Data Integrity 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

Controls and safeguards are needed to protect the integrity of electronic data that is stored, accessed, or transmitted using Information Resources.

# II. Purpose

This policy ensures the integrity of ABC Company’s data. Data should be protected from unauthorized alteration or destruction.

# III. Scope

Data integrity is an enterprise-wide activity that applies to all ABC Company Departments. This policy applies to all ABC Company Staff that store, access, or transmit electronic data.

# IV. Policy

Each department shall protect electronically stored, accessed, or transmitted data. Each Department shall implement processes that:

* Protect data from unauthorized alteration or destruction.
* Monitor access to data to ensure that it has not been altered or destroyed due to unauthorized activity.
* Issue alerts if the data has been altered or destroyed in an unauthorized manner. Upon such alerts, implement corrective action procedures to ensure data is restored and implement controls to ensure data is protected and cannot be altered in an unauthorized manner in the future.

The processes and technologies instituted by a department must achieve a level of protection sufficient to ensure data integrity. Each Department shall provide additional protections as needed when stricter requirements apply.

When designing or implementing security controls, the departments should ensure that they are in compliance with this policy.

On an annual basis, each Department shall submit a list of administrative, physical, and technical data integrity controls to the Chief Security Officer (CSO). The CSO will review the controls to ensure they are appropriate, sufficient, and effective at ensuring data integrity.

# 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 ABC Company Department Heads and those responsible for Information System security.

**Policy History**

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

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 25, 30, 32

HIPAA 164.312(c)(2), 164.312(e)(2)(i)

ISO 27001 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.1.4, A.18.2.2

NIST SP 800-37 P-14

NIST SP 800-53 PM-25, SC-8, SI-1

NIST Cybersecurity Framework PR.AC-5, PR.DS-6, PR.DS-8, DE.DP-2, RS.RP-1

PCI 3.6.5, 4.1, 6.4.6, 10.5, 10.6.1, 11.5, 12.10.5