ICT-05-24

ICT Backup Policy

Document Name: ICT Backup Policy

Policy Number: ICT-012

Version: 003

Date Issued: May 2024

Document Information

Policy	ICT Backup Policy
Version	003
Policy Code	ICT-012
File Name	POL-ICT-05-2024 ICT Backup Policy.doc
Date Issued	May 2024
Policy Enforcer	ICT Manager

Table of Contents

I. Abbreviations and Definitions

Abbreviations	Definitions
ADAM	Active Directory Application Mode
ADRA	Active Directory Recovery Agent
CAS	Polokwane Exchange Client
DAG	Data Availability Group
DC	Domain Controller
DRP	Data Recover Plan
HDD	Hard drive
ICT	Information and Communication Technology
MBX	Mailbox
PC	Personal Computer
SBU	Strategic Business Unit
SQL	Structured Query Language
VEEAM	Is for backing up and managing vSphere and Hyper-V virtual environments – disc to disc backup solution
VM	Virtual Machine

II. Definitions

Accountability: ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action

Authentication: establishing the validity of a claimed entity/verification of the identity of an individual or application

Availability: being accessible and useable upon demand by an authorized entity

Confidentiality: the principle that information is not made available or disclosed to unauthorized individuals, entities or processes

Identification and authentication: functions to establish and verify the validity of the claimed identity of a user

Information and communication systems: applications and systems to support the business, utilizing information technology as an enabler or tool

Information technology: any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

Integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorized manner

Monitoring: performance measurement to ensure the confidentiality, availability and integrity of operational systems and information

Password: confidential authentication information composed of a string of characters

Remote access: the access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection.

Virtual Private Network:

Espionage: Obtaining electronic data while not being authorized for personal gain

Cryptographic devices: Devices to encrypt and decrypt electronic data

1. Preamble

The computer information systems and electronic data are valuable assets to organisations, therefore; backing up data and setting up systems that will allow data recovery. In case of data loss and corruption backup restore shall be implemented to ensure accessibility and availability of electronic data.

2. Purpose and objectives

The purpose of this policy is to define controls that will enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.

The Objectives are:

a) To ensure the regular backups of critical information stored on the network equipment such as servers and etc.

b) To outline the backup and recovery controls for municipal electronic data in line with ICT best practices.

c) To provide continuity, restoration and recovery of critical municipal data and systems.

3. Scope of Application

This policy applies to municipal electronic data stored on the servers, laptops and desktops within the Polokwane Municipal Domain.

4. Legal Framework

The following publications govern the execution of the Municipal Data Backup and Recovery Policy and were taken into consideration during the compilation of the policy:

a) Public Service Governance of ICT Framework Policy

b) The Constitution of the Republic of South Africa, 1996;

c) Local Government: Municipal Systems Act, 2000 (Act 32 of 2000);

d) Local Government: Municipal Finance Management Act, 2003 (Act 56 of 2003);

e) Electronic and Communications Act, 2005 (Act 36 of 2005);

f) Electronic Communications Security Act, 2002 (Act 68 of 2002);

g) Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000);

h) Polokwane Municipality: Supply Chain Management Policy.

i) Minimum Information Security Standard (MISS)

j) Protection of Personal Information Act (POPI Act 4 of 2013)

5. Administration of the policy

The Information Communication Technology Manager is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. Policy Statement

This policy serves to protect all municipal electronic data physically located at Polokwane Municipality, including all its cluster offices, where these systems are under the jurisdiction and/ or ownership of the municipality. All users and staff who utilise such information assets will be made aware of the policy and will act in accordance with it.

7. Requirements

The following shall be adhered to comply with the policy requirements:

a) Backup and recovery procedures must be properly documented.

b) Backup and recovery procedures must be properly implemented by the identified responsible resource(s)

c) Backup and recovery procedures must be tested periodically to ensure effective recovery.

d) Backups, whether physical media, disk or cloud based, must be stored in a manner that ensures quick and reliable access in case of loss of data.

e) Backups must also be protected against unauthorised access, misuse or corruption.

