Your Logo
Will Be
Placed Here

Vendor Cybersecurity Compliance Program

ACME Business Solutions, Inc.

ISO

VCP
Vendor Compliance Program

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 Solutions, 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 Cybersecurity

The objective of this Vendor Compliance Program (VCP) to provide direction to vendors for cybersecurity 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 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 cybersecurity are comprehensive in nature. Therefore, ACME expects VENDOR to also have a comprehensive set of cybersecurity policies, standards and controls to protect ACME's data and systems.

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

- Ensure the Confidentiality, Integrity, and Availability (CIA) 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.

Best Practices Alignment

The ISO/IEC 27002 represents industry-accepted best practices for cybersecurity. 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 a cybersecurity management program.

[1] ISO/IEC 27002:2013 – 5.1

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 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.

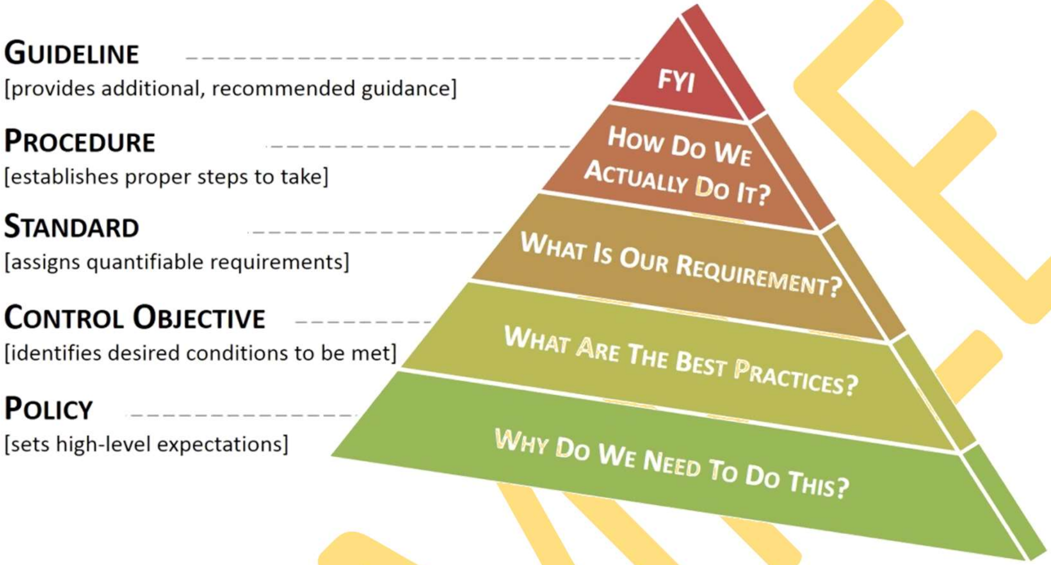
GUIDELINE
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
STANDARD
[assigns quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT IS OUR REQUIREMENT?
WHAT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

Figure 1: Cybersecurity Documentation Framework

VENDOR'S CYBERSECURITY RESPONSIBILITIES

CYBERSECURITY 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. Cybersecurity 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 cybersecurity and be able to demonstrate management commitment.

4. Cybersecurity Function: VENDOR must have an established cybersecurity function that has VENDOR's enterprise-wide responsibility for promoting cybersecurity.

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

6. Cybersecurity Audit / Review: The VENDOR's cybersecurity program must be subject to thorough, independent and regular security audits/reviews.

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

CYBERSECURITY POLICY

1. Cybersecurity Policy: VENDOR must have a documented cybersecurity 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. Cybersecurity Architecture: VENDOR must establish a cybersecurity 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 cybersecurity.

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.

3. Assigned Ownership: VENDOR must assign ownership of critical and sensitive information, business applications, computer systems and networks to individuals (e.g., business managers) and document the responsibilities of these assigned owners.
    a. Responsibilities for protecting critical and sensitive information, business applications, computer systems and networks must be communicated to and accepted by owners.

