Cloud Service Provider Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company uses Cloud service providers to increase employee efficiency, improve our competitive edge, and enhance our image and reputation. Over the past several years, Cloud services have expanded so that almost any resource or service can be rapidly provisioned at low cost and with a minimal amount of effort.

# II. Purpose

Cloud services provide convenient and on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services). The purpose of this policy is to establish the rules for the use of Cloud service providers, their responsibilities, and protection of ABC Company information.

# III. Scope

This policy applies to all ABC Company staff. It applies to Cloud service providers that transmit, collect, store, process, manage, and dispose of ABC Company’s information.

# IV. Policy

Cloud technology has expanded and allows almost any IT related resource to be offered as a service. By knowing the types of Cloud environments available, ABC Company Staff can make informed business decisions. The following are examples of solutions offered by Cloud service providers:

* Anything as a Service (XaaS)
* Communication as a Service (CaaS)
* Database as a Service (DaaS)
* Infrastructure as a Service (IaaS)
* Monitoring as a Service (MaaS)
* Network as a Service (NaaS)
* Platform as a Service (PaaS)
* Security as a Service (SecaaS)
* Software as a Service (SaaS)
* Storage as a Service (STaaS)
* Voice as a Service (VaaS)

Examples of Cloud service providers include, but are not limited to, infrastructure (e.g. Amazon Web Services, Microsoft Azure, Rackspace Hosting), platform (e.g. Google Apps, Salesforce), Internet mail systems (e.g. Yahoo!, Hotmail, Gmail), social media (e.g. LinkedIn, Facebook), storage (e.g. Google, Microsoft, Box), on-line backups (e.g. Carbonite, zip cloud), and related services.

When adopting a Cloud service provider technology, ABC Company Staff shall consider the risks involved. A Risk Assessment shall be performed that identifies risks to the organization. A risk analysis shall be performed to determine the likelihood and impact of various events. A risk treatment plan shall be prepared that identifies preventive, detective, and corrective controls that reduce risks to acceptable levels. See the Risk Assessment Policy for more information.

Prior to entering into an agreement, ABC Company Staff shall follow due diligence in selecting the Cloud service provider. This may include background checks of Cloud service provider and related personnel, length of time in business, experience with similar engagements, etc.

Staff shall ensure that the use of a specific Cloud service provider does not violate ABC Company policies, procedures, agreements, and related documents. ABC Company will provide an IT point of contact for the Cloud service provider. The point of contact will work with the Cloud service provider to ensure the Cloud service provider is in compliance with the above policies, procedures, agreements, and related documents.

ABC Company IT Management shall maintain a list of all authorized Cloud service providers and the services performed by each. IT Management shall maintain copies of all agreements with Cloud service providers.

Agreements with Cloud service providers must specify:

* Confidentiality that protects ABC Company’s information as well as our customer information.
* Controlled access to ABC Company information.
* How ABC Company’s information is protected by the Cloud service provider.
* Acceptable methods for the return, destruction, or disposal of ABC Company information in the Cloud service provider’s possession at the end of the agreement.
* The Cloud service provider must only use ABC Company information and Information Resources for the purpose of the business agreement.
* Any other ABC Company information acquired by the Cloud service provider in the course of the contract cannot be used for the Cloud service provider’s own purposes or divulged to others.

Cloud service provider staff with access to ABC Company Sensitive Information must be cleared to handle that information. Cloud service provider access to Sensitive Information shall be activated only when needed. Access shall be deactivated after services have been provided.

Cloud service provider staff shall report any security incidents directly to the appropriate ABC Company personnel.

Upon Cloud service provider termination, the Cloud service provider shall ensure that all ABC Company Sensitive Information is collected and returned to ABC Company or destroyed within 24 hours. If requested by the ABC Company Chief Security Officer (CSO), the Cloud service provider shall return or destroy all ABC Company information and provide written certification of that return or destruction within 24 hours.

Cloud service providers are required to comply with all State and ABC Company auditing requirements, including the auditing of the Cloud service provider’s work.

Agreements with Cloud service providers shall include explicit coverage of all relevant security requirements. Agreements shall include controls over the processing, accessing, communicating, hosting or managing the organization's Information Resources or adding or terminating services or products to existing information. Agreements shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.

Agreements with Cloud service providers shall specify that the service provider will notify ABC Company within 72 hours of discovery of a Cloud service provider security breach. Upon such notification, ABC Company shall have the right, but not the obligation, to terminate the agreement with the Cloud service provider. If the Cloud service provider had access to ABC Company customer information, the Cloud service provider shall pay for all costs incurred to remedy the breach including, if appropriate, notifying ABC Company’s customers, paying for one year of free credit report for ABC Company’s customers, and related expenses.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO01.11, APO09.05, APO10.05, APO11.09, APO13.07, DSS01.05

GDPR Article 24, 28

HIPAA 164.308(b)(4), HITECH ARRA 13402

ISO 27001 8.3, A.5.1.1, A.17

NIST SP 800-37 Appendix G

NIST 800-53 CP-2

NIST Cybersecurity Framework ID.SC-4-5, DE.CM-6, RS.MI-2

PCI 2.6, 3.5.1, 3.6, 8.2.3 - 8.2.5, 8.5.1, 10.8