Your Logo
Will Be
Placed Here

CYBERSECURITY VENDOR COMPLIANCE PROGRAM (VCP)

ACME Business Consulting, Inc.

PUBLIC
Public Release Authorized

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 PROGRAM OVERVIEW

VENDOR COMPLIANCE POLICY

Vendors must protect the confidentiality, integrity, and availability of ACME Business Consulting, Inc. (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 INFORMATION SECURITY

The objective of this Vendor Compliance Program (VCP) to provide direction to vendors for information security 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 information security requirements.

Protecting ACME data and the systems that collect, process, and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure the confidentiality, availability and integrity 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 data and systems. This also includes against accidental loss or destruction.

SCOPE

The requirements of the VCP applies to all vendors, contractors, consultants, interns or other third-parties that support ACME.

INTENT

ACME's **Minimum Security Requirements (MSR)** for information security are comprehensive in nature. Therefore, ACME expects VENDOR to also have a comprehensive set of information security policies, standards and controls to protect ACME's data and systems.

VENDOR's information security program must be reasonably designed to achieve the objectives to:

- Ensure the Confidentiality, Integrity and Availability of sensitive Personally Identifiable Information (sPII) and ACME business information;
- Protect against any anticipated threats or hazards to the confidentiality, availability or integrity of such information; and
- Protect against unauthorized access to or use of such information.

[1] ISO/IEC 27002:2013 – 5.1

Best Practices Alignment

The ISO/IEC 27002 represents industry-accepted best practices for information security. Therefore, ACME's minimum security requirements for its vendors are consistent with ISO/IEC 27002 requirements to ensure due care and due diligence in maintaining an information security management program.

Information Security Documentation

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

(1) Core policy that establishes management's intent;
(2) Control objective that identifies the condition that should be met;
(3) Standards that provides quantifiable requirements to be met;
(4) Procedures that establish how tasks must be performed to meet the requirements established in standards; and
(5) Guidelines are recommended, but not mandatory.

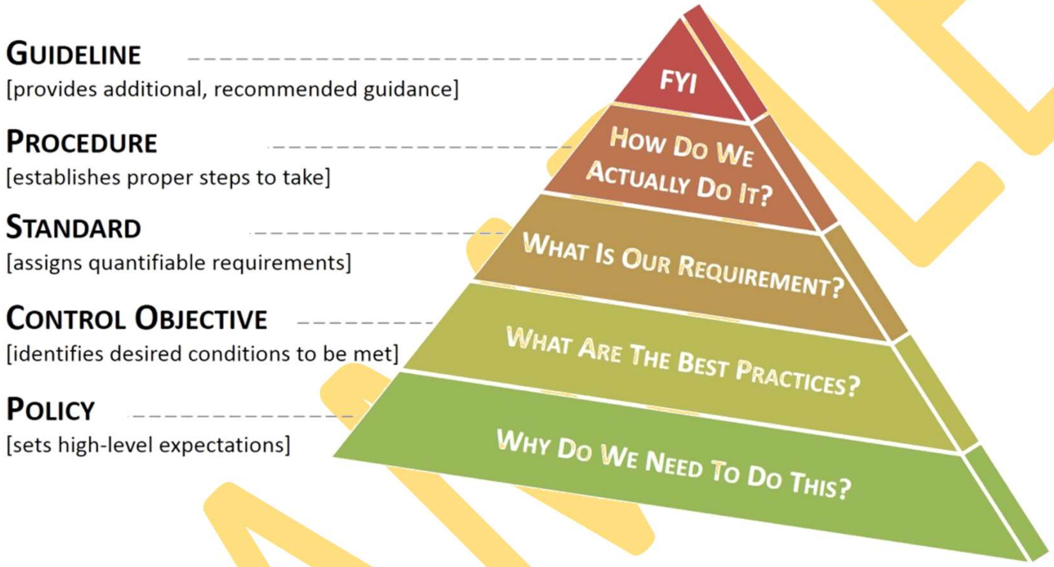
GUIDELINE
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
STANDARD
[assigns quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT IS OUR REQUIREMENT?
WHAT ARE THE BEST PRACTICES?
WHY DO WE NEED TO DO THIS?

Figure 1: Information Security Documentation Framework

VENDOR’S INFORMATION SECURITY RESPONSIBILITIES

INFORMATION SECURITY GOVERNANCE

1. Contract: Before VENDOR can collect, use, transfer or store ACME business information or systems, VENDOR must have a valid contract, statement of work, or purchase order with the privacy and security language in place.

