Certification and Accreditation 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

The formal process of Certification and Accreditation (C&A) ensures that a clearly established set of security requirements is developed and implemented and any residual risk is minimized and formally documented.

# III. Scope

This policy applies to all Department Heads with authorized access to any of ABC Company’s Information Resources.

# IV. Policy

The Certification and Accreditation is a standardized process to ensure that an information system meets documented security requirements throughout its life cycle. Validating security controls provides the following benefits:

* Demonstrates compliance with relevant regulations
* Establishes and formally documents security requirements
* Provides independent verification of the correct implementation of the security requirements
* Provides a formal risk analysis that documents residual risk once all of the security requirements have been met
* Important documentation for the assessed system is contained in one set of documents

Certification is the technical evaluation of the security components and their compliance for the purpose of accreditation. A certifier, usually an independent third party, audits a system for compliance with an established set of security requirements. Accreditation is the formal acceptance of the adequacy of the system’s overall security by ABC Company management.

Through the use of Certification and Accreditation, the Chief Security Officer (CSO) ensures that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The CSO shall use the following guidelines when using Certification and Accreditation to evaluate ABC Company’s security controls.

Guidance – Define the list of standards or guidance documents to be used. The International Standards Organization (ISO), National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and other relevant frameworks help define a set of Security Requirements for the system.

Resources – Identify internal and/or external resources to perform the assessment.

Scope – Define the scope of the system being certified as well as its boundaries.

Security Requirements – Prepare a list of the security requirements that are relevant to the system. The security requirements are created based on the chosen guidance documents.

Description – Describe the system including mission description, system identification, criticality, etc. Document the environment including facilities, physical security, maintenance, etc. Identify the system architecture, interfaces, data flow, etc. Describe the system security requirements.

Test procedures – Every security requirement must have one or more test procedures. Test procedures can include visual verification, interviews, balancing, and other means to validate the security requirement.

Certification – Where possible, the CSO shall use Certified Information Systems Auditors to certify the security controls of ABC Company’s Information Systems. The auditor’s report shall include their project scope, findings, and recommendations.

Risk Analysis – Once the security findings have been sufficiently addressed and verified, a Risk Analysis shall be performed to describe the severity of the residual risk. Residual risk is the risk that remains after security controls have been implemented.

Accreditation – Prior to delivery of the accreditation package to the approving authority, Department Heads may, at the discretion of the CSO, make modifications to the security controls to minimize the risk of a denial of accreditation. When ready, the CSO shall assemble and deliver a complete package to the designed approving authority. The approving authority will either grant accreditation, grant an interim authority to operate, or denied accreditation.

# 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 APO05.03, APO05.05, APO11.09-10, BAI01.03, BAI01.09, BAI07.02, BAI07.06

GDPR Article 32

HIPAA 164.308(a)(8)

ISO 27001 9.2, A.12.7

NIST SP 800-37 3.5

NIST SP 800-53 AU-1, AU-3, AU-6, AU-9, AU-11

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

PCI A3.1.2.b, A3.2.2, A3.2.2.1, A3.2.3, A3.3.2