System Update 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

This policy is an internal IT policy which defines how often and under what conditions computer system updates are performed.

# II. Purpose

This policy establishes a minimum process for protecting Staff from security vulnerabilities. This policy, when combined with the Patch Management Policy, determines how updates are to be performed for both servers and workstations.

# III. Scope

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

# IV. Policy

This policy defines methods used to determine what updates should be applied as well as the timing of the updates.

A. Update Monitoring

Several types of computer updates should be monitored:

* The computer BIOS.
* The operating system.
* Software application updates.
* Miscellaneous updates (e.g. Flash, Adobe Reader).

There are several methods that can be used to determine when updates should be performed:

* Review of posted security flaws and patches for each type of update applicable to the computer system.
* An automatic scanning of the system to determine available updates not yet applied to the system or application.
* The review of posted security flaws and patches should always be used for the computer operating system, BIOS, and applications. The manufacturer website should be used and there may also be other appropriate sites posting relevant bulletins. If automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.

Procedures shall be developed to:

* Determine how to identify appropriate patch or configuration changes for ABC Company’s servers and workstations. Updates for servers shall be checked no less than monthly to determine whether any new updates are required.
* Ensure that appropriate patch or configuration change works as desired without causing other disruptions. Where possible, a test environment should be used to determine whether updates may break production functionality.
* Prioritize updates and patches if several patches need to be applied.

B. Update Preparation

Before approving updates, System Administrators should understand:

* The addressed vulnerability.
* Previous patches or system update required.
* Programs affected by the change.
* Problems that may result as a result of the change.
* Procedures to back out or undo the change.

All patches approved for client computers shall be documented prior to release. When possible, new patches shall be tested in a controlled environment that mimics the infrastructure of the production environment before patches are applied.

IT Staff shall ensure that backups exist of applications and data prior to installing a patch or update. Each server shall have documentation that identifies the list of applications running on the device as well as a patch history.

C. Applying Updates

Depending upon the type of device, operating system, and criticality, workstation updates may be performed manually, using tools, or automatic updates. Automatic updates can save a great deal of time and expense since all workstations can be updated at the same time. All workstations shall have current versions of the operating systems.

Server updates shall be performed by a qualified and authorized System administrator after the update has been tested in a non-production environment. Assuming software compatibility, servers shall have current versions of the operating systems.

# 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 Staff responsible for maintain servers and workstations.

**Policy History**

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

**References:**

COBIT APO05.03, APO05.05, APO11.09-10, BAI06.02, BAI06.05-06, BAI07.06, BAI10.07

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.310(c)

ISO 27001:2013 A.11.2.4, A.11.2.6, A.12.1.2, A.12.6

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 RA-3, RA-5, SI-2, SI-5

NIST Cybersecurity Framework ID.RA-2, ID.RA-6, ID.RM-1, PR.IP-3, DE.DP-2

PCI 6.1, 6.2