2. Information Security Management: VENDOR must develop a data security program that documents the policies, standards and controls in use that relate to the provisions outlined below. This security plan must include organizational, administrative, technical, and physical safeguards and standards appropriate to the size and complexity, the scope of the activities and the sensitivity of the information at issue.

3. Management Commitment: VENDOR must have executive-level direction on information security and be able to demonstrate management commitment.

4. Information Security Function: VENDOR must have an established information security function that has VENDOR’s enterprise-wide responsibility for promoting information security.

5. ACME-Specific Security Coordination: VENDOR must appoint an individual to coordinate the information security arrangements specific to ACME.

6. Security Audit / Review: The VENDOR’s information security program must be subject to thorough, independent and regular security audits/reviews.

7. Records Retention: VENDOR must maintain a formal records retention program.

INFORMATION SECURITY POLICY

1. Security Policy: VENDOR must have a documented Information Security policy in place which meets applicable industry standards and which is subject to review by ACME under a Non-Disclosure Agreement (NDA). This policy must be reviewed on a regular basis by VENDOR.

2. Security Architecture: VENDOR must establish an information security architecture that provides a framework for the application of standard security controls throughout the VENDOR’s enterprise.

HUMAN RESOURCES SECURITY

1. Requirements for Employment: VENDOR must maintain contractual agreements with employees, contractors, consultants and/or other third party staff that formally documents their responsibilities for information security.

2. Roles and Responsibilities: VENDOR must define and document security roles and responsibilities of employees, contractors and third party users to incorporate ACME’s data protection control requirements, to the extent permitted by applicable law:
   a. All employees, contractors, and third-party users must be notified of the consequences for not following your security policy in handling ACME data.
   b. All assets used to manage or store ACME data must be protected against unauthorized access, disclosure, modification, destruction or interference.
   c. All employees, contractors and third party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.
   d. All personnel with access to sensitive Personally Identifiable Information (sPII) must complete a privacy training class and be knowledgeable of any specific privacy requirements for the data being handled. Refresher training is required at least on an annual basis.

        i. Access lists must be reviewed and updated at least once per quarter.
    c. Process, training and policies must be in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.
    d. Emergency exits in controlled areas must sound an alarm when opened and include automatic closure.
        i. Any alarms must trigger an emergency response.

2. <u>Physical Protection</u>: VENDOR must actively manage the physical security controls and ensure all buildings throughout the VENDOR's enterprise that house critical IT functions (e.g., data centers, network facilities and key user areas) are physically protected from unauthorized access.

3. <u>Hazard Protection</u>: VENDOR must ensure computer equipment and facilities are protected against natural and man-made hazards.

4. <u>Power Supplies</u>: VENDOR must protect critical computer equipment and facilities against power outages.

SYSTEM CONFIGURATION

1. <u>Host System Configuration</u>: VENDORS must configure host systems according to an industry standard.
    a. Systems must be configured to function as required and to prevent unauthorized actions.
    b. Examples of best practice configuration include, but are not limited to:
        i. Center for Internet Security (CIS)
        ii. US Department of Defense Secure Technical Implementation Guides (STIGs)
        iii. OEM best practices (e.g., Microsoft, VMware, Oracle, etc.)

2. <u>Mobile Devices</u>: VENDOR must maintain policies, standards and procedures covering the use of mobile/portable devices.
    a. The use of mobile devices (e.g., smart phone, iPad, tablet, USB memory sticks, external hard disk drives, MP3 players, e-book readers, etc.) must be:
        i. Subject to approval; and
        ii. Access must be restricted.
    b. Controls must be implemented to ensure that sensitive information stored on these devices is protected from unauthorized disclosure.

SYSTEM MONITORING

1. <u>Event Logging</u>: VENDOR must log all key information security events, including but not limited to:
    a. All actions taken by any individual with root or administrative privileges;
    b. Access to all audit trails;
    c. Invalid logical access attempts;
    d. All individual user accesses to cardholder data;
    e. Use of and changes to identification and authentication mechanisms, including but not limited to:
    f. Creation of new privileged accounts and elevation of privileges; and
    g. All changes, additions, or deletions to accounts with root or administrative privileges;
    h. Initialization, stopping, or pausing of the audit logs; and
    i. Creation and deletion of system-level objects.

2. <u>System Network Monitoring</u>: VENDOR is required to develop and implement a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes:
    a. Reviewing the following, at least daily:
    b. All security events;
    c. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
    d. Logs of all critical system components; and
    e. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
        i. Firewalls;
        ii. Intrusion Detection Systems (IDS);
        iii. Intrusion Prevention Systems (IPS); and