Firewall 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

Firewalls are hardware devices or software programs that control the flow of traffic between networks, servers, and computer systems. This procedure specifies the steps and actions performed to meet the requirements of ABC Company’s Firewall Policy.

# 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 Staff responsible for staff that implement and manage ABC Company’s firewalls.

# IV. Procedure

The Chief Security Officer (CSO) ensures the following controls are in place:

* A formal process for approving and testing all network connections and changes to the firewall and configurations.
* A current network diagram identifies all connections between environments containing sensitive data and other networks, including any wireless networks.
* A diagram documents sensitive data flows across systems and networks.
* Firewalls are positioned at each Internet connection and between any demilitarized zone (DMZ) and the internal network.
* A description exists for groups, roles, and responsibilities for management of network components.
* Documentation and business justification exist for use of all services, protocols, and ports/services allowed, including documentation for security features implemented for those protocols considered to be insecure.
* Firewall configurations are reviewed at least every six months.
* A standard configuration exists for fast and consistent firewall deployment.
* Critical firewalls have been identified and are under maintenance/replacement contracts.
* Subscriptions/licenses satisfy business requirements.

IT security Staff define how firewalls handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization’s information security policies. IT security Staff:

* Restrict inbound and outbound traffic to that which is necessary for sensitive data and specifically deny all other traffic.
* Perimeter firewalls have been installed between wireless networks and sensitive data. These firewalls are configured to permit only authorized traffic between the wireless environment and environments containing sensitive data.

The IT Director has developed a list of the types of traffic needed by the organization and how they must be secured. The IT Director performs a risk analysis to determine the types of traffic that can traverse a firewall under what circumstances. Generally, all inbound and outbound traffic not expressly required are blocked.

IT security Staff review requirements when determining the types of firewall to be implemented. IT security Staff consider:

* Network related assets as well as the firewall technologies most effective at blocking network related threats.
* Performance considerations
* Concerns regarding the integration of the firewall into existing network and security infrastructures. Requirements related to ABC Company’s physical environment and personnel as well as possible future needs, virtual private networks (VPN), etc.

IT security Staff create network traffic rules that are as specific as possible. IT security Staff consider the types of traffic required and protocols the firewall may need to use for management purposes.

IT security Staff manage firewall architectures, policies, software, and other components throughout the life of the firewall solutions. Examples include:

* Choosing the type or types of firewalls to be deployed
* Firewall positions within the network
* Changes to firewall rules as ABC Company’s requirements change, when new applications or servers are implemented within the network, etc.

Firewall performance is monitored to ensure availability of ABC Company’s Information Resources. Monitoring tools are used to issues and take action before components become overwhelmed. Logs and alerts are continuously monitored to identify threats, both successful and unsuccessful.

Firewall rules and policies are managed by a formal change management control process. Such process considers the potential impact to security and business operations. Firewall rules are reviewed and tested on a periodic basis to ensure continued compliance with the organization’s policies. Firewall software is patched per the Patch Management Policy.

Firewall configurations prohibit direct public access between public networks (e.g. Internet) and any Information Resource containing sensitive information. A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology is used to limit network access to devices that store sensitive data. Configurations restrict all traffic, inbound and outbound, from untrusted networks (including wireless) and hosts and specifically deny all other traffic except for necessary protocols.

IT security Staff:

* Implement a demilitarized zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports/services.
* Configure systems to not disclose private IP addresses and routing information to unauthorized parties. Methods to obscure IP addressing may include, but are not limited to, Network Address Translation (NAT), placing servers containing sensitive data behind proxy servers/firewalls, removal or filtering of route advertisements for private networks that employ registered addressing, and internal use of RFC1918 address space instead of registered addresses.
* Limit inbound Internet traffic to IP addresses within the DMZ.
* Not allow any direct connections, inbound or outbound, for traffic between the Internet and the environments containing sensitive data.
* Include anti-spoofing measures to detect and block forged source IP addresses from entering the network.
* Not allow unauthorized outbound traffic from environments containing sensitive data to the Internet.
* Use stateful inspection, also known as dynamic packet filtering, so that only ”established” connections are allowed into the network.
* Ensure system components that store sensitive data (e.g. database) in an internal network zone are segregated from the DMZ and other untrusted networks.

Physical access to hardware firewall devices is restricted as much as possible. Desktops, laptops, and similar devices have software firewalls installed.

Firewall security log files are configured, maintained, and periodically reviewed for anomalies. Logs are of sufficient size to provide useful information in case of a security event.

IT security Staff receive periodic training regarding new and developing threats, current data security practices, and changes in compliance regulations.

IT security Staff ensure:

* Formal firewall hardening procedures are in place.
* Formal testing procedures are followed whenever configurations change.
* Firewall passwords are long and complex. Default passwords and configurations are changed on all firewalls.
* Firewalls are patched and updated in a timely manner. Documentation and procedures ensure that software updates and maintenance procedures are performed by authorized personnel.
* Firewalls are under support contract with appropriate response time guarantees.

# 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 security Staff.

**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