ELIAS MOTSOALEDI LOCAL MUNICIPALITY

FIREWALL POLICY

MUNICIPAL COUNCIL RESOLUTION NUMBER

M24/25-07

APROVED AT THE COUNCIL SITTING OF 30 AUGUST 2024

M.D

TABLE OF CONTENT

M.D MR

1. Introduction

Firewalls are essential to the information systems security infrastructure of any organization. They control and restrict both Internet connectivity and services, establishing a perimeter where access controls are enforced

2. Terms and Definitions

Term	Meaning
FTP (File Transfer Protocol)	A standard Internet protocol for transferring files over a network
HTTP (Hypertext Transfer Protocol)	A set of rules for transferring files on the World Wide Web.
Security Device	Hardware or software providing security services.
Inbound Traffic	Traffic entering the Local Area Network.
Outbound Traffic	Traffic leaving the Local Area Network.
Exploitation	The process of obtaining and using intelligence information.
Perimeter Firewall	A firewall is installed between a private network and public networks, such as the Internet.
Network Security	Activities designed to protect network usability, reliability, integrity, and safety.
Network Security Architecture	A subset of network architecture addressing network security.
Security Functionality	Security-related features or functions within an information system or supporting infrastructure.
IT Security Requirements	Functional and non-functional requirements for achieving security attributes of an IT system.
Remote Access Points (RAPs)	Provide secure, always-on network access to corporate resources from remote locations.
Data	Information translated into a form convenient for moving or processing.
VPN (Virtual Private Network)	Uses public telecommunication infrastructure to provide secure access to an organization's network.
Proxy Server	A gateway between a local network and a larger network, providing increased performance and security.
Database	A collection of organized information for easy access, management, and updating.
TCP/IP	A set of protocols for getting data from one network device to another.
Authentication	Systematic method of confirming the identity of an individual or system.
Service	A long-running executable performing specific functions without user intervention.
Traffic	Data in a network, encapsulated in packets.

MR

M.A

Term	Meaning
Threat	A possible danger that might exploit a vulnerability to breach security and cause harm.
Vulnerability	A weakness allowing an attacker to reduce a system's information assurance.
Firewall	A software or hardware-based network security system controlling incoming and outgoing traffic.
Information Technology (IT):	Equipment or systems used for automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.

3. Purpose

To define standards for provisioning security devices at Elias Motsoaledi Local Municipality, preventing exploitation of insecure services, and controlling and monitoring traffic.

4. Scope

This policy applies to all devices connected to the Elias Motsoaledi Local Municipality network.

5. Policy Statement

Elias Motsoaledi Local Municipality's perimeter firewalls are key to the Network Security Architecture. This policy governs how perimeter firewalls filter Internet traffic to mitigate security threats.

6. Requirements

1. The firewall system shall control all traffic entering and leaving the internal network.
2. Firewalls shall block all incoming and outgoing blacklisted traffic by default.
3. Rules and Policies are in place to block blacklisted websites, which include pornography and sites threatening the safety of the municipality's network.
4. Allow only authorized traffic through the firewall.
5. Block traffic with invalid source or destination addresses.
6. Block traffic with private destination addresses for incoming traffic or source addresses for outgoing traffic.
7. Block outbound traffic with invalid source addresses.
8. Block incoming traffic with a destination address of the firewall unless required for services.
9. Block external traffic containing broadcast addresses directed inside the network.

M.D

7. Operations

1. Only Network Controllers and System Administrators shall log on to firewall hosts as administrators.
2. Access to firewall hosts shall be tightly controlled and reviewed monthly.
3. Only authorized personnel shall make changes to the firewall, documented in a Change Management System.
4. Logging and audit facilities shall be fully utilized and reviewed monthly.
5. An audit trail of firewall activity shall be maintained.

8. Configuration

1. The firewall shall be configured to deny any service unless expressly permitted.
2. The operating system of firewall hosts shall be configured for maximum security.
3. The firewall system shall reside on dedicated hardware.
4. The firewall configuration shall be documented and regularly reviewed.
5. Security shall not be compromised by the failure of any firewall component.
6. The firewall must be regularly tested for vulnerabilities.

9. Audit and Compliance

1. Regular quarterly testing of the firewall shall be carried out.
2. The firewall system shall have alerts in order to get emergencies/ updates/ breaches that require to be attended to urgently.
3. An active auditing/logging regime shall permit analysis of firewall activity during and after security events.

10. Responsibilities

The ICT Unit is responsible for firewall management and reporting any breach attempts to the ICT Manager and Chief Risk Officer.

11. Change Control

It is crucial to have a change control policy for any firewall. When new rules are introduced, there should be a well-defined method for documenting them. For temporary rules, the removal date should be included in a comment field. Verifying that the firewall enforces the agreed policy can be done using an Intrusion Detection System, a manual verification through a penetration test, or a third-party firewall review.

12. Monitor Stability

A firewall, like any other infrastructure component, must be managed to ensure its stability and availability. It should be monitored continuously to maintain maximum uptime. If a firewall is unstable, users may bypass it, leading to decreased security.

M.D

13. Enforcement

Employees who purposely violate this policy may be subject to Elias Motsoaledi Local Municipality disciplinary procedures including denial of access. Any employee aware of any violation of this policy is expected to report to their supervisor or other authorised representatives.

14. Consequences for Non-Compliance

Non-compliance may lead to disciplinary actions.

15. Signatories

______________________ 30/08/2024

Ms. NR Makgata Pr Tech Eng Date

Municipal Manager

Tladi 30/08/2024

The Mayor Date

Cllr. Tladi DM