Outsourcing 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 outsourcing as a means of reducing costs, accessing specialist expertise, and providing greater focus on non-core functions. This process must be managed to ensure the proper benefits are received and risks remain within acceptable levels.

# II. Purpose

Outsourcing involves the use of third party service providers to perform activities on a continuing basis (including agreements for a limited period), that would normally be undertaken by ABC Company. This policy manages the risks related to outsourcing.

# III. Scope

This policy applies to all Staff responsible for outsourcing ABC Company functions and activities.

# IV. Policy

Department Heads shall ensure that outsourcing arrangements do not diminish ABC Company’s ability to meet our contractual and compliance obligations. Procedures shall be identified to ensure that the outsource provider employs the same standard of care in performing the services as would be employed by ABC Company. Department Heads shall not engage in outsourcing activities that have a high likelihood of damaging ABC Company’s image and reputation.

Per the Risk Assessment Policy, The Risk Assessment and Risk Treatment Plan shall be reviewed on an annual basis to ensure that controls are sufficient and effective at treating risks. During the annual review, Department Heads shall review risks and controls related to outsourcing. Material outsourcing arrangements have the potential to significantly impact ABC Company’s business operations, reputation, and profitability. Department Heads shall use the following indicators to determine outsourcing materiality:

* The level of importance of the service provided by the outsourcer
* The potential impact on our organization should the outsourcer be unable to provide services
* The potential impact of an outsourcer security breach
* Outsourcer costs and related cost controls

Outsourcing risks that should be evaluated and analyzed by the Department Heads include:

* Strategic Risk – the outsourcer may conduct business in a manner inconsistent with that of ABC Company
* Image Risk – unsatisfactory performance may impact ABC Company’s image and reputation
* Operational Risk – the server provider many experience a failure in business operations and be unable to meet its contractual service levels or performance obligations
* Compliance Risk – ABC Company may face compliance related risks related to privacy, security, and regulatory issues
* Legal Risk – ABC Company may be faced with fines or penalties
* Termination Risk – the loss of in-house Staff with specific skill sets might make it more difficult to terminate an agreement with an outsourcer

Outsourcing to any third party service provider can create risks that must be managed, regardless of the location of the provider. Outsourcing to cross-border jurisdictions presents additional risks that must be managed:

* Issues related to distance and/or different time zones
* Risks related to the actions of foreign governments
* Relying on a foreign legal system for enforcement

When analyzing an outsourcing arrangement, Department Heads should consider:

* The ability of the service provider to comply with its obligations and meet the performance service levels required by the department
* The compatibility of ABC Company’s Information Resources with those of the service provider
* Excessive outsourcing arrangements with the service provider
* Outsourcer staff is subjected to background checks equivalent to those performed on ABC Company’s Staff

The outsourcing of any activity does not diminish our obligations and those of Executive Management who have the ultimate responsibility for the outsourced activity. Outsourcing a business process or function shall not interfere with the ability of a department to effectively oversee and manage its activities.

ABC Company is responsible for the actions of the outsourcer and the confidentiality of information collected, transmitted, stored, or processed by the third party service provider. Department Heads shall consider compliance, contractual, and legal requirements when qualifying, evaluating, and selecting an outsourcer. Department Heads shall comply with ABC Company’s Third Party Service Providers Policy.

Department Heads shall:

* Communicate material outsourcing risks to Executive Management in a timely manner
* Ensure procedures are in place to continuously monitor service provider performance to ensure services meet pre-established requirements
* Ensure that outsourcing contingency plans are in place and tested at least annually
* Ensure an independent review and audit of the outsourcer to ensure that risks remain within acceptable levels.

# 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 Department Heads.

**Policy History**

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

**References:**

COBIT APO01.03, APO06.09, APO07.12-13, APO09.05, APO10.05, APO11.09-10, MEA01.05

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.GV-2, ID.RA-4, ID.RM-1, ID.SC-3-4

PCI 12.8