Mergers and Acquisitions 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’s strategic plan includes the ability to grow market share and revenues by merging or acquiring other entities. When merging or integrating Information Resources it is important that ABC Company Staff understand and agree on the appropriate procedures to protect ABC Company’s assets.

# II. Purpose

The purpose of this policy is to establish responsibilities related to mergers and acquisitions (M&A) of outside entities and their Information Resources. This policy also defines minimum security requirements related to integrating outside systems with ABC Company’s Information Systems.

# III. Scope

This policy applies to all ABC Company Staff (current as well as merged/acquired) that have access to ABC Company’s Information Resources.

# IV. Policy

A. M&A Assessment Team

Merger and Acquisition (M&A) assessments are performed to ensure that the new entity’s Information Resources do not pose a risk to ABC Company.

ABC Company will assemble an assessment team consisting of members of the following departments:

* Chief Security Officer
* Legal Department
* IT security

The purpose of the M&A assessment team is to identify and analyze risks related to Information Resources, develop a risk treatment plan, and implement risk reduction and corrective action prior to integrating the new entity’s systems with ABC Company’s Information Resources.

B. Security Requirements

The following minimum requirements must be achieved before the new entity’s systems can be integrated with or connected to ABC Company’s Information Resources:

* Data Center – must comply with ABC Company’s Physical Security Policy
* Facilities – must comply with ABC Company’s Physical Access Policy
* Firewalls – must comply with ABC Company’s Firewall Policy.
* Laptops and other mobile devices – must comply with ABC Company’s Portable Computing Policy
* Routers – must comply with ABC Company’s Router Security Policy
* Security Protection – must comply with ABC Company’s Anti-malware Policy
* Servers – must comply with ABC Company’s Server Hardening Policy.
* Wireless – must company with ABC Company’s Wireless Access Policy.
* Workstations – must comply with ABC Company’s Workstation Security Policy.

Staff from the new entity must receive appropriate training commensurate with their job duties. At a minimum, users must comply with ABC Company’s administrative related policies including, but not limited to:

* Acceptable Use Policy
* E-mail Policy
* Password Policy
* Remote Access Policy
* Removable Media Policy
* Reporting Violations Policy

C. M&A Assessment Report

Once the risk reduction and risk treatment strategies have been implemented, the assessment team will deliver an M&A Assessment Report to ABC Company Legal Department. The M&A Assessment Report will document:

* Initial status of new entity’s systems
* Actions taken to reduce or transfer risks
* Residual risks that remain after risk reduction strategies
* Written recommendation related to the risks

The Legal Department will review the M&A Assessment Report and make a recommendation to ABC Company Executive Management to either proceed with the integration, accepting any residual risk, or delay the integration until such time as the new entity’s systems can meet the above requirements.

# 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 EDM01-05, APO02.08, APO08.05-06, APO09.05, APO10.05, APO12.02, APO12.07

GDPR Article 25, 29, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(2)

ISO 27001:2013 8.1-3, 9.3, A.5.1.2, A.6.1.1-2, A.7.3, A.9.2.6, A.12.1.2, A.14.2.2

NIST SP 800-37 3.1, 3.4, 3.5

NIST SP 800-53 CM-3, CM-5, CM-9, CP-2, PS-7, SA-3, SA-9-10, SI-2, PM-2, PM-10, PS-4-5

NIST Cybersecurity Framework ID.AM-3, ID.BE-4, ID.GV-3, ID.RA-1, ID.SC-1, PR.AC-1

PCI 12.2, A3.1.2, A3.2.3