Your Logo
Will Be
Placed Here

CYBERSECURITY AND DATA PROTECTION PROGRAM (CDPP)

Payment Card Industry Data Security Standard
PCI DSS v4.0
Self-Assessment Questionnaire (SAQ) A-EP

ACME Consulting Enterprises, LLC

CDPP
Cybersecurity & Data Protection Program

EXAMPLE

IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)

TABLE OF CONTENTS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) COMPLIANCE PROGRAM OVERVIEW 6
- INTRODUCTION 6
- POLICY OVERVIEW 6
- SCOPE & APPLICABILITY 6
- POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE 7
- VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES 7
- EXCEPTION TO STANDARDS 7
- UPDATES TO POLICIES & STANDARDS 7
- KEY TERMINOLOGY 7

PCI DSS SECTION 1: BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS 10
- POLICY: NETWORK SECURITY 10
- PRINCIPLE REQUIREMENT #1: INSTALL & MAINTAIN NETWORK SECURITY CONTROLS (NSC) 10
  - *REQUIREMENT 1.1* 10
    - *Defined Approach Requirement 1.1.1* 10
  - *REQUIREMENT 1.2* 11
    - *Defined Approach Requirement 1.2.1* 11
    - *Defined Approach Requirement 1.2.2* 11
    - *Defined Approach Requirement 1.2.3* 12
    - *Defined Approach Requirement 1.2.4* 12
    - *Defined Approach Requirement 1.2.5* 13
    - *Defined Approach Requirement 1.2.6* 13
    - *Defined Approach Requirement 1.2.7* 14
    - *Defined Approach Requirement 1.2.8* 14
  - *REQUIREMENT 1.3* 15
    - *Defined Approach Requirement 1.3.1* 15
    - *Defined Approach Requirement 1.3.2* 15
    - *Defined Approach Requirement 1.3.3* 15
  - *REQUIREMENT 1.4* 16
    - *Defined Approach Requirement 1.4.1* 16
    - *Defined Approach Requirement 1.4.2* 16
    - *Defined Approach Requirement 1.4.3* 17
    - *Defined Approach Requirement 1.4.4* 17
    - *Defined Approach Requirement 1.4.5* 17
  - *REQUIREMENT 1.5* 18
    - *Defined Approach Requirement 1.5.1* 18
- PRINCIPLE REQUIREMENT #2: APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS 18
  - *REQUIREMENT 2.1* 18
    - *Defined Approach Requirement 2.1.1* 18
  - *REQUIREMENT 2.2* 19
    - *Defined Approach Requirement 2.2.1* 19
    - *Defined Approach Requirement 2.2.2* 20
    - *Defined Approach Requirement 2.2.3* 21
    - *Defined Approach Requirement 2.2.4* 22
    - *Defined Approach Requirement 2.2.5* 22
    - *Defined Approach Requirement 2.2.6* 23
    - *Defined Approach Requirement 2.2.7* 23

PCI DSS SECTION 2: PROTECT ACCOUNT DATA 25
- POLICY: DATA PROTECTION & HANDLING 25
- PRINCIPLE REQUIREMENT #3: PROTECT STORED ACCOUNT DATA 25
  - *REQUIREMENT 3.1* 25
    - *Defined Approach Requirement 3.1.1* 25
  - *REQUIREMENT 3.2* 26
    - *Defined Approach Requirement 3.2.1* 26
  - *REQUIREMENT 3.3* 27
    - *Defined Approach Requirement 3.3.1* 27
    - *Defined Approach Requirement 3.3.1.2* 27
    - *Defined Approach Requirement 3.3.1.3* 28
- PRINCIPLE REQUIREMENT #4: PROTECT CARDHOLDER DATA WITH STRONG CRYPTOGRAPHIC DURING TRANSMISSION OVER OPEN, PUBLIC NETWORKS 28

EXAMPLE

REQUIREMENT 4.1 **28**
Defined Approach Requirement 4.1.1 *28*
REQUIREMENT 4.2 **29**
Defined Approach Requirement 4.2.1 *29*
Defined Approach Requirement 4.2.2 *30*
PCI DSS SECTION 3: MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM **31**
POLICY: VULNERABILITY & PATCH MANAGEMENT **31**
PRINCIPLE REQUIREMENT #5: PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE **31**
REQUIREMENT 5.1 **31**
Defined Approach Requirement 5.1.1 *31*
REQUIREMENT 5.2 **32**
Defined Approach Requirement 5.2.1 *32*
Defined Approach Requirement 5.2.2 *32*
Defined Approach Requirement 5.2.3 *32*
Defined Approach Requirement 5.2.3.1 *33*
REQUIREMENT 5.3 **33**
Defined Approach Requirement 5.3.1 *33*
Defined Approach Requirement 5.3.2 *34*
Defined Approach Requirement 5.3.2.1 *34*
Defined Approach Requirement 5.3.3 *35*
Defined Approach Requirement 5.3.4 *35*
Defined Approach Requirement 5.3.5 *36*
REQUIREMENT 5.4 **36**
Defined Approach Requirement 5.4.1 *36*
PRINCIPLE REQUIREMENT #6: DEVELOP & MAINTAIN SECURE SYSTEMS & SOFTWARE **37**
REQUIREMENT 6.1 **37**
Defined Approach Requirement 6.1.1 *37*
REQUIREMENT 6.2 **37**
Defined Approach Requirement 6.2.1 *37*
Defined Approach Requirement 6.2.2 *39*
Defined Approach Requirement 6.2.4 *39*
REQUIREMENT 6.3 **41**
Defined Approach Requirement 6.3.1 *41*
Defined Approach Requirement 6.3.2 *42*
Defined Approach Requirement 6.3.3 *42*
REQUIREMENT 6.4 **43**
Defined Approach Requirement 6.4.1 *43*
Defined Approach Requirement 6.4.2 *44*
Defined Approach Requirement 6.4.3 *44*
REQUIREMENT 6.5 **45**
Defined Approach Requirement 6.5.1 *45*
Defined Approach Requirement 6.5.2 *46*
PCI DSS SECTION 4: IMPLEMENT STRONG ACCESS CONTROL MEASURES **47**
POLICY: IDENTITY & ACCESS MANAGEMENT **47**
PRINCIPLE REQUIREMENT #7: RESTRICT ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA BY BUSINESS NEED TO KNOW **47**
REQUIREMENT 7.2 **47**
Defined Approach Requirement 7.2.2 *47*
Defined Approach Requirement 7.2.3 *48*
Defined Approach Requirement 7.2.4 *48*
Defined Approach Requirement 7.2.5 *49*
PRINCIPLE REQUIREMENT #8: IDENTIFY USERS AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS **49**
REQUIREMENT 8.1 **50**
Defined Approach Requirement 8.1.1 *50*
REQUIREMENT 8.2 **50**
Defined Approach Requirement 8.2.1 *50*
Defined Approach Requirement 8.2.2 *51*
Defined Approach Requirement 8.2.4 *51*
Defined Approach Requirement 8.2.5 *52*
Defined Approach Requirement 8.2.6 *52*
Defined Approach Requirement 8.2.7 *52*
Defined Approach Requirement 8.2.8 *53*
REQUIREMENT 8.3 **53**

EXAMPLE

Defined Approach Requirement 8.3.1 53
Defined Approach Requirement 8.3.2 53
Defined Approach Requirement 8.3.3 54
Defined Approach Requirement 8.3.4 54
Defined Approach Requirement 8.3.5 55
Defined Approach Requirement 8.3.6 55
Defined Approach Requirement 8.3.7 55
Defined Approach Requirement 8.3.8 56
Defined Approach Requirement 8.3.9 56
Defined Approach Requirement 8.3.11 57
Requirement 8.4 **57**
Defined Approach Requirement 8.4.1 58
Defined Approach Requirement 8.4.2 58
Defined Approach Requirement 8.4.3 58
Requirement 8.5 **58**
Defined Approach Requirement 8.5.1 58
Requirement 8.6 **59**
Defined Approach Requirement 8.6.1 59
Defined Approach Requirement 8.6.2 60
Defined Approach Requirement 8.6.3 60
Principle Requirement #9: Restrict Physical Access To Cardholder Data **61**
Requirement 9.2 **61**
Defined Approach Requirement 9.2.1 61
Requirement 9.4 **62**
Defined Approach Requirement 9.4.1 62
Defined Approach Requirement 9.4.1.1 62
Defined Approach Requirement 9.4.2 62
Defined Approach Requirement 9.4.3 63
Defined Approach Requirement 9.4.4 63
Defined Approach Requirement 9.4.6 63
PCI DSS Section 5: Regularly Monitor & Test Networks **65**
Policy: Monitoring for Situational Awareness **65**
Principle Requirement #10: Log and Monitor All Access to System Components and Cardholder Data **65**
Requirement 10.2 **65**
Defined Approach Requirement 10.2.1 65
Defined Approach Requirement 10.2.1.1 65
Defined Approach Requirement 10.2.1.2 66
Defined Approach Requirement 10.2.1.3 66
Defined Approach Requirement 10.2.1.4 66
Defined Approach Requirement 10.2.1.5 66
Defined Approach Requirement 10.2.1.6 67
Defined Approach Requirement 10.2.1.7 67
Defined Approach Requirement 10.2.2 67
Requirement 10.3 **68**
Defined Approach Requirement 10.3.1 68
Defined Approach Requirement 10.3.2 68
Defined Approach Requirement 10.3.3 68
Defined Approach Requirement 10.3.4 69
Requirement 10.4 **69**
Defined Approach Requirement 10.4.1 69
Defined Approach Requirement 10.4.1.1 69
Defined Approach Requirement 10.4.2 70
Defined Approach Requirement 10.4.2.1 70
Defined Approach Requirement 10.4.3 71
Requirement 10.5 **71**
Defined Approach Requirement 10.5.1 71
Requirement 10.6 **71**
Defined Approach Requirement 10.6.1 71
Defined Approach Requirement 10.6.2 72
Defined Approach Requirement 10.6.3 72
Principle Requirement #11: Test Security of Systems and Networks Regularly **73**
Requirement 11.3 **73**
Defined Approach Requirement 11.3.2 73

EXAMPLE

Defined Approach Requirement 11.3.2.1 73
Requirement 11.4 **74**
Defined Approach Requirement 11.4.1 74
Defined Approach Requirement 11.4.3 75
Defined Approach Requirement 11.4.4 75
Defined Approach Requirement 11.4.5 76
Requirement 11.5 **77**
Defined Approach Requirement 11.5.1 77
Defined Approach Requirement 11.5.2 77
Requirement 11.6 **78**
Defined Approach Requirement 11.6.1 78
PCI DSS Section 6: Maintain An Information Security Policy **80**
Policy: Cybersecurity & Data Protection Governance **80**
Principle Requirement #12: Support Information Security With Organizational Policies and Programs **80**
Requirement 12.1 **80**
Defined Approach Requirement 12.1.1 80
Defined Approach Requirement 12.1.2 81
Defined Approach Requirement 12.1.3 81
Defined Approach Requirement 12.1.4 81
Requirement 12.3 **82**
Defined Approach Requirement 12.3.1 82
Requirement 12.6 **83**
Defined Approach Requirement 12.6.1 83
Defined Approach Requirement 12.6.3.1 83
Requirement 12.8 **84**
Defined Approach Requirement 12.8.1 84
Defined Approach Requirement 12.8.2 84
Defined Approach Requirement 12.8.3 85
Defined Approach Requirement 12.8.4 85
Defined Approach Requirement 12.8.5 86
Requirement 12.10 **87**
Defined Approach Requirement 12.10.1 87
Defined Approach Requirement 12.10.3 88
Glossary: Acronyms & Definitions **89**
Acronyms **89**
Definitions **89**
Record of Changes **90**

