"The City of Heritage"

ULUNDI MUNICIPALITY

INFORMATION TECHNOLOGY

Backup and Restore Policy

APPROVED BY

……

His Worship The Mayor
Cllr. W.M. Ntshangase
Date:

APPROVED BY:

……

Municipal Manager
Mr. S. Khomo
Date:

Contents

1. PURPOSE OF POLICY

- To ensure that the Municipality obeys to a standard backup and recovery control process in such a way that it ensures legislative compliance, best practice controls, service efficiency.
- To define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.
- To ensure all relevant systems are backed up.
- Provide guideline to system administration on backup types and frequency.

2. OBJECTIVE OF POLICY

The primary objective of the policy is to protect the Municipality's data. This policy seeks to outline the data backup and recovery controls for Municipal employees so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice

3. SCOPE

Data Backup and Recovery Policy has been created to guide and assist the Municipality to align with internationally recognised best practices, regarding data backup, recovery controls and procedures. This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

This policy covers the data backup schedules, backup protocols, backup retention, and data recovery. The ICT team will be responsible to manage the infrastructure, backup, and recovery of application data. The policy applies to everyone in the Municipal domain, including its service providers and consultants. This policy is regarded as critical to the effective protection of data, of ICT systems of the Municipality.

4. POLICY ABBREVIATIONS

ICT-InformationCommunicationTechnology

DR- Disaster Recovery

DLP- Data Loss prevention

SQL- Structure query language

5. LEGISLATIVE FRAMEWORK

5.1 Constitution Act 108 of 1996
5.2 Municipal Finance Management Act 56 of 2003
5.3 Municipal Structures Act, Act No. 117 of 1998.
5.4 Municipal Systems Act 32 of 2000, Chapter 4
5.5 Promotion of Access to Information Act 2 of 2000
5.6 Minimum Information Security Standards, as approved by Cabinet in 1996.
5.7 National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
5.8 Protection of Personal Information Act, Act No. 4 of 2013.

6. GENERAL POLICY PROVISIONS

Information security is very important to Ulundi Local Municipality, driven in part by changes in the governing environment and advances in technology. Data backup ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction, and loss of data. The data backup policy is responsible for ensuring that all municipality data that is backed-up and stored on approved systems within the Ulundi Local Municipality environment is recoverable in the event of accidental loss or damage on municipal data.

7. PROCEDURES FOR IMPLEMENTING POLICY

7.1 DATA BACKUP STANDARDS

7.1.1 Critical data must be defined by the Municipality in consultation with ICT, and application owner and must be backed up.

7.1.2 Backup data must be stored at a backup location that is physically different from its original creation and usage location (i.e. The Disaster Recovery Site).

7.1.3 Servers Data backup must be stored on servers' different drive from C-drive.

7.1.4 Data restores must at least be tested monthly.

7.1.5 Procedures for backing up critical data and the testing of the procedures must be documented by the System Administrator. These procedures must include, as a minimum, for each type of data and system:

(a) A definition of the specific data to be backed up.

(b) The type(s) of backup to be used (e.g. full backup, incremental backup, etc.)

(c) The frequency and time of data backup.

(d) The number of generations of backed up data that are to be maintained (both on site and off site).

(e) Responsibility for data backup.

(f) The storage site(s) for the backups.

(g) Recovery procedure of backed up data.

8. ROLES AND RESPONSIBILITIES

8.1 The Municipal Manager

The policy is reviewed on an annual basis and where applicable, changes approved by the Council.

8.2 ICT Manager

The Senior Manager and ICT Manager is responsible for maintaining and ensuring compliance to this policy.

8.3 System owner (Service Providers / Consultants)

The designated owner of the system/ application must ensure that their system is able to run backups and provide reports as evidence.

8.4 Employees

Responsible for making sure that their workstations are connected on the municipality ICT network infrastructure every day for more than an hour to make sure automated back-ups of data runs successfully to OneDrive.

8.5 ICT Division

a) The ICT division is responsible for the backing up user data stored on the network servers, operating system images, systems application and critical content.

b) The ICT Unit will have the primary responsibility of performing these functions daily.

c) Monitoring of implementation and liaison with 3rd party providers will also be its responsibility, under the supervision of the Manager.

d) Review of daily backups and sign-off of successful backups.

e) Failed automated backups to be troubleshoot and manual backup to be ran and recorded.

f) Complete backup register of server / systems.

g) Run backups, tests, and restores of backups monthly

9. DATA BACKUP SELECTION

9.1 All data and software essential to the continued operation of the Municipality, as well as all data that must be maintained for legislative purposes, must be backed up.

9.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.

10. BACKUP SCHEDULE

10.1 CHOOSING THE CORRECT BACKUP SCHEDULE:

(a) Backup schedules must not interfere with day-to-day operations. This includes any end of day operations on the systems.

(b) A longer backup window might be required, depending on the type of backups.

10.2 FREQUENCY AND TIME OF DATA BACKUP:

(a) When the data in a system change frequently, backups need to be taken more frequently to ensure that data can be recovered in the event of a system failure.

(b) Immediate full data backups are recommended when data is changed to a large extent or the entire database needs to be made available at certain points in time. Regular, as well as event-dependent intervals, need to be defined.

(c) Backup stored on server for municipal systems must run starting at 20:00pm and 7:00am and for system state at 23:30pm

(d) Backup stored on cloud (Off-site backups) of the systems must run at 7:00pm.

(e) Backups should run daily in the evening and verified every day in the morning.

11. BACKUP SYSTEM MINIMUM REQUIREMENTS

11.1 ON-SITE WORKSTATION BACKUP SYSTEM

- Workstation data is automatically saved on OneDrive account.

11.2 ON-SITE SERVER BACKUP

Automatic and manual Server Backup with the following functionalities:

- Must be able to run automated backup with the scheduled time
- Generate reports on daily backup ran
- Full daily backups
- Store backups on the server but different drive location from C: drive
- SQL configuration for automated backups.
- Test and restores

11.3 OFF-SITE BACKUP SYSTEM (CLOUD BACKUPS)

Cloud automated backup with following functionalities:

- Frequent automatically at a daily scheduled time data backup, with no human intervention
- Secure encryption and encoding only accessible to authorised persons
- Backup history, including detailed log files
- Launch manual backups if necessary
- Complete restore functionality of the complete data set or selected individual files.
- A fully managed service, with assistance in installation, configuration, daily email notifications and restoration

12. RECOVERY OF BACKUP DATA

12.1. Backup documentation must be maintained, reviewed, and updated by the ICT Manager periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:

(a) Identification of critical data and programs; and

(b) Documentation and support items necessary to perform essential tasks during a recovery process.

12.2. Documentation of the restoration process must include:

a) Procedures for the recovery

b) Provision for key management should the data be encrypted.

12.3. Recovery procedures must be tested at least monthly and Disaster Recovery procedures must be tested at least yearly.

12.4. Recovery tests must be documented and submitted to the ICT Manager.

13. REVIEWAL OF THE POLICY

This policy shall be reviewed annually.

14. APPROVAL OF THE POLICY

The Municipal Council must approve this policy and any amendment thereof.