TSWELOPELE
LOCAL MUNICIPALITY
A MUNICIPALITY IN PROGRESS

DISASTER RECOVERY & BUSINESS CONTINUITY PLAN INFORMATION TECHNOLOGY

DOCUMENT APPROVAL			
Positon	Name	Signature	Approval Date

COUNCIL APPROVAL	
Item Number	Approval Date

TABLE OF CONTENTS

1. PURPOSE

1.1 The purpose of the IT Disaster Recovery Plan is to ensure that, should the municipality experience disaster of any nature (e.g. firebreak, power surge or damage to the building, etc.), the municipality has contingency plans for back-up systems.

1.2 The plan is there to make staff aware of what procedures should be followed when connecting back-up systems and who the key contact persons for the systems are.

1.3 This Disaster Recovery Plan is there to ensure that the Disaster Recovery Team is appointed and trained properly, so that, even in the event that IT staff is not in the office, the team can take charge successfully.

2. OWNERSHIP

2.1 The Corporate Services Department is responsible for managing all computer systems for the Municipality; hence, the Corporate Services Department must make sure that in times of disasters a proper plan is in place. The Corporate Services Department is therefore the custodian of the Disaster Recovery Plan.

2.2 The designated Disaster Recovery Plan contact person is the IT Officer: The contact details of the IT Officer are as follows:

Tel (w): (+27 51) 853 1111

Cell: (+27 83) 347 7219

2.3 The Disaster Recovery Plan shall be kept at Tswelopele Local Municipality. The contact person is the Director Corporate Services. The contact details are as follows:

Tel : (+27 51) 853 1111
Fax : (+27 51) 853 1332

3. DISASTER RECOVERY PLAN COVERAGE

3.1 The IT Officer (Department), Chief Financial Officer in consultation with the Municipal Manager, has authority to declare a disaster. The Disaster Recovery Team will consist of IT Officer, Chief Financial Officer, Director Corporate Services and the Municipal Manager.

3.2 The systems that the municipality have in place are:

- Financial Management System
- Payroll System
- Domain Controller
- NAS Devise For(User Data)
- TMS - Telephone Management System
- Virtual server

4. ABBREVIATIONS

DBA Database Administrator
NA Network Administrator
LAN Local Area Network
SAPS South African Police Service
DRP Disaster Recovery Plan
BCP Business Continuity Plan
IDS Intrusion Detection System

5. TERMS & DEFINITIONS

Audit

Activities to detect and investigate events that might represent a threat to security / independent review and examination of system records and activities in order to test for effectiveness of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures.

Authentication

The process of identifying individuals as belonging to a class, which may be a group or an individual.

Authorisation

The process by which a determination is made whether or not the identified individual or class is authorised to access an Information Resources, and at what level (read only, create, delete, modify). Authentication is a term that is also used to verify the integrity of network nodes, programs, or messages.

Authorised User

A municipal employee, student or other individual affiliated with the municipality who has been granted authorisation by the Electronic Information Resource Manager, or his or her designee, to access an Electronic Information Resource and who invokes or accesses an Electronic Information Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with the municipality. The authorisation granted is for a specific level of access to the Electronic Information Resource as designated by the Electronic Information Resource Manager, unless otherwise defined by municipal policies. An example of an authorised user includes someone who handles business transactions and performs data entry into a business application, or someone who gathers information from an application or data source for the purposes of analysis and management reporting.

Availability

Being accessible and useable upon demand by an authorised entity.

Business Continuity Plan

A plan for the continued operation of critical business administration in the case of a disaster affecting normal functioning. A Business Continuity Plan is more all-inclusive than a Disaster Recovery Plan, which normally relates to information systems only.

Disaster

Any event or occurrence that prevents the normal operation of Electronic Information Resource(s) for a period of time, such that the resulting disruption and / or losses exceed the acceptable limits established consistent with the policy. A disaster may occur as a result of a natural disaster such as a flood, fire or earthquake, employee error or other accidents, long-term system failures and criminal or malicious action.

Disaster Recovery Plan

A written plan including provisions for implementing and running Essential Electronic Information Resources at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster.

Information Security

The science and study of methods of protecting information in computer and communication systems against unauthorised disclosure, transfer, modification and destruction whether accidental or intentional.

Integrity

The inherent quality of protection that maintains the accuracy of entities of an information system and the information in a system and ensures that the entities and information are not altered or destroyed in an unauthorised manner.

Intrusive Computer Software

Intrusive computer software (such as a computer virus) is an unauthorised program designed to embed copies of itself in other programs, to modify programs or data, or to self-replicate. Intrusive computer software may be spread via removable storage media (e.g. diskettes for personal computers) or via a network. The term "*intrusive computer software"* as it is used in this policy is intended to encompass the variety of such unauthorised programs, including viruses, worms, Trojan Horses, etc.

Local Area Network (LAN)

A high bandwidth bidirectional communication infrastructure which enables users to share resources and which operates over a limited geographic area.

