VENDOR CYBERSECURITY COMPLIANCE PROGRAM

[NIST CYBERSECURITY FRAMEWORK ALIGNMENT]

ACME Business Consulting, LLC

Table of Contents

INSTRUCTIONS TO VENDORS

ACME's data protection strategy includes the requirement to ensure the security of data protection controls, regardless of the location or the party responsible for those controls. As a vendor, you serve a crucial role to achieve this goal and your cooperation is greatly appreciated.

All vendors are expected to meet the minimum controls identified in this document. In some cases, ACME may require a written response that may be an attestation of compliance, a submission of supporting documentation, or both.

If ACME requests a written response from your organization, you are required to submit an electronic copy of the document(s) confirming compliance. If there are any requirements that are out of scope or that cannot be complied with, those requirements must be fully explained with a business justification and if there are any compensating controls that may exist to reduce risk associated with one of ACME's vendor requirements not being met.

Please note that if your organization processes, stores or transmits ACME data that is considered “sensitive,” additional data protection controls may be required.

VENDOR COMPLIANCE POLICY

Vendors must protect the confidentiality, integrity, and availability of ACME Business Consulting, LLC (ACME) data and systems, regardless of how the data is created, distributed or stored. Vendors' security controls must be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

Management Intent: The successful implementation of ACME's program depends on the successful implementation of each vendor's security controls.

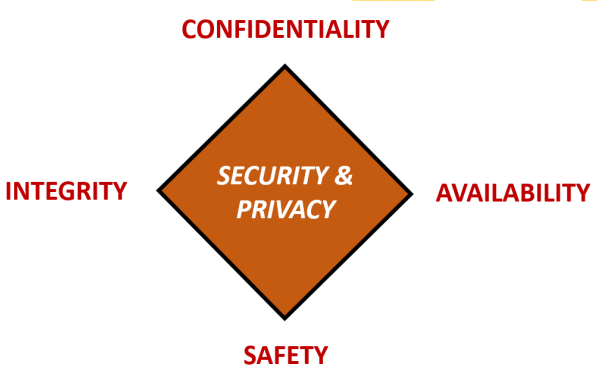
MANAGEMENT DIRECTION FOR VENDOR CYBERSECURITY

- The objective of this Vendor Compliance Program (VCP) to provide direction to vendors for cybersecurity and privacy requirements that are in accordance with ACME's business requirements, as well as relevant laws and other legal obligations for data security and privacy. [1]
-

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 vendor that interacts with ACME data and/or systems. Therefore, it is the responsibility of VENDOR to be aware of and adhere to ACME's cybersecurity and privacy requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems, applications and services must include controls and safeguards to offset possible threats. Commensurate with risk, cybersecurity and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. 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, availability and safety:



- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited 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.
-
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

SCOPE

The requirements of the VCP applies to all vendors that support ACME operations (e.g., suppliers, contractors, consultants, interns or other third-parties). This includes all stakeholders involved in transmitting, processing and storing ACME data.

[1] ISO/IEC 27002:2013 – 5.1

INTENT

ACME's **Minimum Security Requirements (MSR)** for cybersecurity are comprehensive in nature. Therefore, ACME expects VENDOR to also have a comprehensive set of cybersecurity and privacy policies, standards, procedures and controls to protect ACME's data, as well as its systems, applications and services.

VENDOR's cybersecurity program must be reasonably designed to achieve the following objectives:

- Ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of ACME systems, applications, services and data;
- Perform ongoing risk management practices to maintain situational awareness of risk; and
- Reasonably protect against any anticipated threats or hazards.

CYBERSECURITY PRACTICES ALIGNMENT

The National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF) represents leading industry-accepted best practices for cybersecurity.[2] Therefore, ACME's minimum security requirements for its vendors are consistent with NIST CSF controls to ensure due care and due diligence in maintaining its cybersecurity program.

CYBERSECURITY DOCUMENTATION

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 Framework

[2] NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

ACME expects VENDOR to maintain controls that support the National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF). The NIST CSF represents an industry-recognized set of **Minimum Security Requirements (MSR)** for cybersecurity to ensure VENDOR's due care and due diligence in maintaining its cybersecurity program.

Figure 2: NIST Cybersecurity Framework Categories

The NIST CSF is broken up into five (5) NIST CSF-based categories of controls that include: [3]

- Identify
- Protect
- Detect
- Respond
- Recover

IDENTIFY (ID)

These controls are foundational for effective cybersecurity. Understanding the business context, resources that support critical functions and the related cybersecurity risks VENDOR to focus its efforts and resources to properly secure its network.

Controls in this category focus on helping VENDOR understand the following:

- Business context;
- Resources that support critical functions; and
- Related cybersecurity risks.

