Application Implementation 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

When new applications are developed, an impact analysis must be performed to ensure that existing Information Systems remain stable.

# II. Purpose

This policy is designed to protect the organizational resources on the network by defining requirements for new applications. Assessments should be used to identify data classification and security levels, storage, and system requirements.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

ABC Company Staff shall work with application developers and Chief Security Officer (CSO) to assess data requirements for any new applications. Staff shall specify their requirements for the applications and application developers shall work with Staff to identify and categorize data according to Data Classification Policy.

Once the data and application requirements are established, the CSO shall evaluate risk and determine methods, processes, equipment, and procedures to mitigate known risks. The CSO, Staff, and application developers will work together to provide required and reasonable access capability to systems and data both during development and final project implementation while providing effective and sufficient controls at a reasonable cost. Under no circumstances should the overall security of the network be seriously compromised for the benefit of any project.

The data assessment, risk evaluation, and system requirements shall be performed early in the project life cycle since without this information, the overall cost of the project cannot be accurately assessed.

Where possible, IT Staff shall ensure that each server only provides one primary function. This helps prevent instances where separate functions require different security levels on the same device. IT Staff shall enable only necessary services, protocols, and daemons required by the application/system. IT Staff shall develop a baseline configuration for the application and system. Such configuration will be helpful in identifying unusual events and activities.

Prior to placing the application into production, and annually thereafter, a security audit shall be performed on the application. This helps ensure the security of the application, underlying host configuration, and data.

# 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 Staff that use ABC Company Information Resources.

**Policy History**

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

**References:**

COBIT APO05.03, APO05.05, APO12.02, APO12.07, BAI03.05-06, BAI03.09, BAI10.07

GDPR Article 25, 32

HIPAA 164.308(a)(7)(ii)(E)

ISO 27001 A.9.4, A.13.1, A.14

NIST SP 800-37 3.1

NIST SP 800-53 AC-6, CA-8, CM-2

NIST Cybersecurity Framework ID.AM, ID.BE-5, ID.GV-4, DE.DP-2

PCI 2.2, 6.1