Logical Access Control

Access control mechanisms that are implemented and enforced by network operating systems, operating systems, application software and communication processes for example authentication, resource access, audit, etc.

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.

Physical Access Control

Physical control measures to prevent and / or detect unauthorised access to a security area.

Physical Security

Measures used to provide physical protection of resources against deliberate and / or accidental threats.

Security

Measures taken to reduce the risk of unauthorised access to Electronic Information Resources, via logical, physical or managerial means, and damage to or loss of Electronic Information Resources through any type of disaster, such as employee error or other accidents, long-term system failures, natural disasters, and criminal or malicious action. Security also encompasses measures taken to reduce the impact of any violation of security or a disaster that occurs despite preventive measures.

Server

A multi-user computer, including mainframes, servers and personal computers providing services to multiple users. A computer employed, as a single-user workstation is not considered a server.

6. EMERGENCY CONTACT DETAILS OF KEY PERSONS

In the event that a problem cannot be resolved locally, the Disaster Recovery Team in consultation with the Municipal Manager would recommend the relevant companies below to be contacted to resolve the problem.

Details	Contact Person	Telephone Number	E Mail Address
Munsoft System	**Support Centre**	011 215 8000	**nkululeko.nondzaba@itna.co.za**
Ntelecom TMS	**Support Centre**	051 412 6300	support@ntelecom.co.za
Ntelecom Internet	**Support Centre**	051 412 6300	support@ntelecom.co.za
Telkom	**Corporate Service**	10214	10214@telkom.co.za
Ntelecom e-mails	**Support Centre**	051 412 6300	support@ntelecom.co.za
ITNA	**Mr. N. Nondzaba**	076 330 3031	**nkululeko.nondzaba@itna.co.za**
Ntelecom	**Mr Charles van der Berg**	051 412 6300	**charles@ntelecom.co.za**
ITNA	**Miss Nonhlanhla Ngoma**	086 123 4862	**Nonhlanhla.Ngoma@itna.co.za**

7. PRIORITY LEVELS OF KEY SYSTEMS

The Municipal Systems will be listed according to their priority order below:

- Munsoft Financial System
- Ntelecom -TMS System
- Telkom - Diginet lines
- Ntelecom - Managed Internet Gateway - Email & Internet
- Network Switches
- Desktops & Laptops

8. DEADLINE FOR KEY RECOVERY

If there is a disaster of any kind, it must only take a maximum of three days to recover and have all users online. This is dependent on the nature and circumstances surrounding the disaster.

9. CONFUGURATION OF SYSTEMS

SERVERS	
Details	**I.P. Addresses**
Domain Controller (tswelopele.gov.za)	10.0.0.241
Munsoft Financial Management System	10.0.0.253
File Sever (NAS Devise)	10.0.0.20
Payroll System	10.0.0.252
Print Server	10.0.0.246

IP RANGE & GATEWAY			
Details	**IP Addresses**	**Gateway**	**Subnet Mask**
Bultfontein	10.0.0.xx	10.0.0.150	255.255.255.0
Hoopstad	192.168.0.xx	192.168.0.10	255.255.255.0
Tikwana	192.168.0.xx	192.168.0.10	255.255.255.0
Phahameng	192.168.81.xx	192.168.81.253	255.255.255.0
Technical Bulfontein	192.168.182.xx	192.168.182.254	255.255.255.0

TELEPHONE MANAGEMENT SYSTEM – LAN BUFFERS	
Details	**I.P. Addresses**
Bultfontein TMS	192.2.1.20
Hoopstad TMS	192.2.1.20

10. PREVENTATIVE MEASURES

- There are two 20 kVA Uninterrupted Power Supply (UPS) that can power the servers and processing facilities for a minimum of 2 hours.
- There is also an air conditioning system in the server room for the purpose of maintaining a constant cool temperature of 16 degrees Celsius.

11. BACK-UP PROCEDURES

- There are back-ups taken on a daily, weekly & monthly basis for the Financial Management System, Payroll System and the NAS takes back-ups of user data daily.
- Financial Management System and the Payroll System - the municipality make use of Redstor Back-upPro software that is hosted offsite.
- Because the Financial and Payroll System are real life transecting the back-ups are automated setup.
- Back-ups run every evening at 22:00 completed before 07:00.

- The e-mail gets automated send the IT Official who is responsible for monitoring the back-ups.
- For the successful or failure of the Back-up.?????

Below is the screen shot of the Redstor Back-upPro to show the successful back-up completion?

Back-up success report for past week.

Back-up Group: MUNSOFTDR **Back-up Account:** TSWELOPELE [Run]

Back-up Group: MUNSOFTDR\TSWELOPELE	09 Feb 2018	10 Feb 2018	11 Feb 2018	12 Feb 2018	13 Feb 2018	14 Feb 2018	15 Feb 2018
TSWELOPELE	.	.	.	.	.	.	.

Red cross means FAILED
Green dot means SUCCESS!!