ASSET & RESOURCE MANAGEMENT (AM)

The Asset Management (ID.AM) section of NIST CSF addresses the data, personnel, devices, systems and facilities that enable an organization to achieve business purposes that are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

HARDWARE MANAGEMENT

VENDOR maintains accurate inventories of its information systems and components.[4]

SOFTWARE MANAGEMENT

VENDOR maintains accurate inventories of its approved operating systems and applications.[5]

DATA FLOW MANAGEMENT

VENDOR documents its data flows (e.g., ports, protocols and services) through network diagrams and/or Data Flow Diagrams (DFDs).[6]

EXTERNAL INFORMATION SYSTEMS

VENDOR identifies and documents information systems and services hosted or maintained by 3rd parties.[7]

RESOURCE VALUE CATEGORIZATION

VENDOR assigns assets and resources a classification based on the business value and criticality in accordance with VENDOR's policies and standards.[8]

[3] NIST SP 800-64 rev2 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf
[4] ID.AM-1
[5] ID.AM-2
[6] ID.AM-3
[7] ID.AM-4
[8] ID.AM-5

Cybersecurity Roles & Responsibilities

VENDOR establishes and documents cybersecurity-related roles and responsibilities for the entire workforce, including third-party stakeholders (e.g., suppliers, partners, service providers, etc.).[9]

Business Environment (BE)

The Business Environment (ID.BE) section of NIST CSF addresses the organization's mission, objectives, stakeholders and activities. This information is used to inform cybersecurity roles, responsibilities and prioritize risk management decisions.

Supply Chain Stakeholders & Interdependencies

VENDOR identifies and documents its role within the supply chain (e.g., business partners, customers) to determine interdependencies and other points of concern that may impact the supply chain.[10]

Business Role Within Industry

VENDOR identifies and documents its role within its industry in an effort to identify applicable industry sector-based risk.[11]

Mission & Objectives

VENDOR establishes and communicates its mission and objectives to ensure organizational awareness of its critical business functions and how that impacts VENDOR's clients.[12]

Dependencies Analysis

- VENDOR identifies and documents dependencies and critical functions within its business processes that impact the delivery of critical services.[13]
-

Resiliency Analysis

VENDOR identifies and documents resilience requirements to support the delivery of critical services.[14]

Governance (GV)

The Governance (ID.GV) section of NIST CSF addresses the policies, standards, procedures and processes to manage and monitor the organization's statutory, regulatory and contractual requirements. These external and internal influencers need to be understood to properly manage cybersecurity risk.

Cybersecurity Policy & Standards

VENDOR documents formal cybersecurity policies, standards and procedures. This cybersecurity-related documentation is clearly made available to VENDOR's workforce.[15]

Cybersecurity Functions

VENDOR coordinates and aligns designated cybersecurity roles with internal and external stakeholders to ensure all applicable cybersecurity and privacy responsibilities are properly addressed.[16]

Statutory, Regulatory & Contractual Obligations

VENDOR adheres to all applicable cybersecurity and privacy-related statutory, regulatory and contractual obligations.[17]

Cybersecurity & Privacy Program

VENDOR maintains a documented program to govern cybersecurity and privacy risks.[18]

[9] ID.AM-6
[10] ID.BE-1
[11] ID.BE-2
[12] ID.BE-3
[13] ID.BE-4
[14] ID.BE-5
[15] ID.GV-1
[16] ID.GV-2
[17] ID.GV-3
[18] ID.GV-4

Availability Protections

VENDOR configures its systems to operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations).[71]

Detect (DE)

These controls focus on situational awareness to ensure the timely identification and response to potential cybersecurity or privacy incidents. By decreasing response time, VENDOR increases its ability to limit or contain incidents with the least negative consequences.

Controls in this category focus on helping VENDOR understand the following:

- How incidents can be detected;
- What constitutes anomalous behavior; and
- How the systems are being logged & monitored.

Anomalies & Events (AE)

The Anomalies and Events (DE.AE) section of NIST CSF addresses the detection of anomalous activity and the understanding of potential event impacts.

Network Traffic Baselines

VENDOR establishes baselines of network traffic and expected data flows to identify what activities that would be considered anomalous behavior.[72]

Event Log Reviews

VENDOR analyzes detected events to understand the target(s) of attack and the methods used.[73]

Event Correlation

VENDOR correlates events logs to improve detection and escalation by bringing together information from different sources to better understand what occurred.[74]

Event Impact Assessment

VENDOR assesses events to determine appropriate response & recovery activities based on the potential impact.[75]

Incident Alerting Thresholds

VENDOR establishes thresholds to manage incident alerting and escalation.[76]

Continuous Monitoring (CM)

The Security Continuous Monitoring (DE.CM) section of NIST CSF addresses the monitoring of information systems to identify cybersecurity events and verify the effectiveness of protective measures.

Network Monitoring

VENDOR monitors network traffic to detect potential cybersecurity events.[77]

Physical Monitoring

VENDOR monitors the physical environment to detect potential cybersecurity events.[78]

[71] PR.PT-5
[72] DE.AE-1
[73] DE.AE-2
[74] DE.AE-3
[75] DE.AE-4
[76] DE.AE-5
[77] DE.CM-1
[78] DE.CM-2