4. Personnel Screening: VENDOR must ensure a secure workforce. Background verification checks on all VENDOR's candidates for employment should be carried out in accordance with relevant laws, regulations, and ethics and should be proportional to the business requirements and the classification of the information that may be accessed.

5. Staff Agreements: VENDOR must establish agreements with VENDOR's employees and/or VENDOR's employee representative that specify cybersecurity responsibilities. This agreement must be incorporated into the contracts of VENDOR's employees, contractors, consultants and/or other third party staff and be taken into account when screening applicants for employment.

Cybersecurity Education & Awareness

1. Cybersecurity Awareness: VENDOR's employees, contractors, consultants and/or other third party staff must be made aware of the key elements of cybersecurity, why it is needed, and understand their personal cybersecurity responsibilities. A security awareness program must be undertaken to promote security awareness to all individuals who have access to the information and systems of the VENDOR's enterprise.

2. Cybersecurity Education: VENDOR's employees, contractors, consultants and/or other third party staff must be trained in how to run systems correctly, as well as how to develop and apply security controls.

Information Risk Analysis

1. Risk Analysis: VENDOR must perform information risk assessments of critical areas of its business to identify key information risks and determine the controls required to keep those risks within acceptable limits.
    a. Assessments must include, but are not limited to:
        i. Business environments;
        ii. Business processes;
        iii. Business applications (including those under development);
        iv. Computer systems, and
        v. Networks.
    b. VENDOR is required to provide ACME with a documented analysis of how key threats, as identified above in section 1(a), are addressed, as it applies to ACME.

2. Confidentiality Requirements: Non-disclosure agreements must be signed by Vendors prior to being granted access to ACME information.
    a. VENDOR must assess and immediately escalate to ACME about the impact of business information being accidentally or deliberately released to unauthorized parties.
    b. The analysis of integrity requirements must determine how the disclosure of information could have an impact on ACME's business operations with the VENDOR.

3. Integrity Requirements: VENDOR must assess and immediately escalate to ACME about the impact of business information being accidentally corrupted or deliberately manipulated. The analysis of integrity requirements must determine how the accidental corruption or deliberate manipulation of information could have an impact on ACME's business operations with the VENDOR.

4. Availability Requirements: VENDOR must assess and immediately escalate to ACME about the impact of business information being unavailable for any length of time. The analysis of availability requirements must determine how a loss of availability of information could have an impact on ACME's business operations with the VENDOR.

    ix. Process and advise ACME of any security breach involving ACME data or services utilized by ACME; and
    x. Provide ACME with the means to monitor in near real-time service and resource availability; and

  c. All access to cloud computing sites must encrypt data in transit.
    i. Any ACME data stored in a cloud environment must be encrypted either by the VENDOR or the application so that data cannot be read by other users in a multi-tenant environment.

Vendor Management

1. Outsourcing: VENDOR must operate a formal process to address due care and due diligence considerations in the selection and management of third-party VENDORS:
    a. These third-party VENDORS must sign agreements that specify the security requirements to be met before commencing work on behalf of VENDOR that could have an impact on ACME's business operations with the VENDOR;
    b. These security requirements must align with the provisions expected of ACME from VENDOR; and
    c. All subcontracted activities involving ACME information must be approved and secured by VENDOR.

2. VENDOR Exit Strategy: VENDOR must ensure a documented termination of service process is in place that ensures ACME business data is recoverable if must VENDOR terminates a service agreement with a third party VENDOR.

3. Indemnification: VENDOR must address indemnification considerations with third-party VENDORS that could have an impact on ACME's business operations with the VENDOR.

Compliance

1. Statutory / Regulatory / Contractual Compliance. VENDOR must maintain a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements. Examples include but are not limited to PCI DSS, HIPAA, SOX, and GLBA.

