RICHTERSVELD LOCAL MUNICIPALITY BACK UP POLICY AND PROCEDURES

MUNISIPALITEIT
RICHTERSVELD
MUNICIPALITY

Approved Date: 29 August 2017	**Council Resolution Nr: RVN 020/08/2017**
Effective Date: 01 September 2017	**Review Date: 30 Junie 2018**

1. PURPOSE

The practice is responsible under the Data Protection Act for ensuring that all municipal data is identifiable and is recoverable in the event of accident loss or damage.

2. FREQUENCY AND TIMING OF BACKUPS

Backups are automated as follows:

PROMUN & DOMAIN CONTROLLER

Incremental backups of above mentioned server data are taken daily. The backup is scheduled to run automatically at 20:00 every night. Full backups are scheduled to run every Friday at 19:00.

IMIS SERVER

Backups are being done by the responsible service provider (TGIS).

KERIO MAIL SERVER

Incremental backups are scheduled to run daily at 20:00, and full backups are scheduled to run every Friday at 19:00.

.

FILE SERVER

Automated Full backups is done on every Friday 19:00 followed by incremental backups on Monday to Thursday at 20:00 too offsite NAS device.

The following data should be backed up. However, users must ensure that data are backed up on their respective U-Drives.

- Financial and Cooperate Data (LIBRARY)
- User work related data (U-Drives)
- All other data relevant to Richtersveld Local Municipality

3. VERIFICATION & DAILY BACKUP CHECKS

ICT personnel will on a daily basis check and verify the status of the backups performed the previous day. On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors
- To monitor the duration of the backup job
- To optimize backup performance where possible
- To check for any data that might have been skipped
- Remedial and corrective action

4. BACKUP LOGS

ICT personnel will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance for auditing purposes.

5. MAINTENANCE OF THE BACKUP SYSTEM

Regular maintenance and firmware updates of the NAS backup device will be carried out to ensure it is kept in good working order.

6. MANAGING BACKUP FAILURE

Any backup failures will be investigated and a manual backup will be scheduled to run. ICT personnel must immediately:

1. Note any messages / information on the server monitor
2. Report failure immediately to Line Manager
3. Record the failure in the backup log and any actions taken as a result
4. Schedule a manual backup to be performed when all users are logged out.

7. VALIDATION & RESTORE GUIDELINES

Test restores will be done every week on a Friday to verify the integrity of the backup jobs being performed. Random documents will be selected to restore to a different location and once verified the reports will be filed for auditing purposes. Requests to restore data by any user will be done through logging a call and completing the necessary forms, to be approved and authorized by the respective head of department.

8. MANAGEMENT OF OFFSITE BACKUPS

Richtersveld Municipality is currently making use of Symantec Backup Exec 2014 backup solutions to backup and restore municipal data. The solution is a fully automated off-site backup solution that does not involve human intervention. Hard drives on NAS Backup device will be replaced every 2 years.

9. POLICY REVIEWING

At present there is a Clause in all approved policies whereby it be reviewed annually by the Council. There is however only a certain number of policy statements (e.g. finance related) that must be reviewed annually according to legislation.

10. AUTHORITY

MM Approval: Date:

Council Approval: Date: