System and Organization Controls (SOC 2) 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

Security controls and safeguards are part of ABC Company’s risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

# II. Purpose

Service and Organization Controls (SOC 2) audits evaluate service provider risks and help ensure ABC Company’s controls are sufficient and effective.

# III. Scope

This policy applies to all ABC Company Department Heads, Chief Security Officer, Risk Management Officer, and those responsible for information system security.

# IV. Policy

An independent audit assists the Chief Security Officer (CSO) and Risk Management Officer (RMO) in ensuring that controls and safeguards are appropriate, sufficient, and effective at treating risks. The auditor evaluates systems for best practices and compliance with an established set of requirements.

The CSO shall define the scope of the audit. SOC 2 audits focus on evaluating controls grouped into one or more of the following Trust Services Criteria:

* Security – a common criteria that applies to all audits and must be included except for a Privacy Audit. The Security criteria includes protection against unauthorized logical or physical access, use, or modification.
* Confidentiality – evaluates protection of Sensitive Information including unauthorized access, protection of data, agreements with clients, etc.
* Availability – systems are available when needed and according to agreed upon criteria and requirements such as those stated in contracts and Service Level Agreements (SLA).
* Processing Integrity – validates transactions and related processing are complete, error free, timely, and accurate. Data cannot be modified in an unauthorized or undetected manner.
* Privacy – a Privacy Audit evaluates how ABC Company collects and uses personal information. This audit evaluates data handling contractual obligations, ABC Company's Privacy Policy, and related laws and regulations.

Based upon the scope of the audit, the CSO will identify resources to perform the SOC 2 audit.

Access to audit tools shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

SOC 2 audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources.

The auditor’s report shall include their project scope, findings, and recommendations to enhance compliance. The CSO shall:

* Review the security auditor’s report to confirm the findings and verify the recommendations are sufficient and effective.
* Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The CSO shall document important findings in the Audit Log Form and the RMO shall provide necessary reporting to ABC Company Executive Management.

# 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, Chief Security Officer, Risk Management Officer, and those responsible for information system security.

**Policy History**

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

**References:**

COBIT EDM03.02, APO01.03, APO01.11, APO12.02, APO12.07, MEA03.01, MEA04.11

GDPR Article 32

HIPAA 164.308(a)(8)

ISO 27001 9.2, A.15.2.1

NIST SP 800-37 3.5

NIST SP 800-53 3.3, AC-5, AU-6, CA-2

NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2

PCI 2.2.a-d