8. Backup Procedures

This policy will outline the procedures that will be applied in the realisation of the municipality's backup strategy. Below is explanation of procedures for the various types of backups defined.

8.1 Onsite Backup Procedure

a) Backups are scheduled to run daily at 17H00 to a dedicated backup storage (disk to disk).

b) Daily backup reports are generated and automatically sent through an email to the DSS for review and record keeping.

c) In case of failure, the backup solution is configured to re-run the failed backup until it is successful.

8.2 Laptops and Desktops backups procedure

a) The municipality has implemented the solution of OneDrive for laptops and desktops backups.

b) Users should make use of OneDrive to store official information.

c) In case of failure, the stored or saved official information will be restored from OneDrive.

8.3 Offsite Backup Procedure

d) Daily backups from the production environment (disk to disk) are automatically configured to replicate to the offsite storage - as soon as the production site backup jobs are completed.

e) The replication process utilises a dedicated internet line.

f) Monthly backup reports are generated and automatically sent through an email to the Data Storage Specialist for review and record keeping.

8.4 Restore procedure on Request

a) The requester should complete a “Restore Request Form” (the form should be completed and approved by relevant authorities).

b) The restore would be executed as per the request.

8.5 Procedure for Testing Restore

In the Quarterly basis which means every six (6) months an Information Communication Technology team will execute the restore testing as per below steps:

a) A “Restore Testing Plan” should be developed and approved by the ICT Manager.

b) A backup of the previous day will be restored as a separate virtual machine.

c) A test will be conducted on relevant applications to check if the restore was successful.

d) A restore report will be generated, signed and filed.

9. Backup Schedule

The Backup Schedule must be used to identify the specific backups to be performed on an ongoing basis. Backups are scheduled to run daily, weekly, and monthly using VEEAM solution.

The table below shows the schedule, backup type and the retention periods of the backups.

Frequency	Backup Schedule	Backup Type	Backup Media	Retention Period
Daily	Mon-Thu	Incremental	Disk	2 weeks
Weekly	Friday (weekly)	Full	Disk	2 weeks
		Full	Disk	4 weeks
Monthly	Friday (last of the month)	Full	Disk	2 weeks
		Full	Disk	1 year

It is important to choosing the correct Backup Schedule considering the following:

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 chosen.

The Frequency and time of data backup requirements are as follows:

a) When the data in a system changes frequently, backups needs 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.

The importance of the Previous versions:

a) The previous two versions of operating systems and applications must be retained at the off-site storage location.

b) Annual and Monthly backups must be retained at the off-site facility.

10. Storage Medium

When choosing the data media format for backups, it is important to consider the following:

a) Time constraints around identifying the data and making the data available;

b) Storage capacity;

c) Rate of increasing data volume;

g) Cost of data backup procedures and tools vs. cost if restored without backup;

d) Importance of data;

e) Life and reliability of data media;

f) Retention schedules; and

g) Confidentiality and integrity.

Should high availability be required, a compatible and fully operational reading device (e.g. External Hard Drive, SD Card) must be obtainable on short notice to ensure that the data media is usable for restoration even if a reading device fails.

11. Roles and Responsibilities

a) The Data Storage Specialist must ensure that systems/applications are backed-up in accordance to the correct schedule, and in case of data loss the restoration can be effectively performed.

b) The Server Specialist must ensure that both virtual and physical servers are up and running in order for backups to be performed as scheduled.

c) The ICT Manager shall delegate two employees (One primary, one secondary) to commit and adhere to each backup schedule.

12. Information and Communication Technology SBU

The ICT SBU shall provide awareness, enforce compliance, and review this policy. The ICT Manager shall participate in policy exceptions review and serve as the final arbitrator in those reviews.

13. Consequences for Non-Compliance

Any person or entity found to be in violation of this policy may be subject to disciplinary action, including termination of any access to Polokwane Municipality network. Violation of this policy may also lead to termination of contracts and commitments to vendors and other entities.

14. Inception Date

This policy comes into effect from the date of approval.

15. Policy Review

This policy shall be reviewed every three (3) years.

16. Enquiries

Enquiries about the policy should be directed to the ICT Manager.

* * * *