Third-Party Management Policy

Vendor and Supply Chain Management

SA

Secured approach  www.securedapproach.com

Use Disclaimer: This policy has been developed by Secured Approach Inc. for the benefit of the community. You are welcome to use this policy, in whole or in part, for your organization without the need for prior approval. Should you wish to contribute to creating or updating a new version of this policy, please reach out to us via email at resources@securedapproach.com.
Furthermore, if you require assistance in crafting a tailored security policy for your specific environment, do not hesitate to contact us at support@securedapproach.com.

Table of Contents

[Confidentiality Statement 2](#_Toc159342276)

[Disclaimer 2](#_Toc159342277)

[1. Overview 2](#_Toc159342278)

[2. Purpose 2](#_Toc159342279)

[3. Scope 2](#_Toc159342280)

[4. Policy 3](#_Toc159342281)

[4.1 Third-Party Lifecycle Management 3](#_Toc159342282)

[4.2 Third-Party Risk Management 3](#_Toc159342283)

[5. Policy Compliance 3](#_Toc159342284)

[5.1 Compliance Measurement 3](#_Toc159342285)

[5.2 Exceptions 3](#_Toc159342286)

[5.3 Non-Compliance 4](#_Toc159342287)

[6. Related Standards, Policies, and Processes 4](#_Toc159342288)

[7. Revision History 4](#_Toc159342289)

# Confidentiality Statement

This document contains proprietary and confidential information of [Organization Name] and is intended solely for the use of its employees and authorized third parties. Unauthorized distribution, duplication, or disclosure of this document or its contents is strictly prohibited and may result in disciplinary action.

# Disclaimer

This Third-party Management Policy is subject to change and may be updated periodically to reflect the evolving business environment, regulatory requirements, and best practices in third-party risk management. It is the responsibility of all employees and relevant third parties to remain informed about policy updates.

# Overview

The Third-party Management Policy establishes guidelines for the management of third-party relationships, including vendors, contractors, and service providers, to ensure that these relationships do not compromise the security, confidentiality, integrity, and availability of [Organization Name]'s information assets.

# Purpose

To define the responsibilities and processes for effectively managing third-party risks, ensuring compliance with regulatory requirements, and safeguarding [Organization Name]'s information assets throughout the lifecycle of the third-party relationship.

# Scope

This policy applies to all employees and business units within [Organization Name] involved in the selection, engagement, and management of third parties that have access to the organization's information systems and data.

# Policy

## Third-Party Lifecycle Management

* Always follow the predefined processes for the onboarding and offboarding of third parties to ensure all security requirements are met and terminated appropriately.
* Maintain an up-to-date inventory of all third parties and vendors, including services provided, data accessed, and risk assessments.
* Collaborate with the legal department to ensure all contracts and Service Level Agreements (SLAs) include necessary security requirements, compliance obligations, and data protection measures.

## Third-Party Risk Management

* Coordinate with the security department to perform thorough risk assessments of third parties prior to engagement and periodically throughout the relationship.
* Require third parties to promptly report any security incidents or breaches that may impact [Organization Name], including a clear process for escalation and response.
* Establish procedures for the ongoing monitoring of third-party compliance with [Organization Name]'s security policies and standards.
* Reserve the right to audit third parties to verify compliance with this policy and relevant security requirements.

# Policy Compliance

## Compliance Measurement

Regular reviews and audits will be conducted to assess compliance with the Third-party Management Policy.

## Exceptions

Any exceptions to this policy must be submitted in writing with a business justification and approved by the IT Security Department or relevant authority within the organization.

## Non-Compliance

Violations of this policy may result in disciplinary action, up to and including termination of access, employment, legal action, and financial liabilities.

Non-compliance by a Third-Party with the provisions of this policy may result in termination of the relationship, along with potential legal and financial repercussions.

# Related Standards, Policies, and Processes

* Acceptable Use Policy
* Identity and Access Management Policy
* Remote Access Policy
* Data Protection Policy
* Security Awareness Policy

# Revision History

This policy will be reviewed and updated annually or as needed to reflect changes in technology, legal requirements, and organizational priorities. The revision history will be documented here, including the date of the revision, a brief description of the changes, and the version number.

|  |  |  |  |
| --- | --- | --- | --- |
| Date of Change | Responsible | Summary of Change | Version |
| January 2024 | Information Security Manager | Building the first draft | 1.0 |
| January 2024 |  |  |  |
|  |  |  |  |