DSS v3.2 Requirement 7.2
[111] PCI DSS v3.2 Requirement 7.2.1
[112] PCI DSS v3.2 Requirement 7.2.2
[113] PCI DSS v3.2 Requirement 7.2.3

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

PCI DSS CONTROL 7.3

Control Objective: The organization ensures that security policies and operational procedures for restricting access to cardholder data 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 restricting access to cardholder data are kept current and disseminated to all pertinent parties. [114]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.

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

REQUIREMENT #8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. These requirements are applicable to all accounts, including Point of Sale (POS) accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data.

PCI DSS CONTROL 8.1

Control Objective: The organization defines and implements policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.

Standard: Asset custodians and data owners are required to assign all non-consumer users unique user identifications (ID) before allowing them to access system components. User identification controls include the following: [115]

(a) Controlling addition, deletion, and modification of user IDs, credentials, and other identifier objects; [116]
(b) Revoking access for any terminated users within twenty-four (24) hours of employment status change; [117]
(c) Removing or disabling inactive user accounts within ninety (90) days; [118]
(d) Managing user accounts assigned to vendors that are used to access, support, or maintain system components via remote access: [119]
    1. Enabling the accounts only during the time period needed and disabled when not in use; and
    2. Monitoring the accounts when in use;
(e) Limiting repeated access attempts be locked out after not more than six (6) invalid logon attempts; [120]
(f) Setting lockout durations to a minimum of thirty (30) minutes or until an administrator enables the user ID; [121] and
(g) Require users to re-authenticate if a session has been idle for more than fifteen (15) minutes to re-activate the terminal or session. [122]

Supplemental Guidance: An example of uniqueness, the difference can be adding a designator to the end of the username, such as a number. Examples include:

- First user in the system named "John Smith": John.Smith or JSMITH
- Second user in the system named "John Smith": John.Smith1 or JSMITH1
- Third user in the system named "John Smith": John.Smith2 or JSMITH2

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

[114] PCI DSS v3.2 Requirement 7.3
[115] PCI DSS v3.2 Requirement 8.1, 8.1.1
[116] PCI DSS v3.2 Requirement 8.1.2
[117] PCI DSS v3.2 Requirement 8.1.3
[118] PCI DSS v3.2 Requirement 8.1.4
[119] PCI DSS v3.2 Requirement 8.1.5
[120] PCI DSS v3.2 Requirement 8.1.6
[121] PCI DSS v3.2 Requirement 8.1.7
[122] PCI DSS v3.2 Requirement 8.1.8

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for monitoring all access to network resources and cardholder data are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.

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

REQUIREMENT #11: REGULARLY TEST SECURITY SYSTEMS & PROCESSES

Vulnerabilities are being discovered continually by malicious individuals and are being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect the changing environment.

PCI DSS CONTROL 11.1

Control Objective: The organization implements processes to test for the presence of Wireless Access Points (WAPs) and detect and identify all authorized and unauthorized wireless access points.

Standard: Asset custodians are required to implement a process to test for the presence of Wireless Access Points (WAPs) that includes: [202]

(a) Detecting and identifying all authorized and unauthorized wireless access points at least once every ninety (90) days;
(b) Maintaining an inventory of authorized WAPs including a documented business justification; [203] and
(c) Implementing incident response procedures in the event unauthorized WAPs are detected. [204]

Supplemental Guidance: Detection methods must be sufficient to detect and identify both authorized and unauthorized devices. Methods that may be used in the rogue WAPs (802.11) detection process includes, but are not limited to:

- Wireless network scans,
- Physical/logical inspections of system components and infrastructure,
- Network Access Control (NAC); or
- Wireless Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

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

PCI DSS CONTROL 11.2

Control Objective: The organization implements a process for running internal and external network vulnerability scans at least quarterly and after any significant change in the network.

Standard: Asset custodians and data owners are required to perform the following vulnerability scanning-related activities: [205]

(a) Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel; [206]
(b) 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; [207] and
(c) Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. [208]

Supplemental Guidance: A "quarter" is defined as a ninety (90) day period and a "significant change" in the network includes, but is not limited to:

- New system component installations;

[202] PCI DSS v3.2 Requirement 11.1
[203] PCI DSS v3.2 Requirement 11.1.1
[204] PCI DSS v3.2 Requirement 11.1.2
[205] PCI DSS v3.2 Requirement 11.2
[206] PCI DSS v3.2 Requirement 11.2.1
[207] PCI DSS v3.2 Requirement 11.2.2
[208] PCI DSS v3.2 Requirement 11.2.3

- Changes in network topology;
- Firewall rule modifications; and
- Major product upgrades.

