67 Church Street, Mt Ayliff, 4735
Tel: +27 (0)39 254 6000
Fax: +27 (0) 39 255 0167
Web : www.umzimvubu.gov.za

UMZIMVUBU
LOCAL MUNICIPALITY

813 Main Street , Mount Frere
P/ Bag 9020, M t Frere , 5090
Tel: +27 (0)39 255 8500 /166
Fax: +27 (0) 39 255 0167

ICT FIREWALL POLICY

Table of Contents

INTRODUCTION 3
PURPOSE 3
SCOPE 3
FIREWALL RULES MANAGEMENT 3
REMOTE ACCESS CONTROL 4
FIREWALL LOGGING AND MONITORING 4
FIREWALL BACKUP AND REDUNDANCY 5
FIREWALL UPDATES AND PATCH MANAGEMENT 5
INCIDENT RESPONSE AND POLICY COMPLIANCE 5
POLICY REVIEW AND APPROVAL 5
DETAILED POLICY FRAMEWORK 5
POLICY REVIEW AND APPROVAL 7

UMZIMVUBU LOCAL MUNICIPALITY FIREWALL POLICY

1. INTRODUCTION

The Umzimvubu Local Municipality recognizes the importance of securing its network infrastructure to protect sensitive data and ensure business continuity. This Firewall Policy establishes the standards for configuring, maintaining, and monitoring the municipality's firewall systems to safeguard against unauthorized access, cyber threats, and system vulnerabilities.

2. PURPOSE

The purpose of this policy is to:

- Define clear guidelines for firewall management.
- Ensure compliance with industry best practices (COBIT 5, ISO 27001, and NIST).
- Mitigate risks associated with unauthorized access and cyber threats.
- Establish procedures for regular firewall maintenance, updates, and audits.

3. SCOPE

This policy applies to all network firewalls, administrators, IT personnel, and third-party service providers responsible for managing the municipality's firewall infrastructure.

4. FIREWALL RULES MANAGEMENT

4.1 Rule Descriptors

- All firewall rules must include clear descriptors outlining their purpose and business justification.
- Descriptors must specify permitted traffic, source, destination, protocol, and reason for rule existence.

4.2 Firewall Rule Review

- Firewall rules must be reviewed **quarterly** to ensure relevance and compliance.
- A review report must be submitted to ICT management after each assessment.

4.3 Change Management for Firewall Rules

- All firewall changes require documented approval from the ICT Manager.
- Change requests must include business justification, security impact analysis, and testing procedures.
- All changes must be tested in a controlled environment before deployment.

5. REMOTE ACCESS CONTROL

- Remote access to firewall administration must be strictly limited to authorized personnel.
- Secure access protocols such as **VPN with Multi-Factor Authentication (MFA)** or **SSH with key authentication** must be used.
- A log of remote access activities must be maintained and reviewed monthly.

6. FIREWALL LOGGING AND MONITORING

- All firewall traffic must be logged, and logs must be retained for **six (6) months**.
- Firewall logs must be monitored using a **Security Information and Event Management (SIEM)** system.
- Alerts for suspicious or unauthorized activities must be generated and escalated to ICT Security.

7. FIREWALL BACKUP AND REDUNDANCY

- Firewall configurations must be **backed up weekly** and stored securely.
- A redundant firewall must be maintained to ensure high availability in case of failure.
- Backup restoration tests must be conducted quarterly.

8. FIREWALL UPDATES AND PATCH MANAGEMENT

- Firewall firmware and security patches must be updated **monthly**.
- A patch management log must be maintained to track updates and installations.
- Vulnerability assessments must be conducted bi-annually to test firewall effectiveness.

9. INCIDENT RESPONSE AND POLICY COMPLIANCE

- Any firewall-related security incidents must be reported to ICT Security within **24 hours**.
- A firewall incident response plan must be developed and tested annually.
- Non-compliance with this policy may result in disciplinary action or revocation of access privileges.

