

ICT DISASTER RECOVERY POLICY



Sundays River Valley
Municipality

042 230 7700



078 266 6230



srvm@srvm.gov.za



[@sundaysrivervalley](https://www.facebook.com/sundaysrivervalley)



www.srvm.gov.za



23 Middle Street, Kirkwood, 6120



P.O. Box 47, Kirkwood, 6120

Table of Contents

1.	PREAMABLE	Error! Bookmark not defined.
1.1.	Objective	4
1.2.	Scope.....	4
2.	POLICY	5
2.1.	Policy Statements.....	5
2.2.	IT Incidents & Severity Level	5
2.3.	Business Impact Analysis	6
2.4.	Risk Assessment	7
2.5.	DR Testing Policy	7
2.6.	IT DR Training and Awareness Policy	7
2.7.	IT DR Maintenance Policy	7
2.8.	Periodic Review of the IT DRP Policy	7
2.9.	Preventative Actions	7
2.10.	Corrective Actions	7
3.	ROLES AND RESPONSIBILITIES	8
3.1.	IT Disaster Recovery and BCM Committee	8
3.2.	Disaster Recovery Coordinator	8
3.3.	Disaster Recovery Team.....	8
3.4.	Internal Communications.....	8
3.5.	Media and Stakeholder Communications.....	8
4.	NON-COMPLIANCE WITH POLICY	9
4.1.	Exceptions, Migrations and Timeframes	9
5.	REVIEW OF POLICY	

Document Administration
Abbreviations/Acronyms

Term	Description
BCI	Business Continuity Institute
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BIA	Business Impact Analysis (Assessment)
DR	Disaster Recovery
DRP	disaster recovery plan
ISO	International Standards Organisation
IT	Information Technology
IT DR	Information Technology Disaster Recovery
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives

1. Preamble

The core functions of Sunday's River Valley Municipality (hereinafter referred to as "SRVM") heavily depend on computer-supported information processing and telecommunications, thereby IT services. The increasing dependency on computers and telecommunications for operational support poses a risk that a lengthy loss of these capabilities could affect the overall service delivery and performance of the Municipality.

Any event that causes disruption to the IT services of the Municipality, could severely impact upon the Municipality at large and ultimately the customer base. To this extent, the Municipality has initiated an agenda for setting up an IT disaster recovery plan covering various departments and critical technology components. It will be the duty of this programme to ensure continuity and recovery of SRVM IT services, thereby ensuring reliability and redundancy within the IT environment in order to minimise downtime and ensure availability of critical systems during a disaster situation.

The Disaster Recovery programme will ensure that SRVM's continuity objectives are supported from a technology standpoint and ensure the recovery of IT infrastructure in the event of a disaster in line with the Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) defined by business. Therefore, this document should be read in conjunction with SRVM IT disaster recovery plan.

1.1. Objective

The objective of this policy is to formalise SRVM's executive commitment to coordinate the recovery of critical systems and technologies during a disaster or disruptive incident in an orderly and timely manner. This policy establishes the principles and framework necessary to ensure emergency response, resumption and recovery, restoration and recovery of SRVM's IT operations in response to a business disruptive event.

It is important to highlight that human lives (all SRVM employees as well as third-parties who may be working on SRVM premises) are the first priority for SRVM in the event of a disaster occurring onsite. The next most important priority is the restoration of work processes especially from a technology standpoint.

1.2. Scope

SRVM's IT Disaster Recovery (ITDR) scope applies to all information systems and technologies which supports SRVM's day-to-day business processes.

2. POLICY

The following section illustrates DR related policy applicable in SRVM.

2.1. Policy Statements

SRVM is committed to its employees, customers and stakeholders to ensure that critical services are resumed at the earliest possible time, in the event of any disruptive incident.

To this end, SRVM will provide:

- A disaster recovery plan in support of the business objectives which shall cover vital and critical technology elements and systems, in accordance with key business activities.
- ICT personnel within SRVM responsible for reviewing the Disaster Recovery plan and testing its effectiveness on a regular basis.
- Recovery teams ensuring that these plans are capable of supporting a minimum acceptable level of service.

2.2. IT Incidents & Severity Level

The following standard incidents may apply to the SRVM IT environment:

Incident Name	Incident description
Desktop computer unavailability	An IT incident occurs that results in more than 30 desktops/laptops that are in use by SRVM employees are not available, such that the physical desktops, software and data is not available
Server crash	An IT incident occurs resulting in 1 or more servers crashing such that the server hardware is still available however the services/systems/data residing on those servers are unavailable.
Complete server unavailability	An IT incident occurs that results in the servers being unavailable, such that the server hardware, software and data are unavailable.
IT Disaster	An IT incident occurs that results in both of the following scenarios: <ul style="list-style-type: none">• The servers are unavailable, such that the server hardware, software and data is unavailable and the desktops/laptops that are in use employees are not available, such that the physical desktops, software and data is not available.
Business Disaster	An IT incident occurs that results in the following scenarios: <ul style="list-style-type: none">• The servers are unavailable, such that the server hardware, software and data is unavailable; the desktops/laptops that are in use by employees are not available, such that the physical desktops, software and data is not available; and the SRVM buildings are not available.

Outlined below are the severity level definitions for software-related incidents:

Incident Severity Level (Software)	Incident Severity Level Description
Severity Level – 1 (Cosmetic)	<p>Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Acceptable workaround available.</p> <ul style="list-style-type: none"> • Minor problem not impacting service functionality. • Enhancement requests, missing or erroneous documentation. • Minor problem or question that does not affect delivery of service.
Severity Level – 2 (Minor)	<p>System performance issue or bug affecting some but not all users. Short-term workaround is available, but not scalable.</p> <ul style="list-style-type: none"> • Service is operational but partially degraded for some or all customers, and an acceptable workaround or solution exists. • Problem with non-critical feature or functionality
Severity Level – 3 (Major)	<p>Major functionality is impacted or significant performance degradation is experienced. Issue is persistent and affects many users and/or major functionality. No reasonable workaround available.</p> <ul style="list-style-type: none"> • Service is operational but highly degraded performance to the point of major impact on usage. • Important features of the Software as a Service offering are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion. • Access to a particular third-party application or service provider deemed noncritical is impacted.
Severity Level – 4 (Critical)	<p>Critical production issue affecting all users, including system unavailability and data integrity issues with no workaround available.</p> <ul style="list-style-type: none"> • Service is down or unavailable. • A critical part of the Software infrastructure is unavailable or inaccessible, resulting in total disruption of work or critical business impact. • Service crashes or hangs indefinitely causing unacceptable or indefinite delays for resources or response. • Data corrupted or lost and must restore from backup. <p>A critical documented feature / function / software module is not available.</p>

2.3. Business Impact Analysis

Formal business impact analysis (BIA) shall be carried out for all functions/departments at least once every year in order to determine the requirements for the disaster recovery plan. The

business impact assessment (BIA) shall be reviewed and updated on an annual basis, to reflect any changes taking place within the Municipality.

2.4. Risk Assessment

A formal risk assessment shall be carried out at least once a year in order to determine the requirements for the disaster recovery plan. The risk assessment shall be performed and any risk register(s) updated on an annual basis or when changes are introduced in the SRVM IT environment.

2.5. DR Testing Policy

The disaster recovery plan shall be tested at least twice every year and remediation steps shall be adopted where necessary, taking into account the testing results arising from the DR test. This is to ensure that the plan can be implemented in the event of an emergency and that management and SRVM personnel understand how this will be executed.

2.6. IT DR Training and Awareness Policy

General IT DR awareness sessions should be held with all staff (current and new joiners) annually. SRVM staff with specific roles in the IT DR plan should undergo training to ensure that they are able to execute their roles in the event of a disaster.

2.7. IT DR Maintenance Policy

The disaster recovery plan (DRP) shall be continuously monitored to ensure that changes in the way business functions and the supporting infrastructure are reflected in the plan. Improvements identified as a result of testing shall also be included in the DRP. All changes shall be assessed as part of change management process.

2.8. Periodic Review of the IT DRP Policy

SRVM's Internal Audit shall as part of their Annual Planning exercise include the disaster recovery plans for any ad-hoc reviews. This policy should be reviewed at least once every year as part of the annual controls effectiveness cycle assessment.