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

PCI DSS CONTROL 11.3

Control Objective: The organization implements a methodology for penetration testing.

Standard: Asset custodians and data owners are required to implement a methodology for penetration testing that includes the following:

(a) Coverage of all PCI DSS version 3.0 requirements: [209]
   1. Process is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115);
   2. Includes coverage for the entire CDE perimeter and critical systems;
   3. Includes testing from both inside and outside the network;
   4. Includes testing to validate any segmentation and scope-reduction controls;
   5. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in PCI DSS requirement 6.5;
   6. Defines network-layer penetration tests to include components that support network functions, as well as operating systems;
   7. Includes review and consideration of threats and vulnerabilities experienced in the last twelve (12) months; and
   8. Specifies retention of penetration testing results and remediation activities results.

(b) External penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [210]
   1. An operating system upgrade;
   2. A sub-network added to the environment; or
   3. A web server added to the CDE;

(c) Internal penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [211]
   1. An operating system upgrade;
   2. A sub-network added to the environment; or
   3. A web server added to the CDE;

(d) Exploitable vulnerabilities found during penetration testing must be corrected and testing shall be repeated to verify the corrections; [212] and

(e) If segmentation is used to isolate the CDE from other networks, penetration tests must be performed 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 in-scope systems. [213]

Supplemental Guidance: This update to PCI DSS requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.

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

PCI DSS CONTROL 11.4

Control Objective: The organization utilizes intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network.

Standard: Asset custodians and data owners are required to utilize Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) to: [214]

(a) Prevent intrusions into the CDE;

(b) Monitor all traffic at the perimeter of the CDE, as well as at critical points in the CDE;

[209] PCI DSS v3.2 Requirement 11.3
[210] PCI DSS v3.2 Requirement 11.3.1
[211] PCI DSS v3.2 Requirement 11.3.2
[212] PCI DSS v3.2 Requirement 11.3.3
[213] PCI DSS v3.2 Requirement 11.3.4 & 11.3.4.1
[214] PCI DSS v3.2 Requirement 11.4

APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

A-1: 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 ACME.
		· Impact could include negatively affecting ACME'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 ACME
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to ACME.
		· Impact could include negatively affecting ACME'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 ACME, 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 ACME.
		· 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 ACME.
		· Impact would not be damaging or a risk to business operations.

A-2: Labeling

Labeling is the practice of marking an information 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.

A-3: General Assumptions

- Any information created or received by ACME 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.

A-4: Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Passport number
- Permanent resident card
- Driver License (DL)
- Financial account number
- Payment card number (credit or debit)
- Bank account number
- Electronic Protected Health Information (ePHI)

A-5: DATA HANDLING GUIDELINES

HANDLING CONTROLS	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-ACME employees.	▪ NDA is recommended prior to access by non-ACME 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*
Web Sites	▪ Posting to intranet sites is prohibited, unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*

APPENDIX G: RULES OF BEHAVIOR / USER ACCEPTABLE USE

These Rules of Behavior apply to the use of ACME-provided IT resources, regardless of the geographic location:

- Data and information system use must comply with ACME policies and standards.
- Unauthorized access to data and/or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII).

G-1: ACCEPTABLE USE

Users shall:

- In accordance with organizational procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including PII, maintained or in possession of the user.
- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on organization-owned information systems.
- Log-off or lock systems when leaving them unattended.
- Complete security awareness training before accessing any information system and on an annual basis thereafter. Permit only authorized users to use organization provided information systems.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with organization records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information necessary to perform job functions (e.g., need to know).
- Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary.
- Wear organization-issued identification badges at all times in organization-operated facilities.

G-2: PROHIBITED USE

Users shall not:

- Direct or encourage others to violate organizational policies, procedures, standards or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
- Use another user's account, identity, or password.
- Exceed authorized access to sensitive information.
- Cause congestion, delay, or disruption of service to any organization-owned IT resource. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, as does some uses of "push" technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually oriented materials.
- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities or activities otherwise prohibited.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Use organization-provided IT resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).
- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
- Establish unauthorized personal, commercial or non-profit organizational web pages on organization provided information systems.
- Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.

ANNEX 12: INCIDENT RESPONSE PLAN (IRP) TEMPLATE

By the very nature of every incident being somewhat different, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

PLAN OBJECTIVES

The objective of Incident Response Plan (IRP) is to:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update company policies, standards, procedures, and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

IRP ACTIONS

Incident Responders (IR) will be their experience and best judgment to respond to potential incidents in a manner consistent with the severity level posed by the incident. If necessary, the IR will obtain external assistance to help with the triage and cleanup operations.

INCIDENT DISCOVERY

Malicious Actions	Possible Indications of an Incident
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses