Server Hardening Procedure

|  |  |
| --- | --- |
| 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

Server policies provide management direction and guidance to ensure systems and data are properly protected. Procedures document a detailed description of the steps necessary to perform specific operations that comply with ABC Company’s server related policies.

# II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in ABC Company's Server Hardening Policy.

# III. Scope

This procedure applies to IT Department Staff who administer servers.

# IV. Procedure

Physical security. Ensure the server is placed in a physical location that restricts access to authorized individuals. Where possible, consider a locking cabinet/rack in a secure data center.

Alerts, advisories, and vulnerability announcements. Monitor manufacturer alerts, advisories, and vulnerability announcements. Ensure patches and updates are installed at the time a new server is placed into production and on-going per the Patch Management Policy.

Logging and monitoring. Ensure logging is activated per the Logging Policy. Consider centralized logging that consolidates logs for analysis and incident tracking. Log messages may be assigned a severity level whereby specific messages, based on their severity, are sent to remote logging servers. By default, these messages may be transmitted in clear text. Where possible, encryption should be used when transmitting messages.

Domain. If the server is part of Active Directory, most policies will be configured at the domain level. Stand-alone servers can be configured in the local policy editor.

Accounts. Where possible, disable the local Administrator account. For accountability purposes, ensure each Network Administrator uses a unique account/logon. Ensure local guest accounts are disabled.

Passwords. Ensure default credentials are changed. Ensure a long and complex memorized secret (i.e. password) is used to administer the device and complies with the Password Policy. When changing a password, ensure users cannot enter a recent prior password (password history). See the Password Policy for more information.

Account lock. Ensure accounts are locked out after five consecutive failed (invalid) logon attempts within a 24 hour period. The lockout duration shall be at least 30 minutes or until a system administrator re-enables the user ID. Refer to the Securing Information Systems Policy for more information.

Inactivity. Ensure users are automatically logged off after 15 minutes of inactivity. Refer to the Securing Information Systems Policy for more information.

Network configuration. Where possible, configure two Domain Name Servers (DNS) in the event one of the servers fails or is unable to provide services. Production servers should have static IP addresses. Remove unneeded packages/applications and disable unneeded services and drivers.

Firewall. As a general rule, each server should have a software firewall activated on the device. The software firewall helps protect against network based attacks.

Time. An accurate time and date is important for system and event logs. Configure a trusted time source for Network Time Protocol (NTP) and use proper authentication.

Anti-Malware. Ensure the device is protected from malicious software such as viruses, worms, Trojan Horse programs, etc. Ensure the Malware software and definitions are updated in a timely manner. Refer to the Anti-Malware Policy for more information.

Testing. Where possible, the server should be tested prior to installing the device in a production environment.

Management sessions. Administrators should not connect to the device using unsecure services where communications are not encrypted. Ensure only authorized personnel are allowed to access and administer the device.

Warning banners/notices. Some implementations may require the use of warming banners or notices. Network administrators should consult with ABC Company legal staff regarding the posting of notices such as:

* Access is only permitted by authorized personnel
* Activities are logged and monitored and can be used as evidence
* Unauthorized access or use can result in civil and criminal penalties

Backup. A copy of the device configuration should be saved at a separate and secure location to assist in a recovery effort if needed.

Manufacturer resources. Refer to manufacturer resources for additional guidance on hardening servers and specific security functionality.

# V. Enforcement

Any Staff member found to have violated this procedure may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This procedure is to be distributed to IT Department Staff who administer servers and the Chief Security Officer.

**Procedure History**

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