- When the automated back-up fails to run or complete at the scheduled time the investigation team assigned for the back-ups informs the municipality, investigate the issue and run the manual back-up.
- The person responsible for monitoring the municipality's offside back-up is Nonhlanhla Ngoma.

Below is the screen shot of the Redstor Back-upPro to show the successful back-up that failed on 8 October 2017

Back-up success report for past week.

Back-up Group: MUNICIPALITIES\TSWELOPELE **Back-up Account:** TSWELOPELE-PAYDAY [Run]

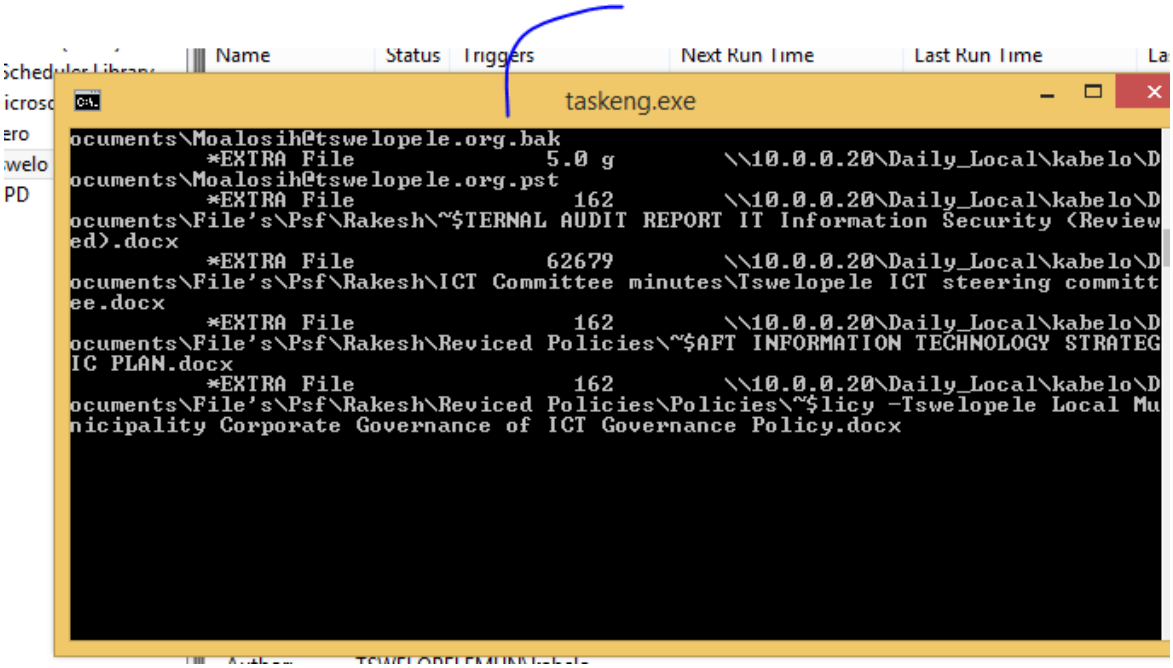
Back-up Group: MUNICIPALITIES\TSWELOPELE\TSWELOPELE-PAYDAY	04 Oct 2017	05 Oct 2017	06 Oct 2017	07 Oct 2017	08 Oct 2017	09 Oct 2017	10 Oct 2017
TSWELOPELE-PAYDAY	.	.	.	.	x	.	.

Red cross means FAILED
Green dot means SUCCESS!!

- The municipality also make use of a Network Attached Storage (**NAS**) device which is a storage device connected to a network that allows storage and retrieval of data from a centralised location for authorised network users and heterogeneous clients.
- The user folders are created on the client workstation with their folder names.

- The users are required to store only their work related documents on the user's folders.
- Non-work related information on the user data folders will be removed from the NAS device.
- Daily in the morning the scrip run from the workstations to synchronize user folders the NAS where the back-up is been stored.

Below the screen shot of the back-up scrip



12. RECOVERY PROCEDURES

- As we said on the back-up procedures the back-ups runs daily & monthly basis on the Financial Management System, Payroll System and the NAS takes back-ups of user data daily.

- On the monthly basis the service provider send municipality the Disaster Recovery Report.

- Biannually the service provider send the Disaster Recovery Simulation Certificate whereby the municipality test the accuracy of data at the data centre then the two parties after doing simulation and they both agrees on the accuracy of data the certificate gets signed for the completeness.

13. ANNEXURES

Annexures Attached are herewith the template of the Disaster Recovery for Munsoft and PayDay Reports.

- DR Reporting - Tswelopele LM- Annexure A

- Extended DR Reporting - Tswelopele LM- Annexure B

14. REVIEW

- This disaster recovery & business continuity plan information technology Plan shall be subjected to the review process after 1 year of its operation should there be any changes. It shall remain in operation during the review process. Changes to it while it is still in operation shall be made after consultation with the Municipal Manager as the Accounting Officer and be approved by the Council.