PIXLEY ka SEME DISTRICT MUNICIPALITY

Information and Communication Technology Firewall Policy

Objective of the Policy

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 to the network in the municipality. IT 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.

Terms and Definitions

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 IT personnel 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.

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, hub etc.

Applicability of the Policy

This policy will be applicable to all staff members of the municipality, external service providers, and consultants rendering services at and/or on behalf of the municipality. This policy refers specifically to the Cyberoam 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:

- Access control between the trusted internal network and untrustworthy external networks.
- Block unwanted traffic as determined by the firewall rule.
- Hide vulnerable internal systems from the Internet.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
- Log traffic to and from the internal network.
- Provide robust authentication.

Policy Statement

- 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.
- 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

MTK

performed by an external service provider permitted by a documented agreement between the Municipality and the said service provider.

- 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.
- The Firewall as a 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.
- 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.
- 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.
- 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.
- Firewall Rules and Configurations require periodic review to ensure they afford the required levels of protection: Network administrator must review all Network Firewall Rules and Configurations during the initial implementation process.
- Firewall Rules and Configurations must be backed up frequently to an 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.
- 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.

Operational Procedure

- 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 IT Support Officer for approval.
- 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.
- From time to time, external service providers, contractors, or other entities may require secure, short-term, remote access to the municipality's internal network. Should such a need arise, a full justification of the need to connect to the municipality's network must be given, the IT Support Officer will give such access after consultation with the immediate supervisor. Typically, this remote access should be handled via a secure, encrypted virtual private network (VPN) connection.

Firewall Log Configuration and Maintenance

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

MTK

- Alerts, critical conditions, error message and
- Unsuccessful login attempts
- Logon Access and configuration attempts made to the firewall.

Firewall Security Services

At a minimum, the municipality's firewall will perform the following security services:

- Access control between the internal network and untrustworthy networks.
- 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.
- Hide system names, network topology, network device types, and internal user ID's from the Internet.
- Log traffic to and from the Municipality's internal network.

Policy Compliance

- 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.
- 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.
- 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.

Policy Review

This policy shall be reviewed on an annual basis by the IT Support services to:

- Determine if there have been changes in International, National or Internal references that may impact on this policy.
- Determine if there are major changes to the network requirements

EXECUTIVE MAYOR : _____

DATE APPROVED : **30 AUGUST 2017**

RESOLUTION : **R 2017 – 08 – 30 (9.7)**