Document Identification: **IT Service Continuity (Backup) Policy**		
Section Applicable to the **IT Service Continuity (Backup) Policy - V2**	**following sections**:	**All**
DEPUTY DIRECTOR PLANNING **AND DEVELOPMENT SERVICES**	**Date:**	**25-05-2023**

Effective date: 25-05-2023

Revised Date: 30-06-2023

Location: IT Policies, Forms and Information

Controlled Document

This is a controlled document and may be subject to change at any time.

Owner: Chief Technology Officer

Status: Final Document

Revision History Release No.	**Date**	**Author**	**Revision Description**
V3.0	2023/05/25	Nhlonipho Mdakane	Final Document

Document Identification: **IT Service Continuity (Backup) Policy**		
Section Applicable to the **IT Service Continuity (Backup) Policy - V2**	**following sections**:	**All**

Contents

Document Identification: **IT Service Continuity (Backup) Policy**		
Section Applicable to the **IT Service Continuity (Backup) Policy - V2**	**following sections**:	**All**
DEPUTY DIRECTOR PLANNING **DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES**	**Date**	**25-05-2023**

IT service continuity policy

1 Overview

The purpose of this policy is to document the municipality's strategy towards ensuring that all business-critical IT systems are available and can be recovered in the case of unforeseen circumstances.

This is a high-level document outlining Roles & Responsibilities, Testing Schedules, On-site and offsite requirements, archival requirements, and special media considerations. Detailed information relating to backup and restoration procedures for IT systems in use by the municipality is documented in the IT Service Continuity Procedures.

2 Policy statement

The Municipality is committed to complying with applicable legislation, rules, and standards. Management and all employees must conduct all business activities in accordance with the Municipality's compliance standards in such a manner that:

- Supports the achievement of the municipality's business objectives and financial soundness.
- Will result in a low risk of non-compliance with the letter and the spirit of legislation, rules, and standards.
- Ensures that instances of non-compliance which arise are promptly resolved in a manner which minimizes the adverse consequences thereof.

3 Purpose / Aim

The purpose of this document is to ensure that standards are set to ensure that business critical IT systems maintain an acceptable level of availability.

4 Scope

This policy is applicable to all business-critical IT systems that are in use in the Municipality, including applications, databases, operating systems, and files.

Document Identification: **IT Service Continuity (Backup) Policy**		
Section Applicable to the **IT Service Continuity (Backup) Policy - V2**	**following sections**:	**All**
DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES	**Date:**	**25-05-2023**

5 Administration of Policy

The IT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the IT Steering Committee on an annual basis and recommended changes must be approved by Council.

6 IT service continuity strategy

In line with the IT Strategic plan, the implementation of Cloud computing will play a major role in Amajuba District Municipality's Backup and IT Service Continuity Strategy. The main thrust of this strategy is to reduce the number of components of critical IT systems that are hosted and managed on-site.

In recent years, hosted systems have begun to play in important role in an overall IT service continuity strategy. [I]

Service providers will be asked to host systems, and as part of the agreement, service providers must ensure that systems function effectively and are backed up. Service providers must provide assurance of service continuity capabilities.

Systems that are managed on-site must be hosted on fault tolerant systems and backed up to tape. Systems that are stored on site are required to be replicated live to another physical server in another building.

7 On-site systems (where unable to migrate to a hosted service)

Some workloads may not be managed and hosted by service providers.

These systems should be virtualized where possible and replicated to another Virtual Machine host in a separate building.

Workloads that cannot be virtualized must run on redundant hardware with an appropriate level of RAID implemented.

Document Identification: **IT Service Continuity (Backup) Policy**		
Section Applicable to the **IT Service Continuity (Backup) Policy - V2**	**following sections**:	**All**
DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES	**Date:**	**25-05-2023**

8 Hosted and managed systems

Service providers must provide assurance of service continuity capability.

9 Internet connectivity

Hosted and managed systems depend on internet connectivity. Internet connectivity must therefore be managed effectively with an SLA that included penalties.

In the case of critical systems, Amajuba District Municipality must be able to provide internet connectivity in the case that the main internet connection fails. This will be done by making mobile internet available to directors.

10 Roles & Responsibilities

The role of Amajuba's IT staff will be to:

- Run backups for systems that are not yet managed and hosted.
- Monitor availability of system that are managed and hosted.
- Obtain evidence from service providers that appropriate steps are taken.
-

The role of Service Providers of hosted and managed systems will be to:

- Perform backups and store information securely.
- Provide evidence that system continuity is effectively managed.

11 Backup Schedule and Retention Period

For systems that are not managed and hosted, retention will be as follows:

- Daily backups are made multiple times per day and are kept for 1 week.
- Weekly backups are made on Friday and are kept for 1 month.
- Monthly backups are made on the last Friday of the month and kept for 1 year.
- Yearly backups are made on the last Friday of the year and kept for 5 years.

Document Identification: IT Service Continuity (Backup) Policy		
Section Applicable to the IT Service Continuity (Backup) Policy - V2	following sections:	All
DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES	Date:	25-05-2023

12 Backup window

Backups must complete within 24 hours of the scheduled time. If a backup does not complete within 24 hours of the scheduled time, an exception report must be generated and submitted to management.

13 Service restoration process

For systems that are hosted and managed, restoration will be managed by the service provider.

13.1 In case of on-site hardware failure

Because all on-site systems will be replicated on redundant hardware, recovery in the case of a single server failure will take only minutes. The procedure for switching over workloads to the replica server is detailed in the disaster recovery processes.

In the unlikely case of failure of multiple server failure, recovery will need to be done from backup tape. This procedure will be detailed in the disaster recovery procedures.

For systems that are not yet migrated to the cloud, Amajuba District Municipality staff will perform service restoration as required.

13.2 In case of internet connectivity failure

Directors are assigned mobile internet devices (3G).

14 Service continuity testing

Service continuity capabilities should be tested at least once per year. Results of these tests must be included in the IT department's quarterly reports.

For locally hosted systems, service continuity testing should include recovering selected data from tape.

For managed and hosted systems, service continuity testing should include accessing the service through an alternative internet connection.

15 On and off-site requirements

Hosted systems must be hosted off-site.

Document Identification: IT Service Continuity (Backup) Policy		
Section Applicable to the IT Service Continuity (Backup) Policy - V2	following sections:	All
DEPUTY DIRECTOR PLANNING AND DEVELOPMENT SERVICES	Date:	25-05-2023

For systems that are not yet hosted off-site, backup media will be kept in a secure room in the Amajuba District Municipality new building.

16 Archival requirements

We are required to keep records for a minimum of 5 years.

17 Special media considerations

Backups of local systems are stored on LTO-4 tapes. The municipality should therefore always maintain an LTO-4 capable tape drive.

https://www-935.ibm.com/services/uk/en/it-services/Transitioning_Business_Continuity_to_the_Cloud.PDF