Production Input Output Controls 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

The production, input/output controls are the security procedures in place that support the operations of Information Systems.

# II. Purpose

Strong, disciplined, and a clearly defined approach to production, and input and output controls helps ensure the confidentiality, availability and integrity of ABC Company’s Information Systems.

# III. Scope

This policy applies to the IT Department and other individuals responsible for the security of ABC Company’s Information Resources.

# IV. Policy

ABC Company’s IT Director is responsible for the security, accuracy and the reliability of Information Systems. IT application controls shall be used to ensure information confidentiality, availability, and integrity.

IT application controls refer to production and transaction processing controls, also known as input, processing, and output controls. IT application controls shall be automated (i.e., performed automatically by the systems) to ensure the complete and accurate processing of data from input through output.

The controls will vary based on the business purpose of the specific application. These controls may also help ensure the privacy and security of data transmitted between applications. The IT Director will identify application controls to be used and can include:

* Authentication - controls that provide an authentication mechanism in the application system.
* Identification - controls that ensure all users are uniquely and irrefutably identified.
* Completeness checks - controls that ensure all records were processed from initiation to completion.
* Validity checks - controls that ensure only valid data is input or processed.
* Authorization - controls that ensure only approved business users have access to the application system.
* Input controls - controls that ensure data integrity fed from upstream sources into the application system.

# 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 ABC Company’s IT Department and the Chief Security Officer.

**Policy History**

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

**References:**

COBIT EDM04.09, APO01.03, APO01.11, APO12.02, APO12.07, DSS01.05, DSS03.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(d), 164.312(e)(2)(i), 164.312(e)(2)(ii)

ISO 27001:2013 8.1, 9.1, A.6.2.2, A.8.2, A.9, A.12.1.1

NIST SP 800-37 3.2, 3.4

NIST SP 800-53 AC-16, CM-6, IA-5, IA-6, PE-5, SC-41, SI-4, SI-10

NIST Cybersecurity Framework PR.AC-1-4, DE.DP-2, RS.MI-2

PCI 6.5, A3.2.5