EMAKHAZENI LOCAL MUNICIPALITY

SERVERS SECURITY POLICY

Approval

DOCUMENT:	**Servers Security Policy**		
Copy Number:	**Master Copy**		
Compiled by:	Niall Carroll Deputy Manager ICT	**Reviewed by:**	
Compilation Date:	August 2013	**Review Date:**	
Version:	Draft V 1.03	**Revision:**	
Distribution:	All	**Classification:**	
Document Release Approval		**Document Acceptance**	
Releasing Authority: Manager: Cooperate Services	ICT Department	**Acceptance Authority:**	Council
Date Released:		**Date Accepted:**	
	Signature:		**Signature:**

0. DOCUMENT CONTROL

0.1 Revision Record

Revision	Date	Change Record	Changed By

0.2 Issue Control

This policy is issued by the DEPARTMENT OF CORPORATE SERVICES on behalf of the Emakhazeni Local Municipality, to whom any change requests or queries should be directed. The review life for this document is 12 months.

0.3 Distribution

Copy No.	Name	Title	Organisation
Master			
01			
02			

The MASTER for this document is held electronically and only signed copies are valid. An unsigned, printed document is not copy controlled and is to be used for information purposes ONLY, as it will not be automatically updated. It is therefore the responsibility of the reader to ensure that it is a currently valid copy.

CONTENTS

1. INTRODUCTION

All internal servers deployed at the Emakhazeni Local Municipality must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Emakhazeni Local Municipality. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Emakhazeni Local Municipality.

2. PURPOSE

The purpose of this policy is to establish standards for the base configuration of internal server equipments that is owned and/or operated by the Emakhazeni Local Municipality. Effective implementation of this policy will minimize unauthorized access to the Emakhazeni Local Municipality proprietary information and technology.

3. OBJECTIVES

The objectives of the SERVER SECURITY POLICY are;

1) To allocate ownership rights to groups using servers in the facilities of the COM ensure such rights are properly managed when accessing the resources of the municipality in the server room or any other site hosting the servers providing applications and data services of the COM
2) Administers the rights of access and the denial thereof these rights as and when violation or breaches are found
3) Provide connectivity to groups onto the municipal servers
4) Ensure that connectivity is done through the proper firewall procedures as defined in the firewall policy, and procedures of the COM but also through proper authentication procedures and methods such as those compliant to the password Protection standards and policy of the COM.
5) Remove or terminate these connectivity rights as and when the contract between the COM and the service providers terminates or ends.

4. DEFINITIONS

TERM	DEFINITION
DMZ	De-militarised Zone. A network segment external to the municipal production network. (ie. Telkom)
COM	Component Object Model (Technologies)
Server	For the purpose of this policy, a Server is defined as an internal Emakhazeni Local Municipality Server, Desktop machine and Lab equipment are not relevant to the scope of this policy.

5. STATUTORY AND REGULATORY FRAMEWORK

Provide the statutory and regulatory framework for the policy. To comply with all relevant legislative requirements including:

- The Constitution of the Republic of South Africa, 1996
- Municipal Structures Act, 1998
- Municipal Systems Act No 32 of 2000
- The Municipal Supply Chain Management Regulations
- Division of revenue act
- Municipal Finance Management Act No 56 of 2003

6. SERVER SECURITY POLICY

a) Servers must be registered within the municipal enterprise management system (Active Directory). At a minimum, the following information is required to positively identify the point of contact:
b) Server contact(s) and location, and a backup contact
c) Hardware and Operating System/Version
d) Main functions and applications, if applicable,
e) Information in the municipal enterprise management system must be kept up-to-date.
f) Configuration changes for production servers must follow the appropriate change management procedures.

6.1 General Configuration Guidelines

a) Operating System configuration should be in accordance with approved Emakhazeni Local Municipality guidelines.
b) Services and applications that will not be used must be disabled where practical.
c) Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

d) 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 municipal business requirements.

e) Trust relationships between systems are a security risk, and their use should be avoided.

f) At no stage must groups use a trust relationship when some other method of communication will be appropriate and can do.

g) Always use standard security principles of least required access to perform a function.

h) No groups shall use root when a non-privileged account will do.

i) 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 using SSH or IPSec).

j) Servers should be physically located in an access-controlled environment.

k) Servers are specifically prohibited from operating from uncontrolled cubicle areas.

6.2 Monitoring

a) All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
   i. All security related logs will be kept online for a minimum of 1 week.
   ii. Daily incremental tape backups will be retained for at least 1 month.
   iii. Weekly full tape backups of logs will be retained for at least 1 month.
   iv. Monthly full backups will be retained for a minimum of 2 to 5 years.

b) Security-related events will be reported to Emakhazeni Local Municipality, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
   i. Port-scan attacks,
   ii. Evidence of unauthorized access to privileged accounts,
   iii. Anomalous occurrences that are not related to specific applications on the host.

6.3 Compliance

a) Computer Audits will be performed on a regular basis by office of the AG and the Internal Audit section of the Emakhazeni Local Municipality.

b) Audits will be managed by the internal audit section or the office of the Auditor General, in accordance with the *Public Audit (PAA) Act, 25 of 2004 and subsection 4 of the PAA*. Emakhazeni Local Municipality will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

c) Every effort will be made to prevent audits from causing operational failures or disruptions.

7. AUDIENCE AND APPLICABILITY

The server security policy is applicable to the server room, to server equipment owned and/or operated by the Emakhazeni Local Municipality, or Disaster Management Center of the Dr Kenneth Kaunda District Local Municipality, external service providers and any servers outside the building belonging to the municipality used for purpose of providing ICT services and are on the network infrastructure of the Municipality.

To servers registered under the following service providers of the Services to the COM:

I. CONLOG.
II. MUNSOFT
III. OBSIDIAN
IV. TELKOM

a) Emakhazeni Local Municipality -owned internal network domain.
b) This policy is specifically for equipment on the internal Emakhazeni Local Municipality's network.
c) For secure configuration of equipment external to the Emakhazeni Local Municipality on the DMZ, refer to the ***Internet DMZ Equipment Policy***.

8. RESPONSIBILITIES AND ACCOUNTABILITIES

8.1 The Municipal Manager is accountable for establishment of the service workstations security policy of the Municipality.

8.2 The Municipal Manager may take the necessary steps in ensuring that that:

8.2.1 The Deputy Manager ICT provides server security services to all service providers contracted by the municipality,

8.2.2 The Deputy Manager ICT in the office of the DEPUTY MANAGER ICT allocates, suspends, monitors, provides access through the **firewall procedures** in term of the firewall policy to service providers contracted by the Municipality only on sensitive information on all servers, back-up all data on the servers of all municipal applications.

8.2.3 The Deputy Manager ICT allocates the responsibility for server security activities without abdicating accountability to the network support employee in the IT section

8.2.4 The network support employee must ensure that all servers is used for work related purpose and not for other reasons other than defined in this sever security policy.

8.2.5 That the network support employee monitors, reports and evaluates from time to tine any violation, potential breaches, and malpractices of the server security usage from any service providers or Users and report weekly or monthly to the Municipal Council of such usage.

9. RESPONSIBILITIES OF THE ACCOUNTING OFFICER

The Accounting Officer at the advice of the Deputy Manager ICT can make a determination on the following:

9.1.1 Review of the server security policy,

9.1.2 Change the server security policy if it is not in compliant with information security legislation,

9.1.3 Propose amendments and/or deletions on the guidelines,

10. RESPONSIBILITIES OF THE DEPUTY MANAGER ICT

10.1.1 The Deputy Manager ICT is responsible for the assessing and evaluating of the risk on the accessing of the abuse or miss-use of the server security responsibility allocated to all the IT Personnel of the Municipality.

10.1.2 Appropriate rights or revocation thereof of those rights to the service providers and any Users violating the server security policy,

10.1.3 Ensure that the server security policy is effective and user friendly.

11. CROSS REFERENCE TO OTHER POLICIES

11.1 The server security policy must be read together with the Information Security Policy for the Emakhazeni Local Municipality and,

11.2 Any other applicable guidelines, norms and standards as defined from time to time by the COM.

12. ESCALATION PROCEDURE

12.1 The NETWORK SUIPPORT employee shall escalate any deviations or violation of the email use to the Deputy Manager ICT.

12.2 The Deputy Manager ICT after evaluating the merits of the violation and the extent of the violation shall report the violation or breach to the Corporate Services Manager.

12.3 The Deputy Manager ICT shall issue a recommendation to the Corporate Services Manager to suspend the use of server access and institute a formal and proper investigation.

12.4 On the outcome of the investigation, the Corporate Services Manager shall inform the Deputy Manager ICT of such for a ruling or upon further investigation which a decision shall be taken on the necessary course of action.

12.5 The Deputy Manager ICT may allow deviations only on the basis of an operation that requires such an intervention.

12.6 The Municipal Manager may approve or decline such requests for a deviation.

13. ENFORCEMENT OF THE EMAIL POLICY

Any service provider or User of a server found to have violated this policy may be subjected to the termination of the contract between the Municipality and the service provider.

14. REPORTING & DISCLOSURE REQUIREMENTS

The Deputy Manager ICT shall report from time to time the management, administration and operational of the policy implementation to the Municipal Council.