EXAMPLE

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) COMPLIANCE PROGRAM OVERVIEW

INTRODUCTION

The Cybersecurity and Data Protection Program (CDPP) provides definitive information on the prescribed measures used to establish and enforce the Payment Card Industry Data Security Standard (PCI DSS) compliance program at ACME Consulting Enterprises, 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 entity that interacts with ACME data and systems, applications and services. Therefore, it is the responsibility of both ACME personnel and third-parties to be aware of and adhere to ACME's cybersecurity and data protection requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity and availability:

- Confidentiality – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal privacy and proprietary information.
- Integrity – This addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- Availability – This addresses timely, reliable access to data, systems and services for authorized users, services and processes.

POLICY OVERVIEW

To ensure an acceptable level of cybersecurity risk, ACME is required to design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

The CDPP addresses the policies, standards and guidelines. Data / process owners, in conjunction with asset custodians, are responsible for creating, implementing and updated operational procedures to comply with CDPP requirements.

ACME users must protect and ensure the Confidentiality, Integrity and Availability (CIA) of data and systems, regardless of how its data 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 system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

SCOPE & APPLICABILITY

These policies, standards and guidelines apply to all ACME data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME. These policies, standards and guidelines apply to all ACME employees, contractors, sub-contractors and their respective facilities supporting ACME business operations, wherever ACME cardholder data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store or dispose of ACME's cardholder data.

Some standards apply specifically to 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 these standards or may create a more restrictive standard, but none that are less restrictive, less comprehensive or less compliant than these standards.

These policies 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. ACME reserves the right to revoke, change or supplement these policies, standards and guidelines at any time without prior notice. Such changes must be effective immediately upon approval by management unless otherwise stated.

ACME's documented roles and responsibilities provides a detailed description of ACME user roles and responsibilities, regarding cybersecurity-related use obligations.

EXAMPLE

POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

ACME's cybersecurity and data protection documentation is comprised of five (5) core components:

(1) Policies are established by the organization's corporate leadership establishes "management's intent" for cybersecurity and data protection requirements that are necessary to support the organization's overall strategy and mission;
(2) Control Objectives identify the technical, administrative and physical protections that are generally tied to a law, regulation, industry framework or contractual obligation;
(3) Standards provide organization-specific, quantifiable requirements for cybersecurity and data protection;
(4) Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
(5) Guidelines are additional guidance that is recommended, but not mandatory.

