Context and Alignment 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

Executive Management is responsible for the design of ABC Company’s corporate strategies. Operational managers and Information Technology (IT) must be properly aligned with corporate strategies and the needs of the organization.

# II. Purpose

IT alignment helps ensure that the organization properly manages its IT projects, service delivery, risks, and meets compliance requirements.

# III. Scope

This policy applies to ABC Company’s Executive Management and department heads.

# IV. Policy

ABC Company strategies and culture is enabled as a strategic asset when there is an understanding and consistent implementation of organization values, policies, and procedures.

Each department shall:

* Create goals that contribute to achieving organization objectives.
* Document how the goals are aligned with the organization.
* Prepare action plans including people, processes, procedures and products that outline steps to implement department goals.
* Assign staff to track and monitor implementation of the action plan. Prepare quarterly status reports for Executive Management.

Executive Management shall:

* Review and approve department action plans.
* Review quarterly action plan status reports and provide feedback as necessary.

The Information Security Management System (ISMS), action plans and status reports shall include internal and external issues that are relevant to ABC Company. The IT Director shall determine the effect of the issues on the organization’s ability to achieve the intended outcomes of the ISMS.

The IT Director shall determine interested parties and Data Owners that are relevant to the ISMS. In addition, the IT Director shall determine the requirements of the interested parties and Data Owners relevant to the ISMS. The requirements of the interested parties and Data Owners should include contractual obligations as well as legal and regulatory requirements.

The IT Director shall determine and document the scope of the ISMS by reviewing the boundaries and applicability of the ISMS. When determining the scope, the IT Department shall consider:

* Internal and external issues that affect the intended outcomes of the ISMS.
* The requirements of the interested parties and Data Owners.
* Interfaces and dependencies between activities performed by the organization and those performed by other organizations.

The IT Director shall ensure that an ISMS is implemented, maintained, continually improved, and is aligned with the needs of the organization.

# 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 Executive Management and the IT Director.

**Policy History**

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

**References:**

COBIT EDM01.01, EDM02.03, APO01.03, APO01.11, APO02.08, BAI01.03, DSS01.05

GDPR Article 24

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(8)

ISO 27001 4, 6, 10

NIST SP 800-37 3.1, 3.2, 3.5

NIST SP 800-53 AT-2, AT-3, CM-2, CM-3, CP-3, IR-2, PL-2, PM-13, SI-4

NIST Cybersecurity Framework ID.RA-1, ID.RA-6

PCI 12.8.4, A3.2.1