Compliance 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 values its relationships with our employees, customers, service providers, regulators, and the business community. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

# II. Purpose

A strong compliance program provides our organization with a competitive advantage, helps protect our image and reputation and reduces costs. By establishing and maintaining a compliance management framework, we comply with company specific and statutory regulations.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

Executive management is responsible for ABC Company compliance with all relevant laws and regulations, compliance processes, and related reporting requirements. Executive management must create an environment of individual and collective accountability that includes the importance of meeting compliance obligations. Executive management must provide sufficient resources such as training, budgeting and staffing, to ensure compliance with company specific and statutory regulations.

Complying with applicable laws, regulations, and standards is the responsibility of every Staff member. The Compliance Department shall identify and communicate minimum compliance requirements for each Staff member and their business activities. Staff must know, understand, and meet compliance requirements that govern daily business activities.

The Compliance Department shall:

* Create, review, and update policies and procedures.
* Monitor departments to ensure compliance with requirements.
* Keep abreast of regulatory and industry trends to identify new compliance requirements and related changes to ABC Company business processes.
* Track and communicate to executive management issues encountered, lessons learned, and changes required.
* Ensure the on-going evolution of compliance management to ensure relevance and strategic competitive advantage.
* Ensure accurate and timely reporting to executive management.

When executive management, legal, or other appropriate Staff perceives a compliance issue, the Compliance Department shall investigate and make recommendations regarding any actions or concerns.

ABC Company’s executive management, compliance, legal, and audit functions are actively involved in managing compliance related risks:

* Management - develops and implements mitigation activities, including monitoring and reporting, for managing compliance in business activities.
* Compliance – the Compliance and Legal Departments monitor related laws, regulations, and standards. The Legal Department translates the laws into compliance obligations and assists in identifying compliance requirements.
* Audit – the audit department provides management with independent, objective assurance on the overall effectiveness of the design and operation of internal controls and activities.

The Chief Security Officer shall ensure:

* The organization has established a plan for outside, independent, periodic technical and non-technical evaluation of IT systems.
* No less than annually, IT systems shall be reviewed by an outside, independent organization to ensure ABC Company maintains reasonable and appropriate security measures. Such review shall include a review of internal and external systems, people, and processes.
* Evaluation reports, analysis, recommendations, and subsequent changes are fully documented.

# 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 company management, the Compliance Department, the Legal Department, CSO, and the Audit Department.

**Policy History**

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

**References:**

COBIT EDM01.01, EDM03.02, APO01.03, APO01.11, MEA02.11, MEA03.01, MEA04.11

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(8)

ISO 27001 A.18

NIST SP 800-37 3.5

NIST SP 800-53 All XX-1 controls (e.g. AC-1)

NIST Cybersecurity Framework ID.GV-3, ID.SC-4, PR.PT-1, DE.DP-2

PCI 11.2, 12.4.1, 12.8.4