EPHRAIM MOGALE LOCAL MUNICIPALITY

SERVER SECURITY POLICY & PROCEDURE

DOCUMENT APPROVAL

Responsible Person:	Name	Signature	Date

Date approved: _____

1. PURPOSE

The purpose of the policy is to establish a standard code for the base configuration of internal server equipment owned by and operated by Ephraim Mogale Local Municipality. Effective implementation of this policy will to a large extent minimize unauthorized access to the Municipality's proprietary and technology.

2. SCOPE

The scope applies to server equipment owned by the Municipality and to servers registered under any Municipal owned internal network domain. This policy is specifically for equipment on the internal Municipal network

3. POLICY

3.1 Ownership and Responsibility:

All internal servers deployed shall be owned by the Municipality who shall grant permission to third parties access the server. Approved serve configuration guide must be established and maintained by the Municipality and the third parties based on the business needs approved. Third parties and the Municipality shall monitor configuration compliant to their environment. Each third party shall establish a process for changing the configuration guides which include review and approval to cover the following:

- Servers must be registered within the corporate enterprise management system, at least the following information must be captured to positively identify the point of contact:
  - i. Server contact(s), location and a backup contact.
  - ii. Hardware and operating system/version.
  - iii. Main functions and applications where applicable.
- Information in the corporate enterprise management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedure.

4. GENERAL CONFIGURATION GUIDELINES

i. operating system configuration should be in accordance with approved guidelines.
ii. Services and applications that will not be used must be disabled where practical.
iii. Access to services should be logged and / or protected through access control methods.
iv. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirement.

v. Trust relationship between systems are a security risk, and their use should be avoided.
vi. Always use standard security principles of least required access to perform a function.
vii. Do not use root when a non-privileged account will do.
viii. If a methodology for secure channel connection is available (i.e technically feasible), privileged access must be performed over secure channels, (e,g encrypted network connections).
ix. Servers should be physically located in an access controlled environment.
x. Servers are specifically prohibited from operating from uncontrolled areas.

5. MONITORING

i. all security related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum 2 weeks.
- Daily incremental tape backups will be retained for at least 2 months.
- Weekly full tape backup of logs will be retained for at least 2 months.
- Monthly full backups will be retained for a minimum of 2 years.

ii. Security related events shall be reported, logs shall be reviewed and reported incidents to the Divisional Manager Admin. & Legal Services. Corrective measures shall be prescribed as needed. Security events include, but not limited to:

- Port scan attacks.
- Evidence of unauthorized access to privileged account.
- Irregular occurrence that are not related to specifications on the host.

6. COMPLIANCE

i. Audit shall be performed on a regular basis by the internal auditors.
ii. Audit shall be managed by the internal audit in accordance with the Audit Policy.
iii. The IT Section shall filter findings not related to a specific third party and present such findings to the appropriate support staff for correction.
iv. Every effort shall be made to prevent audit from causing operational failures or disruptions.

ENFORCEMENT

Any employee forum to have violated this policy may be subjected to disciplinary action.