Server Hardening 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

ABC Company must protect servers from both security and performance issues. Servers are depended upon security to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

# II. Purpose

The purpose of this policy is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

# III. Scope

This policy applies to all individuals responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource security.

# IV. Policy

A server must not be connected to the ABC Company network until it is in an ABC Company accredited secure state and the network connection is approved by ABC Company IT security Staff.

A Server Hardening Procedure shall provide the detailed information required to harden a server and must be implemented for ABC Company IT accreditation. At a minimum, the Server Hardening Procedure shall include:

* Installing the operating system from an IT approved source
* Applying vendor supplied patches
* Removing unnecessary software, system services, and drivers
* Setting security parameters, file protections and enabling audit logging
* Disabling or changing the password of default accounts

ABC Company IT security Staff will monitor security issues, both internal to ABC Company and externally, and will manage the release of security patches on behalf of ABC Company.

Where practical, ABC Company’s IT Department will test security patches against IT core resources before installing in production environments.

In the case of special applications, ABC Company’s IT Department may make hardware resources available for testing security patches.

Critical security patches must be implemented within the specified timeframe (typically 30 days) of notification from ABC Company’s IT Department.

To minimize risks, each server shall have only one primary function (e.g. E-mail, database, Human Resources).

# 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 IT Department Staff and the Chief Security Officer.

**Policy History**

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

**References:**

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(7)(ii)(E)

ISO 27001:2013 6.1.3, 8.3, A.13.1.1, A.14

NIST SP 800-37 3.3, 3.4

NIST SP 800-53 AC-3, AC-17-18, AC-20, PL-2, PL-7-8, SC-7-8, SC-10

NIST Cybersecurity Framework ID.AM-6, ID.RM-1, PR.AC-5, PR.DS-1-2, DE.CM-1

PCI 2.1-3, 2.5-6, 4.1, 5.1, PCI Software Security Framework