10. POLICY REVIEW AND APPROVAL

- This policy will be reviewed **annually** or whenever significant changes occur in the network infrastructure.
- The ICT Manager is responsible for ensuring compliance and implementation of this policy.

11. DETAILED POLICY FRAMEWORK

11.1 Firewall Rule Implementation

- A firewall ruleset document must be maintained, detailing all active rules.

- Every new rule must undergo risk assessment before implementation.
- No "any-any" rules should be allowed unless explicitly approved by the ICT Manager.

11.2 Network Segmentation

- The firewall must enforce proper network segmentation to separate public, internal, and critical assets.
- DMZ (Demilitarized Zone) must be configured for externally accessible services.

11.3 Firewall Access Control

- Only designated personnel shall have administrative access to the firewall.
- Password policies must align with best practices (minimum length of 12 characters, complexity requirements, and MFA enforcement).

11.4 Incident Response Procedures

- A Security Incident Response Team (SIRT) must be designated to handle firewall-related security incidents.
- The ICT Department must conduct quarterly penetration tests to identify potential vulnerabilities.
- Security alerts must be reviewed within **6 hours** of detection, and appropriate action must be taken immediately.

11.5 Continuous Monitoring and Optimization

- Firewall performance must be monitored continuously to detect and mitigate threats.
- Automated tools should be used to analyze logs and identify patterns of malicious activity.
- Monthly firewall reports must be submitted to ICT leadership, highlighting any anomalies and corrective measures taken.

12. POLICY REVIEW AND APPROVAL

- This policy will be reviewed **annually** or whenever significant changes occur in the network infrastructure.
- The ICT Manager is responsible for ensuring compliance and implementation of this policy.

13. DOCUMENT OWNER AND APPROVAL

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation. This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion. Every page of this document must also be initialled by the Governance Champion.

_____ Signature: _____ Date:

_____ Position

- The ICT Manager is responsible for ensuring compliance and implementation of this policy.

DETAILED POLICY FRAMEWORK

1.3 Firewall Rule Implementation

- A firewall ruleset document must be maintained, detailing all active rules.
- Every new rule must undergo risk assessment before implementation.
- No "any-any" rules should be allowed unless explicitly approved by the ICT Manager.

1.4 Network Segmentation

- The firewall must enforce proper network segmentation to separate public, internal, and critical assets.
- DMZ (Demilitarized Zone) must be configured for externally accessible services.

1.5 Firewall Access Control

- Only designated personnel shall have administrative access to the firewall.
- Password policies must align with best practices (minimum length of 12 characters, complexity requirements, and MFA enforcement).

1.6 Incident Response Procedures

- A Security Incident Response Team (SIRT) must be designated to handle firewall-related security incidents.
- The ICT Department must conduct quarterly penetration tests to identify potential vulnerabilities.
- Security alerts must be reviewed within **6 hours** of detection, and appropriate action must be taken immediately.

1.7 Continuous Monitoring and Optimization

- Firewall performance must be monitored continuously to detect and mitigate threats.
- Automated tools should be used to analyze logs and identify patterns of malicious activity.
- Monthly firewall reports must be submitted to ICT leadership, highlighting any anomalies and corrective measures taken.

POLICY REVIEW AND APPROVAL

- This policy will be reviewed **annually** or whenever significant changes occur in the network infrastructure.
- The ICT Manager is responsible for ensuring compliance and implementation of this policy.

DOCUMENT OWNER AND APPROVAL

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation. This document was approved by the Executive Management and is issued on a version-controlled basis under the signature of the ICT Governance Champion. Every page of this document must also be initialled by the Governance Champion.

APPROVAL OF THE POLICY

The Municipality Council has improved this policy and amendments thereof

AUTHENTICATION

The amendment of this policy was approved by the municipal council on the 29/04/2025

As per council resolution number ULMC 073

Signed off

MR. GPT NOTA

MUNICIPAL MANAGER

CLLR. NG MDZINWA

SPEAKER OF THE COUNCIL