Rustenburg Local Municipality

INFORMATION TECHNOLOGY SERVICES CONTINUITY PLAN

TABLE OF CONTENT

1. Policy Statement

1.1 Information Technology Service continuity management plan is a reactive and proactive process which involves contingency planning for recovery in case the Information and communication technology service is damaged or put out of action by a sudden disaster. Service continuity planning (or resiliency planning) is the process of creating systems of prevention and recovery to deal with potential threats to the Municipality.

Information is a critical enabler for providing and improving service delivery as well as enabling the effectiveness of Rustenburg Local Municipality. Growing dependence on information and communications technology (ICT) and increasing integration between Financial System, Document management system, Geographic information system, management of information and systems support services by Rustenburg Local Municipality (RLM) ICT service providers demands higher system, resilience, shorter recovery times and improved ICT continuity readiness to minimise impact on systems disruption and services efficiency in the event of unplanned outages.

The ICT service continuity Plan (ICT SCP) standard identifies requirements for management of the Municipal ICT service continuity management. The primary objectives are to:

a) Guide continuous improvement of Municipality ICT service continuity practice; and
b) Improve alignment with RLM and IT Unit business continuity planning and disaster management arrangements.

2. The Purpose

The main purpose of the IT service continuity management plan is to support the overall business continuity management process by making sure that the IT service provider(s) are always capable of providing acceptable minimum levels of business continuity related services, and enable ongoing operations before and during execution of disaster recovery.

3. The Objectives

3.1 These service continuity management plan (ITSCMP) is aimed at establishing the minimum baseline security policy and requirements for all IT Infrastructure in order to:

a) Protect the critical network infrastructure and assets of the municipality against attacks.
b) Prevent unauthorized access to Municipal Information systems.
c) Enable the Information technology computing environments that meet the security requirements of this policy and support the business needs of the municipality.

d) To maintain a set of plans on IT service continuity and IT recovery which are in support of the overall business continuity plans. They should also perform business impact analysis, risk analysis, and management activities on a regular basis.

e) To minimize the costs which cannot be eliminated.

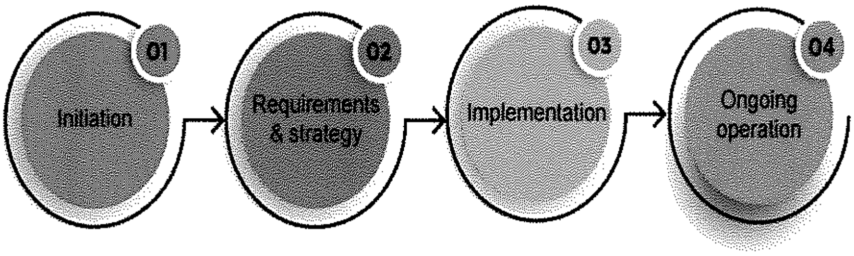
f) To make sure that suitable continuity mechanisms are installed which can meet or exceed the agreed upon targets of business continuity.

g) Analyze the impact which the changes have had on the IT service continuity plans.

h) Make sure that proactive measures are implemented wherever it is economical, which will increase the availability of services.

4. The Implementation of ICT services procedure

Service Continuity Management plan is a process which can evolve over time and not necessarily an end-to-end task which has to be finished in order to possess some value. Service continuity management has to be developed over time. The steps taken to implement service continuity management plan in the Rustenburg Local Municipality are as follows:



Step 1: Identify services and assets

a) Firstly, ICT team should identify all the services and assets in the municipal's possession. Assets are the main component of services.

b) Services and assets can be any of the following:

Service	**Assets**
Printing	Printer
Word Processing	Computer, software
Internet	Computer, LAN, WAN, ISP
Data storage	Server, Hard disk
Technical Support	Procedures. Staff

- The information is critical in the component of the municipality's ICT Technical Support processes.
- ICT technical support processes should be implemented in order to understand the criticality of the services in possession.
- ICT Configuration Management process should be implemented in order to get an idea about the main assets.

Step 2: Identify risks and threats

a) Once the services and assets have been identified, the risks and threats should be identified.

b) What can happen to the services and assets are categorized as risks and the causes which make it happen are categorized as threats.

Risks	**Threats**
Loss of internal ICT services/assets	Fire, power failure, power surge, virus, accidental damage
Loss of external ICT services	Overload of external communication links, bankruptcy.
Loss of data	Technical failure, virus, human error, accidental damage
Unavailability of key technical and support staff	Sickness, transportation problems, resignation
Failure of service providers	Bankruptcy, loss of service provider's own data

Step 3: Make contingency plans

a) Contingency plans are similar to insurance policies.

b) They can be simple & cost effective and can cover minor risks, or they can be complicated & expensive and cover major risks.

c) The type of contingency plan which should be implemented depends on the level of risk which the company is taking.

d) These plans involve prioritizing the services to be restored first, creating backups and storing them on-site and off-site.

Step 4: Document the recovery plan

a) The recovery plan should be documented properly to ensure that all the essential information is present in it.

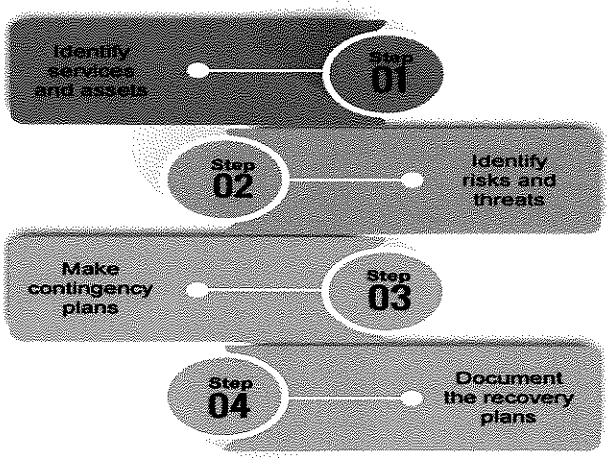
b) This plan should be circulated among the key personnel, who should be kept up to date regarding any changes in the plan.

c) A copy of the plan should be given to the Information Technology Steering Committee as well.

d) Another copy of the recovery plan should be stored off-site to make it accessible in an emergency situation.

4.1 Process Activities for implementation of IT Service Continuity management plan

a) To set up and operate IT service continuity management plan of the municipality, a lifecycle approach should be followed. The stages of the lifecycle approach need to be followed for the IT service continuity management are:


Identify services and assets
Step 01
Step 02
Identify risks and threats
Make contingency plans
Step 03
Step 04
Document the recovery plans

4.1.1 Initiation

The key activities in the initiation stage are:

a) Corporate Governance of ICT Policy Framework implementation.
b) Put Internal Security Control Measure in place.
c) Establish effective Backup solution

4.1.2 Requirements & strategy

The key activities in the requirements & strategy stage are:

a) Business impact analysis
b) Risk assessment
c) Identifies IT operational threats

4.1.3 Implementation

The key activities in the implementation stage are:

a) Develop IT service continuity management plans
b) Develop IT plans, recovery plans, and procedures
c) Risk reduction and recovery
d) Implementation

e) Biannual testing of Recovery plan

4.1.4 Ongoing operation

The key activities in the ongoing operation stage are:

a) Education, awareness, and training to Municipal personnel.

b) Review & audit the Service Continuity plan

c) Information Technology Change Management Policy

5. ICT system criticality assessment.

5.1 The Municipality standard "ICT Critical and At-Risk Systems: Identification and Reporting" outlines the minimum requirements for identifying, managing and reporting on Critical ICT Systems and At-Risk Systems. ICT application criticality assessments shall be managed and reported in line with this standard.

6. ICT system custodianship

6.1 All critical and non-critical ICT applications shall have appointed Application and Data Custodians or Principal end-users. Data and application custodianship includes the appropriate assignment of roles and responsibilities to delegated positions to ensure that Rustenburg Local Municipality data sets and applications are appropriately managed throughout their lifecycle.

