FIREWALL MANAGEMENT POLICY

Date of adoption: 23 May 2017

Council resolves to adopt the under-mentioned revised policy as the Information Technology Policy of the DR BEYERS NAUDE LOCAL Municipality

CONTENT **Page**

1. INTRODUCTION

This document details the procedures undertaken during the operation of the **BNLM** Firewall and details the requirements involved in securing the Municipal Network Facilities with a firewall.

2. SCOPE OF POLICY

This policy covers the management of the **BNLM** firewall. In addition, it will further define the security standards that the **BNLM** Firewall must comply with in its operational role.

This Policy will document the procedures and mechanisms for requesting and applying changes to the firewall rule sets protecting the municipality on its Internet Gateway.

3. POLICY

3.1 Firewall

A system designed to prevent unauthorised access to or from a private network through protecting and controlling both internal and external connections based on applied rules and configurations on the network it exists both as software to run on general purpose hardware and as hardware appliance.

3.2 Change Procedures

Firewall changes are deemed as business as usual (BAU) changes or standard agreed changes by the Systems Administrator and the following process must be followed:

- Complete a Change Request Form (See Appendix 1)
- Requested or required changes must be assessed and approved by a Director: Finance and Corporate Services. This assessment will evaluate such areas as the potential impact upon other Network Devices and Network Services.
- Change application must either be approved or rejected, providing justification for the change approval/rejection.
- Change must be implemented at a time that will have the least impact upon normal Firewall/Network Operations.

All of the change procedures must be fully documented and authorized and retained by the Systems Administrator.

3.3 Firewall Security

The security of all the network devices may be addressed on two levels: the physical and the logical. ***These two aspects ensure that all devices are secure and that no unauthorised access is permitted.***

3.3.1 Physical Security

The Firewall physical device is located in a secure area of the Municipal premises. This location is restricted through the use of a locked server/network room. These areas may only be accessed by the ICT employees.

3.3.2 Logical Security

Access to the Municipal Firewall is governed by password authentication. Only the Systems Administrator is permitted access to the Firewall. Any changes to the device must be performed by the Systems Administrator. No other employee is authorised or capable of accessing the Firewall.

3.4 Firewall Monitoring

Regular monitoring of the Firewall will occur to ensure that the device is functioning effectively. It will also ensure that the Municipal Network is being provided with the requisite protection as stipulated in the Firewall, It should be monitored for availability to ensure maximum uptime.

3.5 Suspicious Activity Monitoring

The Firewall will be continually monitored for any suspicious activity occurring. This monitoring will enable the Systems Administrator to identify any potential threats arriving through the Firewall and enable a swift response to potential dangers.

3.6 Log File Monitoring

Due to the nature and size of log files, it is accepted that regular monitoring is not always feasible. As such, monitoring of any Firewall logs will occur only under specific circumstances such as:

- An attempted intrusion
- Suspicious Inbound/Outbound activity
- On the request of the Senior Manager: Finance, Director: Finance and Corporate Services or Accounting Officer.

The circumstances in which firewall logs will be monitored are not limited to the above.

3.7 Security Monitoring

The System Administrator will perform regular monitoring of the Firewall to ensure that the integrity of said devices has not been compromised. Examples of this monitoring will take the form of:

- regularly monitoring access to the devices to ensure that only authorised users have gained access
- Monitoring the devices for any suspicious activity.

The monitoring is not limited to the above.

3.8 Analysis

Information gathered from the monitoring of the Firewall will be utilised to assess such areas of security. This will enable the Systems Administrator to efficiently assess the performance of the device and ensure that security is maintained.

3.9 Port Control

The Firewall will provide access to the municipal network only through a restricted number of ports. Any port that is not used to provide a connection will be disabled to prevent unauthorised access and ensure the Municipal Network Security is maintained.

