Vendor Management Policy

ACME Evil Anvil Corporation

March 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners.

b. This policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of the organization's technology and sensitive information, or who are within the scope of the organization's information security program.

c. This policy applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of the organization.

2 Background

a. The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

3 References

a. Information Security Policy

b. Security Incident Response Policy

4 Policy

a. IT vendors are prohibited from accessing the organization's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

b. All IT vendors must comply with the security policies defined and derived from the Information Security Policy (reference (a)).

c. All security incidents by IT vendors or partners must be documented in accordance with the organization's Security Incident Response Policy (reference (b)) and immediately forwarded to the Information Security Manager (ISM).

d. The organization must adhere to the terms of all Service Level Agreements (SLAs) entered into with IT vendors. As terms are updated, and as new ones are entered into, the organization must implement any changes or controls needed to ensure it remains in compliance.

e. Before entering into a contract and gaining access to the parent organization's information systems, IT vendors must undergo a risk assessment.

    i. Security risks related to IT vendors and partners must be identified during the risk assessment process.

    ii. The risk assessment must identify risks related to information and communication technology, as well as risks related to IT vendor supply chains, to include sub-suppliers.

f. IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The organization strictly adheres to all applicable legal, regulatory and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).

g. The organization may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.