6.2 The Application Custodian shall liaise with the Information Technology Manager who has primary responsibility for the day-to-day management of an application including the planning, development, installation, configuration, maintenance and support of the application. This role shall coordinate ICT service providers responsible for the technologies required to support the application including software technologies, hardware and network support. A single application may depend on multiple ICT service providers spread across Municipality Units as well as external vendors.

7. ICT service continuity Processes

7.1 Business continuity requirements

7.1.1 Business continuity requirements shall be managed by the Application Custodian or User Department. The Application Custodian shall engage with agreed RLM and/or Municipality application stakeholders to determine the level of dependence of critical business functions, services and processes on the enterprise application. The importance of this review is to check if the level of business criticality has changed and should be performed on an annual basis for critical systems.

7.1.2 The Application Custodian or User department shall represent the agreed stakeholder requirements to the IT Manager for negotiation and agreement. The Application Custodian shall advise the IT Manager of key business continuity parameters such as hours of usage, application criticality, maximum allowable outage (MAO) and the level of tolerance for data loss due to a disruptive ICT event. This input informs service level requirements and negotiations with the IT Manager and ICT service providers in terms of application recovery priority, recovery time objective (RTO) and recovery point objective (RPO).

7.1.3 The Application Custodian shall maintain a business continuity plan (BCP) describing temporary arrangements and workarounds required to continue business processes and operations during disruptive events causing the application to be fully or partly unavailable. As a minimum, the business continuity plan shall include:

a) BCP owner
b) scope and description of application
c) critical business functions, services and processes
d) business recovery priorities system criticality, business and service continuity objectives including MAO, RTO and RPO
e) system overview criteria for activation and deactivation of the BCP
f) response and recovery strategies including manual processes/workarounds to mitigate the effects of disruptions and return to business as usual including acceptance testing resource requirements;
g) contact details for relevant personnel and stakeholder's communication strategies to keep staff, supplies and stakeholders informed internal and external interdependencies including critical information systems support model including agreed and supported actions by upstream providers and downstream customers where relevant;
h) BCP testing plan.

7.1.4 System recovery plans

7.1.4.1 ICT service continuity readiness shall be managed by the IT Manager. The IT Manager shall engage with the Application Custodian to inform and establish The ICT service continuity requirements to meet the business continuity requirements. The IT Manager shall maintain an application specific system recovery plan (SRP) detailing failover and recovery actions to be taken where there is an impact to critical ICT components. The application SRP response and recovery resilience design, timeframes (RTO and RPO) and recovery priorities are informed by application criticality and MAO. As a minimum the application

SRP shall include:

SRP owner
scope and description of application system criticality, business and service continuity objectives including MAO, RTO and, RPO system overview, resilience architecture and dependencies information security requirements time critical business functions and recovery priorities criteria for activation and deactivation of the SRP

a) failover/ failback processes and work instructions including user acceptance testing.
b) ICT service continuity testing plan.

7.1.4.2 The Information Technology Manager shall engage the internal and external ICT service providers supporting the application to ensure that component ICT system recovery objectives comply with the relevant application business continuity objectives. Where ICT component RTO and/or RPO parameters do not meet the committed application performance, the Information Technology Manager shall undertake the necessary steps to address the gap with the ICT service providers. Where the gap cannot be resolved within existing ICT service capabilities, the Application Custodian shall perform a risk assessment to determine risk rating and recommend the required treatments for Application Custodian consideration and endorsement. Any consequent risks for which the Information Technology Manager is accountable including ICT service provider gaps shall be recorded in the Information Technology Manager's risk management system and managed in accordance with the endorsed treatments.
ICT service providers shall ensure that component ICT systems for which they are responsible meet the required RTO and RPO criteria. They shall participate in planning, documentation, validation and testing of the performance of their services as agreed with the Application Custodian.