2. Compliance Status: VENDOR must have a process to document non-compliance of any statutory, regulatory or contractual requirement:
    a. VENDOR must identify and quantify the risks and mitigation plans and document the business decision for alternate controls or risk acceptance; and
    b. The mitigation plan and business decision must be signed off by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability on behalf of the VENDOR.

3. Breach Notification: VENDOR must maintain a documented breach notification process that meets all applicable legal and contractual requirements. The ACME business owner of the solution must:
    a. Approve VENDOR breach notification process; and
    b. Own the ACME response process.

4. Payment Card Industry Data Security Standard (PCI DSS): If VENDOR's solution processes, stores or transmits ACME customers' cardholder data, VENDOR falls within scope of ACME's PCI DSS compliance and therefore must:
    a. Maintain documented compliance with the most current version of the PCI DSS;
    b. Conduct quarterly network scans by an Approved Scanning Vendor (ASV); and
    c. Obtain a Report of Compliance (ROC) from an annual on-site PCI Data Security Assessment with a Qualified Security Assessor (QSA).
        i. VENDOR may provide an annual Self-Assessment Questionnaire (SAQ) in lieu of an annual ROC that is issued by a QSA.

5. Notification of Inquiries: VENDOR must immediately inform ACME, in writing of any:
    a. Request for access to any Personal Information received by VENDOR from an individual who is (or claims to be) the subject of the data, or a request to cease or not begin processing, or to rectify, block, erase or destroy any such Personal Information;
    b. Request for access to any Personal Information received by VENDOR from any government official (including any data protection agency or law enforcement agency), or a request to cease processing, or to rectify, block, erase or destroy any such Personal Information;

c. Inquiry, claim or complaint regarding the Processing of the Personal Information received by VENDOR;
d. Other requests with respect to Personal Information received from ACME's employees or other third parties, other than those set forth in the agreement or a request to cease or not begin processing, or to rectify, block, erase or destroy any such Personal Information.

6. European Union General Data Protection Regulation (EU GDPR): VENDOR must be willing to sign a Data Processing Agreement with ACME.
   a. All VENDOR-provided systems and applications must satisfy EU GDPR requirements; and
   b. VENDOR must be capable of:
      i. Delivering the solution according to "privacy by design" principles; and
      ii. Supporting incident response operations to meet EU GDPR requirements.

7. Data Minimization: VENDOR may collect no more personal information from individuals than the minimum necessary to achieve the business goal. This business goal must be documented and be shared with ACME.

Glossary: Acronyms & Definitions

Acronyms

AD. Active Directory
APT. Advanced Persistent Threat
BCP. Business Continuity Plan
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
COOP. Continuity of Operations Plan
CTI. Controlled Technical Information [2]
CUI. Controlled Unclassified Information [3]
DAC. Discretionary Access Control
DISA. Defense Cybersecurity Agency
DLP. Data Loss Prevention
DRP. Disaster Recovery Plan
EAP. Extensible Authentication Protocol
EPHI. Electronic Protected Health Information
FICAM. Federal Identity, Credential, and Access Management
FIM. File Integrity Monitor
GDPR. General Data Protection Regulation
HIPAA. Health Insurance Portability and Accountability Act
IRP. Incident Response Plan
ISMS. Cybersecurity Management System
ISO. International Organization for Standardization
LDAP. Lightweight Directory Authentication Protocol
MAC. Media Access Control
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard
PDCA. Plan-Do-Check-Act
PIV. Personal Identity Verification
RBAC. Role-Based Access Control
TLS. Transport Layer Security

Definitions

ACME recognizes two sources for authoritative definitions:

- Unified Compliance Framework (UCF) Compliance Library[4]
- The National Institute of Standards and Technology (NIST) IR 7298, Revision 2, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms. [5]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (i.e., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method, or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[6]

[2] CUI Registry - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html
[3] CUI Registry - https://www.archives.gov/cui/registry/category-list
[4] UCF Compliance Library - https://compliancedictionary.com
[5] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
[6] ISO/IEC/IEEE 29148