4. FIREWALL ROLES RESPONSIBILITIES WITHIN THE PROCESS

<u>Systems Administrator Roles</u>:

- Implements the ICT Firewall Management Policy into specific firewall rules on the network devices to block malicious, spam from penetrating the network
- Ensure that Standard Network configurations are in place, unused ports are blocked to avoid illegal connectivity to the network
- Performs periodic verification of applied and configuration rules on firewall
- Recommends upgrades to the rules and changes to the policy
- Logs and analyses request for urgent or non-standard rules required by the municipality
- Performs daily spot checks of all Internet activity and monitoring for illegal web use as specified in the Policy

- Ensure that virus protection (**Eset Mail Security for Microsoft Exchange Server (EMSMES), Semantic Backup Exec, Semantics Agent, Eset Remote Administrator** for Servers, Computers and Notebooks are up-to-date, and cleaning of any virus infections that infect the municipal systems.
- Monitor the Virtual Private Network (VPN) and keeping it clean" of any unauthorised user access
- Manage the virus and SPAM protection through **Eset Mail Security for Microsoft Exchange Server**
- Maintain a Microsoft Active Directory environment, which consists of Microsoft Group Policies, Microsoft Firewalls and Microsoft File protection

Operational responsibility rests with the Systems Administrator and the IT Technician when the Systems Admin is unavailable

5. PROCESSES OF FIREWALL

Access to Firewall Hosts shall be tightly controlled; only the System Administrator is allowed to have user accounts on firewall hosts. The System Administrator must have personal accounts e.g. no group logins are allowed.

Change to all Firewall access must be made through a single approved interface. Firewall must have a trusted path for its management for example physical secure dedicated management process with a password based identification and authentication system.

Only personnel with the appropriate authorization must make changes to the firewall access rules, software, hardware or configuration. All changes must be as a result of an authorised “Request for firewall change” form. Only authorized personnel must be able to implement the changes and an audit log must be retained.

Logging and audit facilities provided by the firewall system shall be fully utilized. All significant traffic through the firewall shall be logged. System Administrators must examine logs on regular bases and also set up mechanism to respond to alarms.

BNLM employees may request changes to the firewall configuration in order to allow previously disallowed traffic. A firewall Changes request Form must be submitted to ICT Unit and approved by Senior Manager: Finance. All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case an explanation will be provided to the original request and alternative solutions will be explored.

BNLM employees may require access from the internet for services located on the internal network. Typically, this remote access is handled via secure encrypted virtual private network (VPN Connection). A request for VPN access must be fully motivated by the requestor including the reason for access, the period of access required and motivation justifying the Remote Access. A request must be approved by the Director: Finance and Corporate Services and submitted to the Systems Administrator for implementation.

6. CONFIGURATION OF FIREWALL

The perimeter Firewall System must be configured to deny any service unless is expressly permitted. Where there are, no rules defined for the BNLM network address, then traffic to or from that, address must be denied. Access to the BNLM must be blocked during start up procedure for the firewall.

Firewall Operating system must be configured for maximum security. The underlying operating system of firewall hosts must be configured for maximum security, including disabling of any unused services.

Firewall product suite must reside on dedicated hardware. Applications that could interfere and thus compromise the security and effectiveness of firewall products shall not be allowed to run on the host machine.

The initial build and configuration of the Firewall must be fully documented. This provides a baseline description of the firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.

Security must not be compromised by the failure of any firewall component. If any component of the firewall fails, the default response will be to immediately prevent any further access, both outbound as well as inbound. A firewall component is any piece of hardware or software that is an integral part of the firewall system. A Hardware failure occurs when equipment malfunctions or is switched off. A Software failure can occur for many reasons e.g. bad maintenance of the rules database on the firewall or software which is incorrectly installed or upgraded

There must be regular reviews to validate the Firewall system to meet the needs of the municipality regarding information security. The configuration of the firewall must be checked to ensure they still match the municipality requirement regarding the security. It may be necessary to implement separate Firewall modules to protect against the vulnerabilities of certain services.

6.1 The Firewall is configured to provide at least the following:

- Network Address Translation
- Proxy Services
- Port Blocking and Control
- Packet Sniffers
- Intrusion Detection and Virus attack Protection
- Www management Features
- Logging audit information
- Custom rule formulation and configurations

6.2. Network Configurations for Firewall

- The Firewall System shall control all traffic entering and leaving the **BNLM** internal Network
- **BNLM** blocks all incoming and outgoing traffics by default
- Only authorized incoming and outgoing traffic allowed to pass through **BNLM**
- Traffic with invalid source or destination address are blocked
- Traffic with invalid source address for incoming or destination address for outgoing traffic (Invalid "External" address) is blocked at network perimeter.
- Traffic with private destination address for incoming traffic or source address for outgoing (an "Internal " address) is blocked at the network perimeter
- Outgoing traffic with invalid source address is blocked
- Incoming traffic with a destination address of the firewall itself is blocked unless the firewall is offering services for incoming traffic that require direct connections
- Traffic from outside the network containing broadcast addresses that are directed to inside the network are blocked

6.3 Configurations for Network Firewalls

- Deny all traffic (In both Directions) which is not explicit permitted in both Directions (Inbound and Outbound)
- Permit inbound Mail Communication from any Server to Ports:
- SMTP (TCP 25) to Public SMTP Server
- HTTPS (TCP 443) to Public Webmail Server
- IMAP (TCP 143) and IMAPS (TCP 993) to Public Exchange Server
- POP3 (TCP 110) and POP3S (TCP 995) to Public Exchange Server
- Permit Outbound Mail Communication from any Ports of the Public SMTP server to port SMTP (TCP 25) of any Server on the Internet
- Permit Outbound DNS Communications form any ports of the public SMTP server and public DNS Server to port DNS (UDP and TCP 53) of any Servers on the Internet

- Permit inbound HTTP/HTTPS communication from any server to ports 80, 443 of the public GIS server.
- Permit inbound SSH communication from any server to port 22 of proxy server
- Permit internal traffic from LAN to proxy server 192.168.172.2
- Permit outbound traffic from 163.203.144.4 to internet
- Permit outbound traffic from 163.203.144.6 to internet
- Permit outbound traffic from 163.203.145.149 to internet
- Permit outbound traffic from 163.203.145.12 to internet
- Permit outbound traffic from Cisco Telephone System 163.203.146.0/27 to internet
- Permit outbound traffic from LAN to DNS port 53 on internet
- Permit outbound traffic from LAN to MAIL ports 110,143,585,993,995
- Permit outbound traffic from LAN to VNC ports 5900-5920
- Permit outbound traffic to port 25 from 163.203.144.8

6.4 Configuration for Network Core Firewalls:

- Deny all traffic which is not explicitly permitted in both directions (Inbound and Outbound)
- Permit inbound Mail Communication on Ports:

o SMTP (TCP 25) to internal SMTP Server
o IMAP (TCP 143) to Internal IMAP Server
o HTTPS (TCP 443 to internal webmail Server)

- Permit inbound DNS Communications on ports:

o DNS (UDP 53) to internal DNS Server

7. AUDIT AND COMPLIANCE

Regular testing of the Firewall must be carried out. The firewall must be regularly tested for:

- Configuration errors that may represent a weakness that can be exploited by those with hostile intent
- Consistency of the firewall rule set
- Secure Base System implementation

The firewall System must have an alarm capability and supporting procedures. When an agreed specified event occurs, an alarm must be sent to the Systems Administrator. In the event that the firewall itself is the subject of malicious attempts to penetrate it and the firewall has the capability, delivery of services should be terminated rather than permit uncontrolled access to the Municipality network.

8. ENFORCEMENT

ICT Unit is responsible for enforcing this policy and continuously ensuring monitoring and compliance wherever possible. Technological tools will be used to enforce this policy and mitigate security risks.

Any employee found to have violated this policy may be subject to disciplinary action.

9. WWW BROWSER ACCESS:

All browsers are configured to access internet via proxy server or via site proxy server which is configured to access internet. No other form of access to sites on the internet is permitted. This includes connections to alternative service providers by means of dial up modem. Users shall be held liable for breaches of security, loss of data or the compromise of information caused by unsafe browsing practices.

10. REVIEW

This policy shall be reviewed at least annually.

Appendix 1: Request for Firewall Change

Section 1: For completion by the requesting Department
Department Name:

Name and Surname	**Telephone Number**	**Email**

Requirements:
Requester Signature: **Supervisor Signature:**
Section 2: For completion by Systems Administrator

Change Reference Number:	**Date Received:**
External Host(s):	**IP Address(es):**
Internal Host(s):	**IP Address(es):**

Port Number(s):	**Application Protocol:**	**TCP**	**UDP**	**Other (please state):**

Action To Be Taken:
Section 3: Authorization by Director: Finance and Corporate Services
Comment:
Authorised:

Section 4: Action Taken by ICT
Comment:
Implemented by:
Reviewed by: