EMAKHAZENI LOCAL MUNICIPALITY

BACK-UP MANAGEMENT POLICY

Approval

DOCUMENT:	**BACK UP MANAGEMENT POLICY**		
Copy Number:	**Master Copy**		
Compiled by:	Niall Carroll	**Reviewed by:**	
Compilation Date:	August 2013	**Review Date:**	
Version:	Draft V 1.03	**Revision:**	
Distribution:	All	**Classification:**	
Document Release Approval		**Document Acceptance**	
Releasing Authority: Corporate Services	ICT Division	**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 GOVERNANCE] 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

INTRODUCTION

The policy is responsible under the Protection of Privacy of Personal Information (POPI) Act and the Protection of State Information Bill as amended for ensuring that all personal and identifiable municipal data in any format (text, images, voice, video, sound, or any other communicable data) is recoverable in the event of accident loss or damage.

1. FREQUENCY AND TIMING OF BACKUPS

1.1. A full back up of operational data is taken every day including:

a) All clinical or customer records and system audit trail.
b) All files held on the Shared directory, hard drives, and Active Directory area of the network.
c) The backup is scheduled to run automatically at **16:00 pm** daily.

1.2. The following should also be backed up where these are held on computer. However, a separate backup routine may be required which should also be detailed in this policy.

a) Munsoft Accounting System.
b) Other Municipal relevant software/systems.

2. BACKUP

2.1. ICT and Finance (VIP) are responsible for:

a) Manual Backup VIP: inserting disc at close of day. Mr. Dirk De Wet (Finance- Senior Accountant Salaries)
b) Manual Backup Munsoft: Periodic backups preformed by Finance Department by Mr. Dirk De Wet (Finance- Senior Accountant Salaries)
c) Storing the backup VIP: External HDD and DR Server (Auto Backup).
d) Checking the backup has been successful.
e) Managing a backup failure.
f) Maintaining the backup log.

g) Auto Backup: Daily at 19:00Hrs from main server at Head Office to offsite DR Server at Entokozweni Municipal Office

2.2. The rota includes clear deputising arrangements for cover in the event of staff absence (both planned and unplanned).

3. VERIFICATION OF BACKUP STATUS

3.1. The designated member of staff must check the backup status on the system first thing each morning and report any failures to the practice manager and system supplier (**See Annexure 3: Verification log sheet)**.

4. BACKUP LOG

4.1. A daily backup log (**see attached Annexure 4: Daily backup log sheet**) is issued to keep a report of backups, their status, which tapes are used and housekeeping of the backup system. These logs are stored in a safe in the computer room and copies at the Main Civic Building, Room 023.

5. HOUSE-KEEPING OF THE BACKUP SYSTEM

5.1. Regular maintenance of the backup device is carried out to ensure it is kept in good working order.

5.2. Cleaning tapes are used in accordance with manufacturer's instructions. DLT tape drives should be cleaned monthly or more often if the cleaning light is illuminated.

6. MANAGING BACKUP FAILURE

6.1. In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:

6.2. Note any messages / information on the server monitor.

6.3. Contact system supplier to report the failure.

6.4. Report the failure to the Deputy Manager ICT.

6.5. Record the failure in the backup log and any actions taken as a result.

6.6. If the backup fails repeatedly, it may be necessary to perform a manual backup. This takes time, and must be performed when all users are logged out.

7. VALIDATION OF BACKUP

7.1. A backup is validated by system supplier every 3 months. As part of this process the supplier checks to ensure data can be fully restored from the DR Server (Munsoft).

8. MANAGEMENT OF DR SERVERS

8.1. Off Site server should be checked on a regular bases and any problems dealt with immediate effect. .

9. Municipal Software

9.1. Only the following member(s) of staff are authorised to load software onto any part of the network: (names) according to the software installation policy.

9.2. Any other member of staff found to be loading software without authorisation may be subject to disciplinary procedures.

9.3. Niall Carroll who is the DMICT will ensure that all staff is aware of this by both signing of the policy, induction, workshop, etc.

9.4. Original copies of copies of software and licensing agreements are stored in the fireproof media safe in the Data Center of the Municipality.

10. AUDIENCE AND APPLICABILITY

10.1. THE COM BACK UP MANAGEMENT POLICY APPLIES EQUALLY TO ALL INDIVIDUALS WITH AUTHORIZED ACCESS TO ANY COM INFORMATION RESOURCES.

11. STATUTORY AND REGULATORY FRAMEWORK

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

11.2. The Constitution of the Republic of South Africa, 1996

11.3. Municipal Structures Act, 1998

11.4. Municipal Systems Act No 32 of 2000

11.5. The Municipal Supply Chain Management Regulations

11.6. Division of revenue act

11.7. Municipal Finance Management Act No 56 of 2003

12. RESPONSIBILITIES AND ACCOUNTABILITIES

12.1. The Municipal Manager is accountable for establishment of the Back Up Management policy of the Municipality.

12.2. The Municipal Manager may take the necessary steps in ensuring that that: The Deputy Manager ICT provides Back Up Management services to all municipal employees,

12.3. The Deputy Manager Information Communication Technology creates, allocates, suspends, monitors, deleted, archived, un-suspends and administer the Back Up Management of employees.

12.4. The Information Communication Technology Manager allocates the responsibility without abdicating accountability to the Systems Maintenance employee in the ICT section.

12.5. That ICT employees monitors, reports and evaluates from time to time any violation, potential breaches, and malpractices of Back Up Management system from any Users and report monthly to Section 80 of such usage.

13. RESPONSIBILITIES OF THE ACCOUNTING OFFICER

13.1. Change the Back Up Management policy if it is not compliant with information security legislation,

13.2. Propose amendments and and/or deletions on the guidelines,

14. RESPONSIBILITIES OF THE DEPUTY MANAGER ICT

14.1. 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 Back Up Management system of the Municipality.

14.2. Appropriate rights or revocation thereof of those rights to the Municipal employees violating the Back Up Management policy,

14.3. Ensure that the Back Up Management policy is effective and user friendly.

15. CROSS REFERENCE TO OTHER POLICIES

15.1. The Back Up Management use policy must be read together with the Information Security Policy for the City of Emakhazeni and,

15.2. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

16. ESCALATION PROCEDURE

16.1. The system maintenance employee shall escalate any deviations or violation of the Back Up Management Policy to the Information System Manager.

16.2. The Information Systems Manager after evaluating the merits of the violation and the extent of the violation shall report the violation or breach to the DMICT.

16.3. The DMICT shall immediately issue a directive to the IS Manager to suspend the Use of Backups to institute a formal and proper investigation.

16.4. On the outcome of the investigation, the DMICT shall inform the Accounting Officer of such for a ruling or further investigation upon which a decision shall be taken on the necessary course of action.

16.5. The DMICT may allow deviation only on the basis of an operation that requires such an intervention.

16.6. The Municipal Manager may approve or decline such request for a deviation.

17. ENFORCEMENT OF THE ACCOUNT MANAGEMENT POLICY

17.1. Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or

expulsion in the case of a student. Additionally, individuals are subject to loss of [COM] Information Resources access privileges, civil, and criminal prosecution.

17.2. Any employee of the municipality found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and must cooperate with authorized [COM] management investigating security incidents procedures.

18. REPORTING & DISCLOSURE REQUIREMENTS

18.1. The Deputy Manager ICT shall report from time to time the management, and Section 80 of the policy implementation.