Your Logo
Will Be
Placed Here

Vendor Cybersecurity Compliance Program

[ISO/IEC 27002:2013 Cybersecurity Requirements]

ACME Business Consulting, LLC

PUBLIC
Public Release Authorized

Table of Contents

INSTRUCTIONS TO VENDORS

ACME Business Consulting, LLC (ACME) takes data protection seriously and part of ACME's data protection strategy includes the requirement to ensure the adequacy of data protection controls, regardless of the location or the party responsible for those controls. As a vendor to ACME, 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.

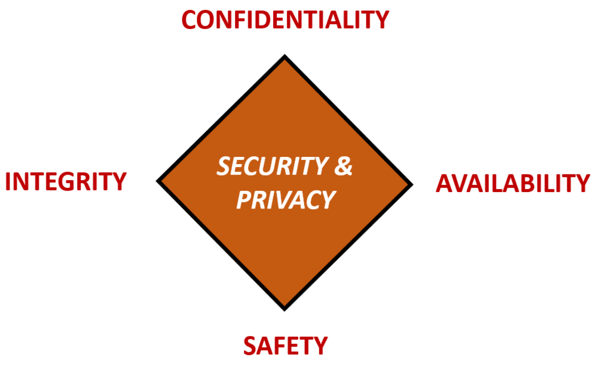
Management Direction for Vendor Cybersecurity

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 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 (2013 version) requirements to ensure due care and due diligence in maintaining a cybersecurity management 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.

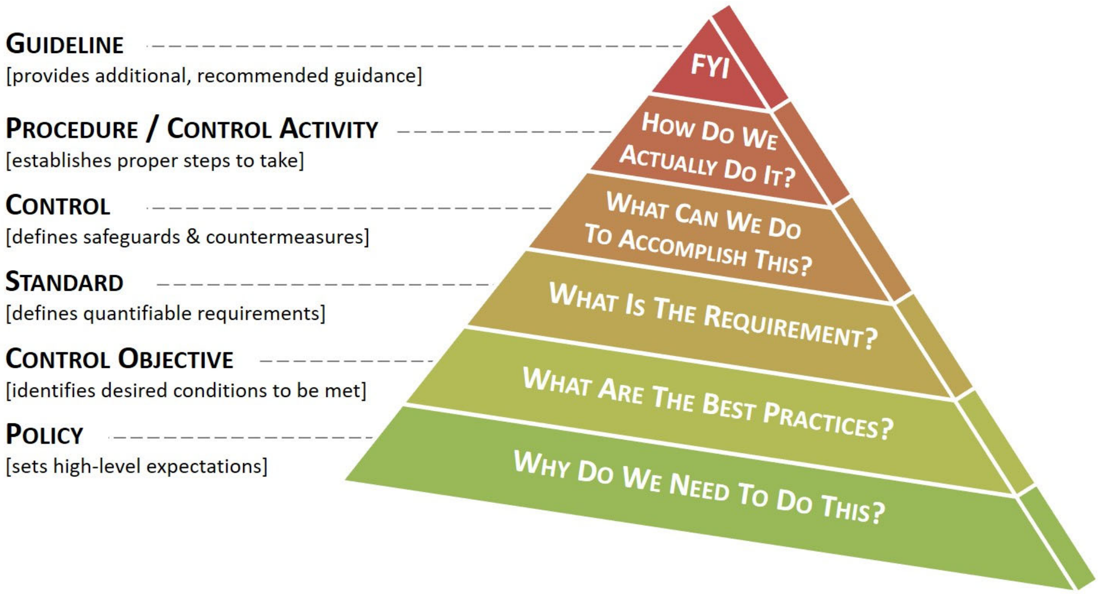

GUIDELINE
[provides additional, recommended guidance]
PROCEDURE / CONTROL ACTIVITY
[establishes proper steps to take]
CONTROL
[defines safeguards & countermeasures]
STANDARD
[defines quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT CAN WE DO TO ACCOMPLISH THIS?
WHAT IS THE 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.

2. Alignment with ACME Privacy: VENDOR must ensure sPII is collected, used, stored, transferred, and destroyed according to ACME's privacy requirements.

Malware Protection

1. Malware Controls: VENDOR must implement and manage enterprise-wide detection, prevention and recovery controls to protect against malware that includes having procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.

2. Malware Prevention: VENDOR must ensure the installation and regular update of malware detection and repair software to scan systems and media as a precautionary control, or on a routine basis. The scan carried out should include:
   a. Scan any files received over networks or via any form of storage medium, for malware before use;
   b. Scan electronic mail attachments and downloads for malware before use; and
   c. Scan web pages for malware.

Vulnerability Management

1. Vulnerability Management: VENDOR must ensure a vulnerability management program exists to eliminate vulnerabilities that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). This includes, but is not limited to:
   a. Vulnerability remediation;
   b. Software and firmware patching; and
   c. Hardware maintenance.

2. Web-Enabled Applications: VENDOR must implement and manage specialized technical controls for web-enabled applications to ensure that the increased risks associated with web-enabled applications are minimized:
   a. All internets facing websites must be scanned for security vulnerabilities that potentially open the site up to malicious behavior.
   b. ACME's minimum list of validation is the Open Web Application Security Project (OWASP) Top 10 vulnerabilities (e.g., cross-site scripting (XSS), SQL injection, Admin access, open directories, insecure data transfer, etc.).

Communications & Operations Management

1. Communications Security: VENDOR must support standards and procedures that ensure confidentiality, integrity, and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

2. Operations Management: VENDOR must maintain sufficient overall operational control and visibility into all security aspects of how data is processed, stored and transmitted:
   a. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility;
   b. Vendor must have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process; and
   c. Vendors are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

System Acquisition, Development & Maintenance

1. Specification of Requirements: VENDOR must take into consideration the cybersecurity requirements for the system under development when designing the system to ensure ACME's business requirements (including those for cybersecurity) are documented and agreed upon before detailed design commences.