DR NDZ LOCAL MUNICIPALITY

IT
BACKUP POLICY

Core Business Areas	Corporate Services Department
Operational Area	IT Unit

Version	
Date	
File Name	IT Backup Policy
Business Owner	Director Corporate Services
Date Approved	

Document Classification:
Confidential

Table contents

1. Introduction

Computer information systems and electronic data are valuable assets to the Local Municipality and a substantial investment in human and financial resources has been made to create these systems and information and, as such, a formalised policy has been implemented to:

- □ Safeguard the risk of losing data
- □ Safeguard the confidentiality and integrity of information contained within the systems
- □ Ensure availability of critical data so that information can be utilised as the valuable asset that it is
- □ Reduce business and legal risk.

Departmental critical data and non-departmental critical data are stored on File-servers, and Application-servers. This data can be categorised as:

- □ Personal User data
- □ Business Unit data
- □ Shared data
- □ Databases
- □ Application / System data

2. Scope

The goal for ICT is to ensure that departmental data can be recovered within required and agreed business timescales.

The ICT Manager is responsible for backing up File-servers and Application-servers, according to agreed cycles, and storing these backups in a secure designated area.

- In addition to backing up departmental data, ICT shall perform regular disk capacity management on all data servers and have the right to delete all non-departmental related data after consultation with involved employees. If the disposal of old or damaged backup media is required, such media will be destroyed to prevent the recovery of data from said media.
- All electronic information residing on any departmental computer system is the property of the KZN 436 Municipality and Management may peruse,

monitor and take copies of any information or communication made or received utilising any of the aforementioned systems. Therefore, ICT requires:

- That all requests to restore an employee's user data, residing on File-servers, not requested by the employee or without the permission of such employee, must be authorised by a Supervisor and may be accessed by the ICT Unit.

This policy defines the backup strategy for servers and data within KZN 436 Local Municipality.

4. Timings

Backups run nightly (daily backup) every day.

5. Data Backed up

5.1 Data to be backed up includes but is not limited to the following

5.1.1 Users data

5.1.2 System state of all servers

5.1.3 Mailboxes

5.1.4 Application Data

6. Excluded extensions

User Data / Documents: not all files will be backed up. The following extensions or file formats will be omitted unless for work related purposes:

□	Mpeg	: Animation
□	Mpa	: Audio
□	Mp2	: Audio
□	Mp3	: Audio
□	Mp4	: Audio
□	Exe	: Executable
□	Vob	: Video
□	Wsf	: Window Script file
□	Wma	: Audio

□ Wav : Audio

7. Procedures

- Incremental backups will be performed daily. Data will be added onto the existing media.
- Monthly backups will be made on the last Friday of each month and stored in an offsite storage facility.

8. Media Storage

All weekly and monthly backup media must be stored offsite.

9. Reporting

Backup reports must be reviewed monthly to ensure that relevant data is backed up and to ensure testing and recovery of data. It is recommended that data be randomly selected for recovery to ensure data consistency. These reports are to be signed off and dated by the ICT Manager.

10. Responsibility

The ICT Manager shall perform regular backups. The ICT Manager shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis. The designated person will take weekly and monthly tapes to offsite storage where necessary.

Employees are responsible for ensuring that critical data on their systems is saved in a location that will be backed up to a "Network Drive" or a file server, where it will be backed up. Where such an action is not possible, as in cases where it is done away from access to the Local Municipality network, the data must be copied over at the first available opportunity. It will be the sole responsibility of the employee, under all circumstances, to backup and maintain security regarding personal data.

In addition to workstations, employees have been allocated space per user, secured per user logon ID, on the file servers.

11. Restorations

Data restoration will be done by the ICT Department.

Users that need files restored must submit a request to the ICT Manager in writing and must be approved by their Supervisor.

Information regarding the request where possible must include the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

12. COUNCIL APPROVAL AND EFFECTIVE DATE

Approval of Policy by Council and Effective date: 06/06/2017

MUNICIPAL MANAGER DATE

PP K 19/06/2017