Firewall 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

Firewalls are hardware devices or software programs that control the flow of traffic between networks, servers, and computer systems.

# II. Purpose

This policy helps protect ABC Company’s Information Resources and related information asset availability, confidentiality, and integrity.

# III. Scope

This policy applies to all Staff responsible for security and protecting ABC Company’s Information Resources.

# IV. Policy

ABC Company uses a multi-layered approach to protect Information Resources and related "information assets". At one time, most firewalls were deployed at network perimeters. This provided some measure of protection for internal hosts, but did not recognize all instances and forms of attack when attacks were sent from one internal host to another and did not pass through network firewalls. Network security design shall include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to protect devices that are placed directly onto external networks.

The Chief Security Officer (CSO) shall ensure 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.
* Description of groups, roles, and responsibilities for management of network components.
* Documentation and business justification for use of all services, protocols, and ports/services allowed, including documentation for security features implemented for those protocols considered to be insecure.
* Examples of insecure services, protocols, or ports that include, but are not limited to, FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.
* Procedures review firewall configurations 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 shall define how an organization’s firewalls should 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 shall:

* Restrict inbound and outbound traffic to that which is necessary for sensitive data and specifically deny all other traffic.
* Install perimeter firewalls between any all wireless networks and sensitive data and configure these firewalls to deny or, control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment and environments containing sensitive data.

The IT Director shall conduct a risk analysis to develop a list of the types of traffic needed by the organization and how they must be secured. The risk analysis shall include which types of traffic can traverse a firewall under what circumstances. Generally, all inbound and outbound traffic not expressly required should be blocked. This practice reduces the risk of attack and can also decrease the volume of traffic carried on the organization’s networks.

IT security Staff shall identify the requirements that should be considered when determining the types of firewall to be implemented. IT security Staff should consider network related assets as well as the firewall technologies most effective at blocking network related threats. IT security Staff shall consider performance considerations as well as concerns regarding the integration of the firewall into existing network and security infrastructures. The firewall solution design should involve requirements related to ABC Company’s physical environment and personnel as well as consideration of possible future needs, virtual private networks (VPN), etc.

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

IT security Staff is responsible for managing the firewall architectures, policies, software, and other components throughout the life of the firewall solutions. There are many aspects to firewall management. For example, choosing the type or types of firewalls to deploy and their positions within the network can significantly affect the security policies that the firewalls can enforce. Policy rules may need to be updated as ABC Company’s requirements change, when new applications or servers are implemented within the network, etc.

Firewall performance should be monitored to ensure availability of ABC Company’s Information Resources. If possible, monitoring tools shall be used to monitor issues and take action before components become overwhelmed. Logs and alerts should also be continuously monitored to identify threats, both successful and unsuccessful.

Firewall rules and policies should be managed by a formal change management control process because of their potential to impact security and business operations, with rules, reviews, or tests performed periodically to ensure continued compliance with the organization’s policies. Firewall software should be patched as vendors provide updates to address vulnerabilities.

Configurations shall 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 must be used to limit network access to devices that store sensitive data. Configurations shall 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 shall:

* Implement a demilitarized zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports/services.
* 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.
* Implement 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, segregated from the DMZ and other untrusted networks.
* 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.

Physical access to hardware firewall devices must be restricted as much as possible. Desktops, laptops, and similar devices should have software firewalls installed. These software firewalls provide an additional layer of protection and must not be disabled without prior authorization from IT security Staff.

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

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

IT security Staff shall 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 under support contract with appropriate response time guarantees.

# V. Enforcement

Any Staff member 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 ABC Company security Staff.

**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 164.312(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