Third Party Service Providers 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

Third party service providers play an important role in the support of the IT infrastructure and providing information services. In some instances, service providers may collect, store, and maintain Sensitive Information. Setting limits and controls on third party service providers helps eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to ABC Company.

# II. Purpose

The purpose of this policy is to establish the rules for service provider access to company information, third party responsibilities, and protection of ABC Company information.

# III. Scope

This policy applies to all Staff responsible for the installation of new Information Resources assets, the operations and maintenance of existing Information Resources, monitoring and troubleshooting of Information Resources. It applies to third party service providers that collect, store, process, manage, and dispose of ABC Company’s information.

# IV. Policy

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

Service providers must comply with all applicable ABC Company policies, practice standards and agreements, including, but not limited to:

* Acceptable Use Policy
* Anti-Malware Policy
* Approved Application Policy
* Audit Policy
* Bring Your Own Device Policy
* Data Privacy Policy
* E-mail Policy
* Guest Access Policy
* Identification and Authentication Policy
* Network Security Policy
* Outsourcing Policy
* Password Policy
* Personnel Security Policy
* Physical Access Policy
* Physical Security Policy
* Remote Access Policy
* Removable Media Policy
* Secure Software Development Lifecycle Policy
* Security Policy
* Software Development Policy
* Staffing Policy
* User Privilege Policy
* Vendor Access Policy

As appropriate, service providers shall comply with ABC Company’s compliance related policies including, but not limited to:

* Certification and Accreditation Policy
* Compliance Policy
* Electronic Data Retention Policy
* HIPAA and HITECH Policy
* PCI Policy

ABC Company will provide an IT point of contact for the service provider. The point of contact will work with the service provider to ensure the service provider is in compliance with the above policies.

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

Agreements with third party service providers must specify:

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

Each service provider must provide ABC Company with a list of all staff working to provide services to ABC Company. The list must be updated and provided to ABC Company within 24 hours of staff changes.

Each on-site service provider Staff member must acquire an ABC Company identification badge that will be displayed at all times while on ABC Company premises. The badge must be returned to ABC Company when the service provider’s Staff member leaves the premises.

Each service provider staff member with access to ABC Company Sensitive Information must be cleared to handle that information. Third party access to Sensitive Information shall be activated only when needed. Access shall be deactivated after services have been provided. IDs used by vendors to access, support, or maintain system components via remote access shall only be enabled during the time period needed and disabled when not in use. Third party service provider access to Information Systems shall be monitored during use.

Service providers with remote access to customer premises (e.g. for support of Point of Sale devices or servers) must use a unique authentication credential (i.e. password/phrase) for each client.

Service provider personnel must report all security incidents directly to the appropriate ABC Company personnel. If service provider management is involved in ABC Company security incident management the responsibilities and details must be specified in the agreement.

Service provider must follow all applicable ABC Company change control processes and procedures.

Regular work hours and duties will be defined in the agreement. Work outside of defined parameters must be approved in writing by appropriate ABC Company management.

All service provider maintenance equipment on the ABC Company network that connects to the outside world via the network, telephone line, or leased line, and all ABC Company IT service provider accounts will remain disabled except when in use for authorized maintenance.

Service provider access must be uniquely identifiable and password management must comply with the ABC Company Password Policy. Service provider’s major work activities must be entered into the Third Party Service Provider Log Form and made available to ABC Company management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

Upon departure of a service provider staff from the agreement for any reason, the service provider will ensure that all Sensitive Information is collected and returned to ABC Company or destroyed within 24 hours. Upon termination of service provider or at the request of ABC Company, the service provider will return or destroy all ABC Company information and provide written certification of that return or destruction within 24 hours.

Upon termination of contract or at the request of ABC Company, the service provider must surrender all ABC Company identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the service provider must be documented by authorized ABC Company management.

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

All software used by the service provider in providing service to ABC Company must be properly inventoried and licensed.

Agreements with third party 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 third party service providers shall require the provider to acknowledge that they are responsible for the security of ABC Company sensitive information the service provider possesses or otherwise stores, processes, or transmits on behalf of ABC Company to the extent that they could impact the security of the data environment.

Agreements with third party service providers shall specify that the third party service provider will notify ABC Company within five (5) working days of discovery of a service provider security breach. Upon such notification, ABC Company shall have the right, but not the obligation, to terminate the agreement with the service provider. If the service provider had access to ABC Company customer information, the 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.

When dealing with health information, service providers shall provide an on-line and print description of security and privacy directives, guidelines, policies, and security safeguards that protect Sensitive Information.

# V. Enforcement

Any Staff member 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 Staff responsible for the installation of new Information Resources assets, the operations and maintenance of existing Information Resources, monitoring and troubleshooting of Information Resources.

**Policy History**

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

**References:**

COBIT APO09.05, APO10.05, APO12.02, APO13.07, BAI02.05-06, DSS01.05, DSS05.07

GDPR Article 25, 26, 28, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(b)(4), 164.502(b)(1), ARRA 13404(b), ARRA 13405(b)

ISO 27001:2013 8.1, A.13.1.2, A.14.2.7

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 PS-7, RA-9, SA-4, SA-10-12, SA-15, SA-17

NIST Cybersecurity Framework ID.AM-4-6, ID.BE-4, ID.RA-4, ID.RM-1, ID.SC-3-4, DE.CM-6

PCI 12.8, PCI Software Security Framework