Example Firewall Policy Template

Summary

[Company Name] is committed to providing a secure and reliable network infrastructure for our employees, customers, and partners. One of the key components of our network security is our firewall, which is designed to protect our network and systems from unauthorized access and attacks.

Our firewall policy is designed to ensure that our firewall is used and managed in a way that provides the necessary level of protection for our network and systems. This policy outlines the scope of our firewall, including its purpose, configuration, management, and testing. It also provides guidelines for access control, firewall exceptions, enforcement, documentation, and violations and penalties.

Purpose

This firewall policy aims to define the rules, procedures, and guidelines for using firewalls in *[Company Name]*. Following our organization's overall security requirements, the firewall will be configured to perform the following security services:

- Block unwanted traffic using a firewall.
- Control access between the trusted internal network and untrusted external networks.
- Log traffic going to and from the internal network.
- Provide robust authentication.
- Provide virtual private network (VPN) connectivity for secure remote access.
- Hide vulnerable internal systems from the internet.
- Keep sensitive information (such as system names, network topologies, and internal user IDs) hidden from the internet.

Scope

This firewall policy applies to all employees, contractors, vendors, and other third-party entities accessing our organization's network and systems. It also applies to all devices that connect to our network, including computers, servers, mobile devices, and other network-enabled devices.

The policy covers all firewalls and related components, including hardware, software, and configuration settings, regardless of their location or ownership. This includes firewalls deployed at our organization's data centers, offices, remote sites, and cloud environments.

Exceptions

Exceptions to firewall rules and policies may be requested by authorized personnel when the business requires access to specific services or ports that are not allowed by default. Firewall exceptions must be approved by the appropriate authority and documented in accordance with *[Company Name]* security requirements and industry best practices.

The following guidelines must be followed when requesting and approving firewall exceptions:

- **Approval:** All firewall exceptions must be approved by *[name of the department/personnel in charge]*. The approval process should include an assessment of the risks associated with the exception and the justification for the business need.
- **Documentation:** All firewall exceptions must be documented and stored securely. This documentation must include information on the specific services and ports that are allowed through the firewall, the reason for the exception, and the approval authority.
- **Review:** Firewall exceptions must be reviewed regularly to ensure they are still required and not introducing unnecessary risks to the network and systems.
- **Removal:** Firewall exceptions must be removed when they are no longer required or when the business need no longer exists.

Firewall Configuration

All firewalls used by our organization must be configured in accordance with our security requirements and industry best practices. The firewall configuration must be documented and reviewed regularly to ensure it is up to date and effective.

The following guidelines must be followed when configuring firewalls:

- **Default Deny:** The firewall must be configured to block all incoming traffic except for the specific services and ports required for business operations.
- **Least Privilege:** Access to firewall configurations and settings should be restricted to only authorized personnel with a legitimate need. Access controls should be implemented using industry best practices such as role-based access control (RBAC) or multifactor authentication (MFA).
- **Documentation:** All firewall configurations, changes, and exceptions must be documented and stored securely. This documentation must include information on the specific services and ports allowed through the firewall, as well as any exceptions that have been granted.
- **Disaster Recovery:** Procedures must be in place to recover firewall configurations and settings during a disaster or other emergency.

Firewall Testing

Regular testing of *[Company Name]*'s firewall is essential to our overall security program. Firewall testing helps ensure that our firewall is functioning as intended and provides the necessary level of protection for our network and systems.

The following guidelines must be followed when conducting firewall testing:

- **Frequency:** Firewall testing must be conducted on a regular basis. The frequency of testing should be determined based on the level of risk associated with our network and systems and in accordance with industry best practices.
- **Methodology:** Firewall testing should be conducted using industry-standard methodologies such as vulnerability scanning, penetration testing, or firewall rule review.
- **Testing Scenarios:** Firewall testing should include various scenarios, such as testing for known vulnerabilities, testing for zero-day vulnerabilities, testing for misconfigurations, and testing for traffic filtering.
- **Updates and Patches:** Firewalls must be updated with the latest security patches and updates to ensure that they are protected against the latest security threats.
- **Reporting:** The results of firewall testing must be documented and reported to *[name of the department/personnel]*.
- **Remediation:** Any vulnerabilities or misconfigurations discovered during firewall testing must be remediated promptly. Remediation must be tracked and documented to ensure that all issues are addressed and resolved.

Firewall Documentation

Proper documentation ensures that our firewall is configured correctly and is providing the necessary level of protection for our network and systems.

The following guidelines must be followed when documenting our firewall:

- **Configuration Documentation:** Our firewall must be documented in detail, including its configuration settings, network topology, and firewall rules. This documentation must be updated and readily available to authorized personnel.
- **Change Management Documentation:** Any changes made to our firewall must be documented in detail, including the reason for the change, the person who made the change, and the date and time of the change. This documentation must be updated and readily available to authorized personnel.
- **Network Diagrams:** Network diagrams should be created to illustrate the overall network topology and the position of the firewall within the network.
- **Standard Operating Procedures (SOPs):** Standard Operating Procedures must be developed for the management of the firewall. These SOPs should include details on configuration changes, testing, monitoring, and incident response.
- **Retention Period:** All firewall documentation must be retained for a specified period in accordance with industry best practices and any legal or regulatory requirements.

Violations and Penalties

Violations of our firewall policy may result in disciplinary action, including termination of employment or contract.

Examples of violations of our firewall policy include:

- Attempting to bypass the firewall.
- Making unauthorized changes to the firewall configuration.
- Disabling the firewall or any of its components.
- Sharing firewall credentials with unauthorized personnel.
- Failing to report violations of our firewall policy.

Acknowledgment of Firewall Policy

This form is used to acknowledge receipt of and compliance with the organization's Firewall Policy.

PROCEDURE

Complete the following steps:

1. Read the Firewall Policy.
2. Sign and date in the spaces provided.
3. Return this page only to *[department in charge—often, but not always, the HR manager].*

SIGNATURE

Your signature attests that you agree to the following terms:

- **I. I have received and read a copy of the Firewall Policy and understand and agree to the same.**
- **II. I understand the organization may monitor the implementation of and adherence to this policy to review the results.**
- **III. I understand that violations of the Firewall Policy could result in the termination of my employment and legal action against me.**

Name Title

Department/Location Email

Supervisor Supervisor Email

Employee Signature Date

DISCLAIMER: THIS POLICY IS NOT A SUBSTITUTE FOR LEGAL ADVICE. IF YOU HAVE LEGAL QUESTIONS RELATED TO THIS POLICY, PLEASE SPEAK WITH YOUR LEGAL DEPARTMENT OR ATTORNEY.