2.9. Preventative Actions

SRVM's Information Technology department shall ensure necessary steps are taken to periodically conduct risk assessments and review the DR policy, procedures and plans to identify potential non-conformities and their causes to reduce or eliminate the chances for recovery failures. All such action taken shall be documented.

2.10. Corrective Actions

SRVM's Information Technology department shall take actions to eliminate the causes of non-conformities identified with the implementation and operation of the disaster recovery plan to prevent their recurrence. All such actions taken shall be documented.

3. ROLES AND RESPONSIBILITIES

3.1. IT Disaster Recovery and BCM Committee

The proposed composition of the committee comprise of the following:

- Chief Financial Officer (CFO)
- Manager of Human Resource Manager
- Manager of ICT Services
- Director of Corporate Services
- Director Of Community Services
- Manager of Supply Chain Management
- At least 2 X Representatives from Operations

The Committee is a decision-making group that coordinates Emergency Management, Crisis Management, Business Continuity and Information Technology Disaster Recovery efforts across the SRVM. The committee addresses municipality-wide issues that relate to the continuity of business following a disaster and makes recommendations and resolutions.

3.2. Disaster Recovery Coordinator

The Disaster Recovery Co-ordinator shall have the overall accountability and responsibility for the coordination, implementation and maintenance of the disaster recovery and overall monitoring of all DR processes.

3.3. Disaster Recovery Team

The Disaster Recovery Team shall be responsible for implementing the disaster recovery operations including the restoration of computer processing and networking activities, as well as providing on-going technical support during the recovery effort and shall be headed by the Manager of ICT Services with support from the staff in the ICT Department. Other team members shall be drawn by the Committee as required and coordinated with the Disaster Recovery Co-ordinator.

3.4. Internal Communications

The Communications Manager / Media Liaison Officer shall be responsible for handling all internal employee communication in the event of a disaster and relevant information during the restoration.

3.5. Media and Stakeholder Communications

Media Communication shall be handled in line with approved SRVM media communication policy. The office of the Municipal Manager shall be informed of all media and other external stakeholder communications. The responsible Communications Manager / Media Liaison Officer shall obtain communication directives from the Disaster Management Team, and shall communicate information during the disaster and restoration phases to employees, suppliers, other external stakeholders and the media. SRVM employees and visitors are not permitted to

give media interviews in any way regarding disruptive or non-disruptive disasters. All communication with the media shall be facilitated by the responsible Communications Manager/ Media Liaison Officer.

4. NON-COMPLIANCE WITH POLICY

Safety of employees and continuity of operations during a crisis or an incident is the responsibility of everyone physically working on SRVM premises including all employees, service providers and third-party vendors. The Information Technology Disaster Recovery (IT DR) policy statements described herein, defines the basic minimum level of requirements for 'safety, availability and continuity' of SRVM's resources and services to clients. This policy also provides guidelines for developing, maintaining and testing IT DR plans and risk assessments. Non-compliance with the required measures and behaviours outlined in this policy could pose a business risk to SRVM and could significantly impact SRVM's operations and damage its assets and reputation. Therefore, compliance with SRVM's IT DR policy is **mandatory** for all SRVM employees, as well as any third parties (such as outsourcing providers, contractors, alliance partners, licensees, etc.) who may be required to physically work on SRVM premises or utilise SRVM's information technology platforms.

It is prohibited to bypass the Disaster Recovery mechanisms provided by SRVM in this policy or in any supporting plans, guidelines or procedures.

4.1. Exceptions, Migrations and Timeframes

All SRVM personnel and systems must comply with the statements in this policy from the date of release. Where a longer transition is required to achieve compliance, a documented business justification must be submitted with proposed timelines as an Exception to the IT DRP team.


Any exceptions to this Policy must be clearly documented and submitted to the Committee for evaluation and approval. Only exceptions which have been approved are valid. All exceptions to this Policy will be fully motivated and documented by those seeking the exception, and agreed to by the relevant affected parties. All exceptions will be reviewed at least annually by the relevant Individual/s around the particular area/s affected by the exception.

5. REVIEW OF POLICY

This Policy will be reviewed annually and when there are changes to the ICT system.

6. VERSION CONTROL

VERSION	DATE	AUTHOR	STATUS
1	30 June 2022	ICT	Final Draft
2	8 July 2022	Council Approved	Final



S H RINE
MAYOR

08 JULY 2022