Documentation 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

Documentation is important to ensure the continued operation of Information Resources in a reliable, secure, and sound manner.

# II. Purpose

This policy establishes the framework for Information Resources documentation.

# III. Scope

This policy applies to the IT Department and other departments responsible for acquiring, implementing, and maintaining Information Resources.

# IV. Policy

A. Responsibilities

The Chief Security Officer shall ensure:

* The organization makes documentation available to those responsible for implementing the procedures to which the documentation pertains.
* The organization reviews documentation periodically, and update as needed, in response to changes affecting the security of sensitive information.
* Operating procedures are documented and made available to all Staff that need them.

Documentation is a mandatory requirement for all of ABC Company’s Information Resources. Such documentation shall be kept up-to-date and be available to authorized personnel. The documentation shall be reviewed annually by a Documentation Analyst to verify it is appropriate, sufficient, and effective at continuing Information Resource availability, confidentiality, and integrity.

The Documentation Analyst shall collect and assemble documentation into an Information Resources Documentation Manual (Manual). The Documentation Analyst shall ensure that the Manual is updated on an annual basis or more frequently if changes occur.

B. Network Documentation

Network documentation shall include:

* Documentation on servers and major applications including data owners.
* Network diagrams with the locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
* The various security zones on the network and devices that control access between them.
* Connectivity between all segmented networks.
* All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information.

Configuration information on all network devices including switches, routers, hubs, and firewalls shall include:

* IP Address
* Netmask
* Default gateway
* DNS server IP addresses for primary and secondary DNS servers

Network connection information shall include the Internet provider, type of connection to the Internet, provider contact information, configuration information, and physical location including building and circuit number.

C. Documentation Access

Access to documentation shall be permitted as follows:

* The Documentation Analyst has full access to all Information Resources documentation.
* The IT network and security staff shall have full access to all network documentation.
* The IT network staff shall have the ability to read and modify network documentation.
* The Help Desk staff shall have read access to network documentation.
* Security staff shall have access to read and change security related documentation.

D. Documentation Review

The Documentation Analyst shall ensure that Information Resources documentation is kept current by performing an annual review of documentation. The Documentation Analyst will review Help Desk and Incident Response logs to determine whether changes were made to Information Resources. In addition, the Documentation Analyst will review projects related to Information Resources to determine whether the documentation needs to be updated.

E. Documentation Storage

Information Resource documentation shall be maintained in both written and electronic form and retained through the full life of the Information Resource.

# 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 IT Department personnel and other ABC Company staff members responsible for acquiring, implementing, and maintaining Information Resources.

**Policy History**

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

**References:**

COBIT APO01.02-03, APO05.05, APO11.09-10, APO12.02, APO12.07, APO13.07, BAI11.09

GDPR Article 30, 33, 49

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E)

ISO 27001 7.5, 8.1-3, 9.1-3, 10.1, A.8.1.3, A.9.1.1, A.12.1.1, A.14.2.5, A.15.1.1

NIST SP 800-37

NIST SP 800-53 All XX-1 controls, SA-5, SA-8, SA-12

NIST Cybersecurity Framework ID.RA-1, ID.RA-3, PR.PT-1, RS.MI-3

PCI 1.1.2-3, 1.1.5-6, 1.5, 2.5, 3.5-7, 4.3, 5.4, 6.4.5