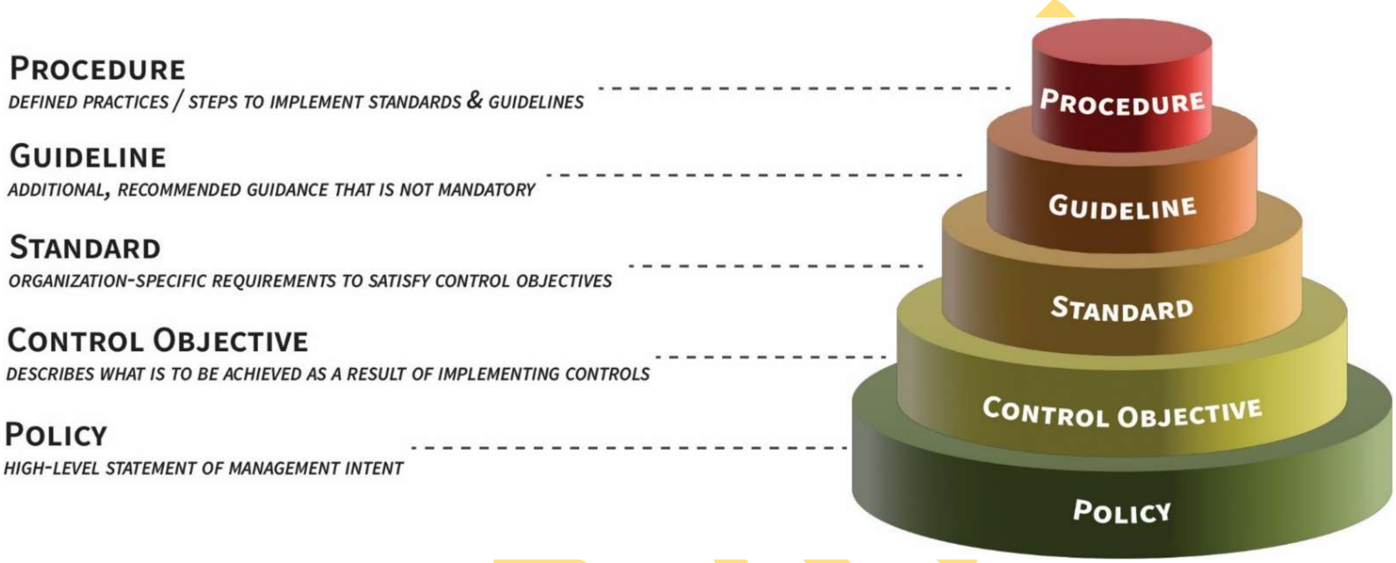
PROCEDURE
DEFINED PRACTICES / STEPS TO IMPLEMENT STANDARDS & GUIDELINES
GUIDELINE
ADDITIONAL, RECOMMENDED GUIDANCE THAT IS NOT MANDATORY
STANDARD
ORGANIZATION-SPECIFIC REQUIREMENTS TO SATISFY CONTROL OBJECTIVES
CONTROL OBJECTIVE
DESCRIBES WHAT IS TO BE ACHIEVED AS A RESULT OF IMPLEMENTING CONTROLS
POLICY
HIGH-LEVEL STATEMENT OF MANAGEMENT INTENT
PROCEDURE
GUIDELINE
STANDARD
CONTROL OBJECTIVE
POLICY

Figure 1: Cybersecurity Documentation Hierarchy

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 must submit a business justification for deviation from the standard in question.

UPDATES TO POLICIES & STANDARDS

Updates to the Cybersecurity and Data Protection Program (CDPP) 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, procedures, standards and guidelines.

KEY TERMINOLOGY

For PCI DSS-specific terminology, the **PCI Security Standards Council's Glossary** is the authoritative source for terminology definitions.[1] For other cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the alternative reference document that ACME uses to define common cybersecurity terms. [2] Key terminology to be aware of includes:

Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to or modification of information.

---

[1] *PCI SSC Glossary - https://www.pcisecuritystandards.org/pci_security/glossary*
[2] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*

Asset: A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that a ACME owns or controls.

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

Cloud Computing. A term describing a technology infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Control: A term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help ACME accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align ACME with accepted due diligence and due care requirements.

Cybersecurity / Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies. *Annex 1: Data Classification & Handling Guidelines* provides guidance on data classification and handling restrictions.

Data Controller. A term describing the privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing Personal Data (PD) other than natural persons who use data for personal purposes

Data Principle. A term describing the natural person to whom the Personal Data (PD) relates

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

Information Technology (IT). A term includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

Personal Data / Personal Information (PD). A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[3]

EXAMPLE

---

[3] *European Union General Data Protection Requirement – Article 4 (1)*

POLICY: NETWORK SECURITY

Management Intent: The purpose of the network security policy is to ensure sufficient security controls are in place to protect the confidentiality and integrity of ACME's communications, as well as to provide situational awareness of activity on ACME's networks.

Policy: ACME shall leverage industry-recognized network security management practices to strengthen the security and resilience of its network infrastructure. Layered defenses shall be utilized to restrict the ability of adversaries to transverse unimpeded across ACME's network. The concepts of "least privilege" and "least functionality" shall be consistently implemented across all network access points.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

PRINCIPLE REQUIREMENT #1: INSTALL & MAINTAIN NETWORK SECURITY CONTROLS (NSC)

Network Security Controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules. NSCs are designed to examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.

Common examples of untrusted networks include the Internet, dedicated connections such as business-to-business communication channels, wireless networks, carrier networks (such as cellular), third-party networks, and other sources outside the entity's ability to control. Furthermore, untrusted networks also include corporate networks that are considered out-of-scope for PCI DSS, because they are not assessed, and therefore must be treated as untrusted because the existence of security controls has not been verified. While an entity may consider an internal network to be trusted from an infrastructure perspective, if a network is out of scope for PCI DSS, that network must be considered untrusted for PCI DSS.

REQUIREMENT 1.1

Processes and mechanisms for installing and maintaining network security controls are defined and understood.

DEFINED APPROACH REQUIREMENT 1.1.1

Control Objective: Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

PCI DSS Requirement Description: All security policies and operational procedures that are identified in Requirement 1 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

Standard: The Cybersecurity and Data Protection Program (CDPP) document represents the consolidation of ACME's PCI DSS-specific policies and standards. The CDPP is endorsed by ACME's executive management and shall be:

(a) Disseminated to the appropriate parties to ensure all affected personnel are made aware of and understand their applicable requirements to protect cardholder data;
(b) Reviewed and updated on no less than an annual basis, or as business/technology changes require modifications to the CDPP, to ensure proper coverage for applicable PCI DSS requirements;
(c) Enforced by ACME personnel through "business as usual" secure practices in the form of Standardized Operating Procedures (SOP) that shall be developed, enforced and maintained at the control operator level;
(d) Enforced through ACME's supply chain in the form of contractual requirements with those third-parties that have the ability to directly or indirectly influence the confidentiality, integrity and/or availability of cardholder data.

EXAMPLE

Guidelines: It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives.

- Security policies define the entity's security objectives and principles.
- Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

REQUIREMENT 1.2

Network Security Controls (NSCs) are configured and maintained.

DEFINED APPROACH REQUIREMENT 1.2.1

Control Objective: The way that NSCs are configured and operate are defined and consistently applied.

PCI DSS Requirement Description: Configuration standards for NSC rulesets are:

- Defined.
- Implemented.
- Maintained.

Standard: ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and enforce baseline secure configuration requirements for Network Security Controls (NSCs) that:

(a) Are capable of addressing applicable legal, statutory and regulatory compliance obligations, including specific PCI DSS requirements; and
(b) Follow industry-recognized secure practices for NSC hardening:
    1. Center for Internet Security (CIS);[6]
    2. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs); [7] or
    3. Original Equipment Manufacturer (OEM) security configuration guidance.

Guidelines: The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset). Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.

DEFINED APPROACH REQUIREMENT 1.2.2

Control Objective: Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.

PCI DSS Requirement Description: All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

Standard: Data/process owners and asset custodians must follow ACME's established change control processes for all changes to system components. Change control for systems, applications and services within scope for PCI DSS must:

(a) Be approved a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and
(b) Document:
    1. The impact of the change;
    2. Prior approval for the change;
    3. Functionality testing to verify the change:
        i. Did not adversely impact the security of the network; and
        ii. Performs as expected; and
    4. Back-out procedures; and
(c) As applicable, update affected documentation s to include the changes to prevent inconsistencies between network documentation and the actual configuration.

Guidelines: Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.

EXAMPLE

---

[6] *CIS Benchmarks - https://www.cisecurity.org/cis-benchmarks/*

[7] *DISA STIGs official site: https://public.cyber.mil/stigs/*

PCI DSS SECTION 4: IMPLEMENT STRONG ACCESS CONTROL MEASURES

POLICY: IDENTITY & ACCESS MANAGEMENT

Management Intent: The purpose of the Identification & Access Management (IAM) policy is to implement the concept of "least privilege" through limiting access to ACME's systems and data to authorized users only.

