Standard Operating Procedure 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

Standard Operating Procedures provide a uniform and consistent approach to managing Information Resources, implementing best practices, and ensuring quality.

# II. Purpose

The purpose of this policy is to ensure standard operating procedures are implemented and maintained and provide ABC Company with enhanced service, better quality, and accountability.

# III. Scope

This policy applies to all ABC Company Staff.

# IV. Policy

A. Overview

Various regulations, governance frameworks, and security best practices require organizations to prepare, approve, and follow standard operating procedures (Procedures). Procedures ensure Staff carry out routine tasks and activities in a clear and consistent manner that reduces errors and ensures quality.

B. Department Head Responsibility

This policy specifies actions to be performed to ensure Procedures are implemented and maintained. Each ABC Company Department Head shall:

* Identify processes and procedures that require a Procedure.
* Ensure Procedures are implemented and maintained.
* Procedures use the format listed below.
* Ensure validation steps are performed to ensure the Procedures achieve the desired outcomes and results.
* Verify the Procedures are reviewed and modified on an as needed basis.
* Ensure training is provided as needed both at the time a new Procedure is rolled out, new Staff are involved, and/or revisions are made to the Procedure.

C. Procedure Format

Each Procedure shall use a consistent format as identified below.

* Title: Short title name that identifies the Procedure.
* Procedure information: Applicable policy library, approved date, approved by, effective date, and current version.
* Overview: Brief description of the Procedure.
* Purpose: Description of requirements and why the Procedure is needed.
* Scope: Description of applicable departments, systems, or Staff involved.
* Procedure: Detailed step-by-step instructions to perform actions. Staff that perform the actions, systems involved, and frequency of activities. Reports, documentation, or output generated. If needed, include diagrams, flowcharts, or other aids. Identify steps to be taken to ensure the Procedure is effective and achieves the desired outcomes and results.
* Enforcement: Actions taken to enforce the procedure.
* Distribution: Staff and other recipients that receive a copy of the Procedure.
* Procedure History: Brief history with description of revision changes and associated dates.
* References: List of compliance and security frameworks that support the Procedure.

D. IT Procedures

At a minimum, the IT Department shall implement and maintain Procedures that support the following policies/activities:

* Access Control Policy
* Anti-Malware Policy
* Backup Policy
* Change Management Policy
* Configuration Management Policy
* Firewall Policy
* Hardware and Software Maintenance Policy
* Logging Policy
* Patch Management Policy
* Problem Management Policy
* Server Hardening Policy
* Workstation Hardening Policy

# 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 all ABC Company Executive Management and Department Heads.

**Policy History**

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

**References:**

COBIT EDM01.11, EDM02.05, APO01.11, MEA02.11

GDPR Article 13, 28

HIPAA 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A-C), 164.308(a)(4)(ii)(B)

ISO 27001:2013 A.7.2.1, A.7.2.2, A.8.2.3, A.8.3, A.12.1.1, A.12.5.1, A.14.2.2, A.16.1.1

NIST SP 800-37 2.4, 2.7

NIST SP 800-53 AC-1, AU-1, CM-1, IR-1, MA-1, SI-1

NIST Cybersecurity Framework ID.AM-6, PR.AC-1, PR.AT-4, PR.DS-3, PR.IP-1, PR.IP-3-4

PCI 1.5, 2.1.1.b, 2.2.d, 2.5, 3.1, 3.4-6, 4.3, 5.4, 6.4, 6.7, 8.1, 8.4