Firewall Management Policy

Document Version: 1.0

Effective Date: [Date]

Approved By: [Approver Name/Title]

1. Purpose

This policy establishes the requirements and procedures for the configuration, management, and monitoring of firewalls within the organization to protect information systems from unauthorized access and threats.

2. Scope

This policy applies to all firewalls owned, managed, or operated by [Organization Name], including physical and virtual appliances, and covers all employees, contractors, and third-party users.

3. Policy

3.1 Firewall Configuration

- All firewalls must be configured to deny all traffic by default and explicitly permit only required traffic.
- Configuration changes must follow the approved change management process.
- Unused network services and ports must be disabled or blocked.

3.2 Rule Management

- Rules must be documented and reviewed at least quarterly.
- Rules allowing public access must be justified and approved by IT Security.
- Temporary rules must have an expiration date.

3.3 Firewall Administration

- Firewall management interfaces must not be accessible from untrusted networks.
- Access to administer firewalls must be restricted to authorized personnel only.
- Administrative activities must be logged and monitored.

3.4 Monitoring and Logging

- All firewall activity must be logged.
- Logs must be reviewed on a regular basis for suspicious activity.
- Logs must be retained for at least [Retention Period].

3.5 Incident Response

- Detected or suspected firewall breaches must be reported in accordance with the Incident Response Policy.
- Forensic analysis must be conducted as needed.

4. Roles and Responsibilities

Role	Responsibility
IT Security	Firewall policy enforcement, configuration review, and monitoring.
Network Administrators	Implementation and maintenance of firewalls.
All Users	Compliance with approved network access restrictions.

5. Policy Review

This policy will be reviewed annually or upon significant changes to network infrastructure or relevant regulations.

6. Enforcement

Violation of this policy may result in disciplinary action, up to and including termination or legal action.

7. Exceptions

Exceptions to this policy must be approved by IT Security management in writing and recorded for audit purposes.