Policy: ACME shall implement and maintain the principle of "least privilege" within logical access control mechanisms so that only authorized users can gain access to ACME's systems and data.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

PRINCIPLE REQUIREMENT #7: RESTRICT ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA BY BUSINESS NEED TO KNOW

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

- "Access" or "access rights" are created by rules that provide users access to systems, applications, and data, while "privileges" allow a user to perform a specific action or function in relation to that system, application, or data. For example, a user may have access rights to specific data, but whether they can only read that data, or can also change or delete the data is determined by the user's assigned privileges.
- "Need to know" refers to providing access to only the least amount of data needed to perform a job.
- "Least privileges" refers to providing only the minimum level of privileges needed to perform a job.

These requirements apply to user accounts and access for employees, contractors, consultants, and internal and external vendors and other third parties (e.g., for providing support or maintenance services). Certain requirements also apply to application and system accounts used by the entity (also called "service accounts").

REQUIREMENT 7.2

Access to system components and data is appropriately defined and assigned.

DEFINED APPROACH REQUIREMENT 7.2.2

Control Objective: Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.

PCI DSS Requirement Description: Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s) for Identity and Access Management (IAM), must develop and implement Role-Based Access Control (RBAC) to enforce the "principle of least privilege" so that only authorized individuals have access to information or functionality based on a legitimate business need, as defined by the user's role and responsibilities at ACME. RBAC must:

(a) Assign individuals the least privileges necessary for the operability of system(s), application(s) and/or processes based on the individual's designated role and responsibilities; and
(b) Be set to "deny all" unless specifically allowed, based on a user's need to know.

Guidelines: RBAC is a type of Discretionary Access Control (DAC). Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID. Access rights are granted to a user by assignment to one or several functions. Assess is assigned depending on the specific user functions and with the minimum scope required for the job.

Entities may wish to consider use of Privileged Access Management (PAM), which is a method to grant access to privileged accounts only when those privileges are required, immediately revoking that access once they are no longer needed.

EXAMPLE

- SUPPLEMENTAL DOCUMENTATION -

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

ANNEXES, TEMPLATES & REFERENCES

EXAMPLE

Version 2022.1

Table of Contents

Annexes 3
- Annex 1: Data Classification & Handling Guidelines 3
- Annex 2: Data Classification Examples 8
- Annex 3: Data Retention Periods 10
- Annex 4: Baseline Security Categorization Guidelines 12
- Annex 5: Rules of Behavior (Acceptable & Unacceptable Use) 14
- Annex 6: Guidelines for Personal Use of Organizational IT Resources 16
- Annex 7: Risk Management Framework (RMF) 17
- Annex 8: System Hardening 20

Templates 22
- Template 1: Management Directive (Policy Authorization) 22
- Template 2: User Acknowledgement Form 23
- Template 3: User Equipment Receipt of Issue 24
- Template 4: Service Provider Non-Disclosure Agreement (NDA) 25
- Template 5: Incident Response Plan (IRP) 26
- Template 6: Incident Response Form 37
- Template 7: Appointment Orders (Information Security Officer) 38
- Template 8: Privileged User Account Request Form 39
- Template 9: Change Management Request Form 40
- Template 10: Change Control Board (CCB) Meeting Minutes 42
- Template 11: Plan of Action & Milestones (POA&M) / Risk Register 43
- Template 12: Ports, Protocols & Services (PPS) 44
- Template 13: Business Impact Analysis (BIA) 45
- Template 14: Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP) 47
- Template 15: Privacy Impact Assessment (PIA) 51

References 53
- Reference 1: CDPP Exception Request Process 53
- Reference 2: Electronic Discovery (eDiscovery) Guidelines 54
- Reference 3: Types of Security Controls 55
- Reference 4: Information Security Management System (ISMS) 56

EXAMPLE

ANNEXES

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.

PUBLIC Public Release Authorized	**INTERNAL USE** Access Limited to Internal Use Only
CONFIDENTIAL Access Limited to Authorized Personnel	**RESTRICTED** Access Limited to Authorized Personnel

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.

EXAMPLE

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*

SAMPLE

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.

SAMPLE

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	