BELA-BELA LOCAL MUNICIPALITY

Chris Hani Drive, Bela- Bela, Limpopo. Private Bag x 1609
BELA-BELA 0480
Tel: 014 736 8000 Fax: 014 736 3288
Website: www .belabela.gov.za

OFFICE OF THE MUNICIPAL MANAGER

Information and Communication Technology

Firewall Policy

TABLE OF CONTENTS

POLICY AUTHORITIES

Compiled by	D Nkuna
Designation	Divisional Manager IT
Signature	
Date	
Supported/Not Supported	ML Mashishi
Designation	Acting Corporate Services Manager
Signature	
Date	
Approved/Not Approved	MM Maluleka
Designation	Municipal Manager
Signature	
Date	
Effective Date	

POLICY CHANGE RECORD

The following changes have been made to this policy:

Version	Description of Change	Date Approved

1. MANDATE OF THE ICT DIVISION

1.1 The Information and Communications Technology (ICT) Division has the mandate to deliver services, support and maintain ICT infrastructure for the Municipality to realise its mandate.

2. OBJECTIVE OF THE POLICY

2.1 ICT will implement a firewall between the Internet and private internal network in order to create a secure operating environment for the Municipality's computer and network resources.

2.2 A firewall is just one element of a layered approach to network security. The purpose of this Firewall Policy is to describe how the firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access.

3. APPLICABILITY OF THE POLICY

3.1 This policy refers specifically to the Sophos firewall already installed in the Municipality premises. The role of this firewall is to protect internal systems and restrict unwanted access into the Network. The firewall will (at minimum) perform the following security services:

3.1.1 Access control between the trusted internal network and untrusted external networks.

3.1.2 Block unwanted traffic as determined by the firewall rule.

3.1.3 Hide vulnerable internal systems from the Internet.

3.1.4 Hide information, such as system names, network topologies, and internal user IDs, from the Internet.

3.1.5 Log traffic to and from the internal network.

3.1.6 Provide robust authentication.

3.1.7 Provide virtual private network (VPN) connectivity.

3.2 This policy applies to all employees, including contractors and consultants.

4. TERMS AND DEFINITIONS

Term	Definition
Electronic Equipment	All Municipality-owned or issued and any personally-owned computer or related equipment that attaches to the ICT network, or is used to capture, process or store Departmental data, or is used in the conduct of official business of the Municipality.
Enterprise System	Enterprise systems are software systems that provide core services used across the institution and on which other applications often are dependent
Firewall	Any hardware and/or software designed to examine network traffic using policy statements to block unauthorised access while permitting authorised communications to or from a network or electronic equipment.
Firewall Administrator	The ICT function charged with the responsibility of Firewall Configuration and/or Rules administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rules.
Firewall Configuration	The system settings affecting the operation of a firewall appliance.
Host Firewall	Software running on a single host that can restrict incoming and outgoing network activity for that host only
Network Device	Any physical equipment attached to the network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points.

5. ACRONYMS

COBIT	Control Objectives for Information Technology
ICT	Information and Communication Technology
ITIL	Information Technology Infrastructure Library
SITA	State Information Technology Agency

6. REFERENCES

6.1 International Guidelines

a. Control Objectives for Information Technology (COBIT)

6.2 International Standards

b. Information Technology Infrastructure Library (ITIL)

c. ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

6.3 National Policy

d. Constitution of the Republic of South Africa, Act 108 of 1996

e. The Electronic Communications and Transactions (ECT) Act 25 of 2002

f. National Strategic Intelligence Act 2 of 2000 applicable for South Africa

g. Regulation of Interception of Communications Act 70 or 2002

h. State Information Technology Act 88 of 1998

7. POLICY STATEMENT

7.1 Where Electronic Equipment is used to capture, process or store data identified as confidential information and the Electronic Equipment is accessible via a direct or indirect Internet connection, a network Firewall appropriately installed, configured and maintained is required.

7.2 All installations and implementations of and modifications to a Firewall and its Configuration and Rules are the responsibility of the authorised Firewall Administrator, with this exception: maintenance of a Firewall Rule may be performed by an external service provider permitted by a documented agreement between the Municipality and the said service provider.

7.3 Access to the Firewall is governed by password authentication. Only the Firewall Administrator and the Network Administrator are permitted access to the Firewall. Any changes to the device must be performed by either of the Firewall Administrator or the Network Administrator roles. No other member of staff is authorised or capable of accessing the Firewall.

7.4 The Firewall physical device is housed in a secure area of the Municipality premises. This location is restricted through the use of secure key and may only be accessed by a restricted number of authorised technical team members.

7.5 The Firewall will provide access to the 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 network security is maintained.

7.6 Where Electronic Equipment is used to capture, process or store data identified as confidential information and the Electronic Equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is required where the operating environment supports that installation.

7.7 All Network Firewalls installed and implemented must conform to the current standards as determined by ICT. Unauthorised or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

7.8 All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The Rules should be opened incrementally to only allow permissible traffic.

7.9 Firewalls must be installed within production environments where confidential information is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.

7.10 Firewall Rules and Configurations require periodic review to ensure they afford the required levels of protection:

7.10.1 ICT must review all Network Firewall Rules and Configurations during the initial implementation process.

7.11 Firewall Rules and Configurations must be backed up frequently to alternate storage media in order to preserve the integrity of the data, should restoration be required. Access to rules and configurations and backup media must be restricted to those responsible for administration and review.

7.12 Network Firewall administration event logs (showing traffic activity) are to be reviewed from time to time. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.

8. OPERATIONAL PROCEDURES

8.1 Employees may request changes to the firewall's configuration in order to allow previously disallowed traffic. A change request form, with full justification, must be submitted to the ICT Division for approval.

8.2 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 high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

8.3 Employees may request access from the Internet for services located on the internal Municipality network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection.

8.5 From time to time, external service providers, contractors, or other entities may require secure, short-term, remote access to the Departmental internal network. Should such a need arise, an access request memo, with full justification, must be submitted to the ICT for approval. Approval is not guaranteed.

9. FIREWALL LOG CONFIGURATION AND MAINTANANCE

9.1 The firewall will be configured to use system logging. At a minimum, the firewall log will be configured to detect:

9.1.1 Alerts, critical conditions, error message and
VPN sessions,

9.1.2 Unsuccessful login attempts

9.1.3 Logon Access and configuration attempts made to the firewall

10. FIREWALL SECURITY SERVICES

10.1 At a minimum, the departmental firewall(s) will perform the following security services:

10.1.1 Access control between the internal network and untrusted networks.

10.1.2 Block unwanted traffic, as determined by firewall rule sets designed to implement the Municipality's Security Policy while providing security that does not place an undue burden on authorized users.

10.1.3 Hide system names, network topology, network device types, and internal user ID's from the Internet.

10.1.4 Log traffic to and from the Municipality's internal network.

11. POLICY COMPLIANCE

11.1 Wherever possible, technological tools will be used to enforce this policy and mitigate security risks. Violation of this policy, may lead to restriction of access to ICT facilities or disciplinary action.

11.2 Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual will be the responsibility of that user or that individual. The penalty, thereof, will be determined by the Municipality disciplinary process.

11.3 The Municipality may use any legislation relevant to the usage or protection of Information Systems (or information), in prosecuting the person who has violated this policy.

12 POLICY REVIEW

12.1 This policy shall be reviewed on an annual basis by the ICT Division to:

a. Determine if there have been changes in International, National or Internal references that may impact on this policy.

b. Determine if there are major changes to the network requirements