7.1. 4.3 ICT Infrastructure plans of RLM shall maintain an overarching ICT Service Continuity Plan (ICT SCP) that outlines the overall process for the recovery of critical underpinning Municipality ICT infrastructure and systems by asset (e.g. data centre, enterprise network, identity management). Municipal Management shall ensure that all ICT service providers meet their respective service level requirements relating to ICT service continuity and disaster recovery planning (DRP). Where Municipality ICT service providers deliver critical applications, underpinning infrastructure or services under formal service and support agreements directly to IT unit, they shall engage the accountable Municipal ICT representative (IT Manager or similar position) to agree the approach for aligning Municipality ICT service continuity response with the Municipal Integrated Development plan.
Municipality ICT service providers shall:

a. publish service level details for the relevant critical applications, underpinning infrastructure or services, including key contacts and escalation arrangements, support hours of coverage, service availability targets, RTO and RPO targets;

b) participate in Municipal ICT service continuity planning and testing as required to ensure alignment of critical applications, underpinning infrastructure or services response and restoration activities with Municipal business continuity and ICT service continuity arrangements;

c) maintain system recovery plans for the restoration of the relevant critical applications and underpinning infrastructure and services in accordance with agreed performance criteria; and

d) perform routine testing and validation of system recovery plans and report readiness to Municipality accordance with the service and support agreement.

e) To assist effective Municipality ICT service continuity readiness, it is desirable that RLMs will:

plan for and manage Municipal business continuity response in the event of a major incident that impacts access to critical applications, underpinning infrastructure or services used by the municipality;

f) conduct business impact assessments on critical Municipal functions to inform ICT Service criticality and continuity requirements to develop business continuity objectives Including MAO and downtime procedures;

g) maintain an overarching municipal ICT service continuity (disaster recovery) plan incorporating critical Municipality applications and underpinning infrastructure and services to minimise the business impact and provide timely recovery of ICT services in accordance with municipal business requirements; and coordinate testing and validation of municipal service continuity (disaster recovery) plans with Municipality ICT Service Providers as required.

7.2 ICT service continuity testing

7.2.1 Critical applications, infrastructure and services must undergo scheduled ICT Service continuity tests to:

a. ensure that resilience design and recovery strategies meet business objectives;

b) demonstrate the ability of ICT providers to respond and recover services within agreed service levels and recovery objectives;

c) ensure familiarity of business and ICT staff with downtime and recovery practices.

7.2.2 The User department shall determine the risk and appetite for testing ICT service continuity and associated business continuity procedures across all critical applications in collaboration with Municipality application stakeholders.

8. Roles and Functions of IT Service Continuity Management Personnel

8.1 Municipal Manager

The Municipal Manager establishes and maintains appropriate systems of internal control and risk management in accordance with the Municipal System Act 32 of 2000 as amended, Municipal Finance Management Act of 2003 as amended.

8.2 Director: Corporate Support Services responsible for IT Unit shall:

a) ensure capability to conduct ICT service continuity is maintained for their accountability area;

b) communicate the importance of effective ICT service continuity management and ensure ICT Unit Personnel are aware of their roles and responsibilities to ensure effective response to disruptive events; and confirm responsibility and point(s) of contact for coordinating ICT Service Continuity arrangements within the municipality.

8.3 IT Manager

a) Handles the responsibility of service continuity

b) Owns the service continuity management process

c) Leads the service continuity recovery plan's development

d) Invokes the service continuity recovery plan personally

e) Is a senior member of the ICT or technical support Personnel

f) Has no need to be technical

g) Should have an understanding of the ICT priorities of the users.

h) Should appoint someone else to cover during absence

i) Should not delegate responsibility

8.4 Service continuity recovery team

a) Is led by the IT Unit head/ IT Manager

b) Participates in the testing and invocation of the service continuity recovery plan.

c) Includes the technical staff for technical procedures

d) Includes users for testing and during the actual invocation

e) Includes representatives from the departments for communication and coordination.

8.5 ICT service providers responsible for technologies required to support an application is required to:

a. participate in testing and exercises for continuity arrangements related to ICT
b. component systems for which they are responsible;
c. contribute to business continuity arrangements and BCPs developed by Chief Risk Officer;
d. ensure the redundancy, resilience and recovery performance of all component ICT systems meet the agreed business criticality and continuity requirements; and
e. maintain component ICT documentation and work instructions as part of the system recovery plans.

8.6 Chief Risk Officer responsible to ensure the effectiveness and supports ICT service continuity plan readiness is:

a. complying with and participate in strategies for preparedness, prevention, response and recovery including ensuring appropriate monitoring and governance proactively communicate risks with relevance to critical business functions to the responsible executive and/or director consider any necessary provisions to support business continuity and/or ICT disaster recovery in contracts and third-party agreements.

8.7 All Municipal Personnel shall:

a. Be aware of the Municipal business continuity arrangements, where appropriate (through training, awareness and testing of plans).

b) Comply with and participate in preparedness, prevention, response and recovery strategies to ensure business continuity of critical business functions.

9. LEGISLATIVE FRAMEWORK

9.1 Municipality must be aware of and comply with the legislative landscape applicable to and within their context, including the followings but not limited to:

a) King IV Report on Corporate Governance 2016.
b) Control Objectives for Information Technology (COBIT).
c) Information Technology Infrastructure Library (ITIL).
d) Municipal Finance Management Act of 2003.
e) The Electronic Communications and Transactions (ECT) Act 25 of 2002.
f) National Strategic Intelligence Act 2 of 2000 applicable for South Africa.
g) Municipal System Act 2000 as amended.
h) State Information Technology Act 88 of 1998
i) Disaster management act 57 of 2002

10. POLICY REVIEW

10.1 This policy shall be reviewed after three years from date of adoption and may also be reviewed when there is a need to address a critical issue not addressed or not adequately addressed by this policy. The policy may also be reviewed to address issues as indicated by the Auditor General's Office.

11. GLOSSARY

Application / ICT System A software system deployed by the agency which has part of an agency's business process embedded with it.

Application Custodian A position designated with accountability for the operations, use, management, care and maintenance of an Application software.

Information Technology Manager A position designated with responsibility for the day-to-day Management of an application including the planning, development, installation, configuration, maintenance and support of the application.

Business Continuity The uninterrupted availability of essential Municipal Functions.

Business Continuity Plan (BCP) Documented procedures that provide guidance on how to prepare, prevent, respond and recover from a disruptive event. This includes business activities associated with maintaining availability of people, assets and property vital for the continuity of critical municipal functions.

Business Impact Analysis (BIA) The process of analysing business/municipal functions and the effect that a disruption may have upon them.

Critical ICT Service An ICT system that is relied upon to the extent that an outage would pose significant risk to the business and therefore, required a higher level of maintenance to ensure availability and performance. This is reflected in the ICT system having a consequence of failure of High or Very High according to the municipality risk analysis matrix.

Data Custodian A position designated with responsibility and overall accountability for the Data within the Data Set, Data Collection and/or Application allocated.

ICT Service Provider A position designated with responsibility for the technologies required to support the application including software technologies, hardware and network support. Technologies are involved with either essential infrastructure or general productivity software and hardware; an application is related to business processes.

Disruptive event Maximum Allowable Outage Maximum time that an municipal can tolerate the disruption of a critical (MAO) business function. Also known as Maximum Tolerable Period of Disruption (MTPD).

Recovery Point Objective (RPO) The point in time to which systems and data must be recovered after an outage (e.g. end of previous day's processing). RPO(s) are often used as the basis for the development of backup strategies.

Recovery time Objective (RTO) The period of time in which minimum levels of services and /or products and the supporting systems, applications or functions must be recovered after a disruption has occurred.

System Recovery Plan (SRP) An ICT Service Provider technical artefact detailing failover and recovery actions to be taken where there is an impact to critical Information and Communications Technology (ICT) Components.