Firewall 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

Firewall 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 firewall 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 Firewall Policy.

# III. Scope

This procedure applies to all ABC Company Staff who administer firewalls.

# IV. Procedure

Physical security. Ensure the firewall 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 in a timely manner.

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. Unless required, firewall administrators should generally avoid logging messages at a debug level as this can produce a high load on the device.

Protocols and services. Document authorized inbound and outbound activity and only allow authorized ports/services to be open. All other inbound and outbound ports/services should be closed. Use secure protocols such as Secure Shell (SSH) and Secure File Transfer Protocol (SFTP).

Authentication. Ensure a long and complex memorized secret (i.e. password) is used to administer the device. Ensure default credentials are changed.

Lockout. If the device has a lockout feature, activate the lockout where the account is locked after a number of failed or invalid logon attempts.

Session timeout. Sessions should be terminated after a period of inactivity (e.g. 5 minutes).

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.

CPU notification. If available as a feature, activate the feature that allows an administrator to be notified if the CPU load exceeds a set threshold for a period of time.

Management sessions. Administrators should not connect to the device using unsecure services such as http or telnet as communications are not encrypted.

Accountability. Each firewall administrator should use their own unique administrator account when managing the firewall. This provides an audit trail with accountability.

Console ports. Console ports may provide special administrator privileges such as the recovery of passwords. The firewall administrator should ensure only secure local and remote access to the console port is permitted.

Warning banners/notices. Some implementations may require the use of warming banners or notices. Firewall 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 on a separate and secure location to assist in a recovery effort if needed.

Manufacturer resources. Refer to manufacturer resources for additional guidance on hardening firewalls 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 all ABC Company Staff who administer firewalls.

**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 164.312(d), 164.312(e)(2)(i)

ISO 27001 6.1.3, A.9.1.2

NIST 800-41 4, 5

NIST SP 800-53 AC-3, AC-4, AC-5, CA-3, CM-7, SA-9, SC-7, SC-28

NIST Cybersecurity Framework ID.RA-1, PR.AC-3, PR.AC-5, PR.DS-1-2, DE.DP-2, RS.RP-1

PCI 1.1-3, 2.1