Approved Application 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

To protect the security of ABC Company Information Resources, all Staff must ensure that only approved applications are used.

# II. Purpose

This policy is designed to protect Information Systems by requiring all Staff to only run application programs deemed safe by the IT department.

# III. Scope

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

# IV. Policy

The IT Department shall prepare and maintain a list of software applications that are approved for general use by ABC Company Staff. The list of programs that appears on the approved list of software applications shall include general office products such as word processing, spreadsheet, and presentations as well as programs specific to a department or function (e.g. anti-malware).

Staff may use and operate programs that appear on the approved list of software applications. If a Staff member wants to use an application that does not appear on the approved list, the Staff member must submit a request to the IT department to evaluate the application. This process applies to licensed applications, shareware, freeware, trial programs, and other software. The IT Department will evaluate requests and update the approved list of software applications on an as needed basis.

Only approved software applications are allowed to access ABC Company networks and Information Resources. Under no circumstances shall Staff use programs that are not on the approved list of Software applications. Staff members who introduce a security issue by installing and running an unapproved program risk disciplinary action.

Special exceptions may be made to this policy for specific employees depending on the required job function and the skills of the employee. Some reasons for exception include:

* A Staff member who tests new applications on a test network and then on the main network
* A programmer that must run applications in order to test the software
* Network administrators who install and test software as a part of their regular job duties

On a periodic basis, software inventory tools shall be used to identify and classify software installed on Information Systems. See the Asset Management Policy for more information.

Where possible:

* Approved software applications shall be whitelisted to ensure that only authorized software can be executed
* Unauthorized software shall be blocked from executing on Information Systems

# 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 APO01.02, APO01.06, BAI02.04, BAI06.01

GDPR Article 32

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

ISO 27001 A.9.4

NIST SP 800-37 2.2, 3.5

NIST SP 800-53 AC-2, AC-3, AC-20, CA-6, CM-2, CM-11, PM-5, SA-1

NIST Cybersecurity Framework ID.AM-2, ID.AM-3, ID.AM-4, PR.DS-3, PR.IP-3, DE.CM-1

PCI 6.4.5, 6.4.6, 12.3.4