BELA-BELA LOCAL MUNICIPALITY

Chris Hani Drive, Bela- Bela, Limpopo. Private Bag x 1609
BELA-BELA 0480
Tel: 014 736 8000 Fax: 014 736 3288
Website: www .belabela.gov.za

OFFICE OF THE MUNICIPAL MANAGER

Information and Communication Technology

Disaster Recovery Policy

TABLE OF CONTENT

POLICY AUTHORITIES

Compiled by	D Nkuna
Designation	Divisional Manager IT
Signature	
Date	
Supported by	
Designation	
Signature	
Date	
Approved by	
Designation	
Signature	
Date	
Effective date	From date of approval

1. MANDATE OF THE ICT DIVISION

1.1 It is the mandate of the ICT Division to ensure business recovery and availability of critical business functions during or after a loss of normal business operations.

2. OBJECTIVE OF THE POLICY

2.1 The objective of this document is to provide a plan that responds to a disaster that destroys or severely cripples ICT services.

2.2 The intent is to restore critical business operations as quickly as is practical with the latest and most up-to-date data available.

3. APPLICABILITY OF THE POLICY

3.1 This policy applies to the ICT Division

4. TERMS AND DEFINITIONS

	Term	Definition
	Disaster Recovery	Disaster recovery (DR) is the restoration of systems and infrastructure back to agreed service levels following a disaster. This may be temporary in the first instance, requiring full service restoration later.
	Risk Assessment	Risk Assessment: The overall process of risk analysis and risk evaluation.

5. ACRONYMS

COBIT	Control Objectives for Information Technology
ICT	Information and Communication Technology
ICTSC	Information and Communication Technology Steering Committee
ITIL	Information Technology Infrastructure Library

6. REFERENCES

6.1 International Guidelines

a. Control Objectives for Information Technology (COBIT)

6.2 International Standards

a. Information Technology Infrastructure Library (ITIL)

b. ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

c. ISO24762 (ISO 24762) Disaster Recovery Services

6.3 National Policy

a. Constitution of the Republic of South Africa, Act 108 of 1996

b. The Electronic Communications and Transactions (ECT) Act 25 of 2002

c. National Strategic Intelligence Act 2 of 2000 applicable for South Africa

d. Regulation of Interception of Communications Act 70 or 2002

e. State Information Technology Act 88 of 1998

7. POLICY STATEMENT

7.1 This policy is developed to guide the ICT Division in the recovery of data, information, computing and network services in the event that a disaster destroys all or part of municipality facility.

8. INFORMATION BACKUP

a. Backups shall be scheduled to run after working hours.

b. There shall be daily, weekly and monthly backups.

c. Backup copies shall be taken to the safe or storage area within the first hour of the business day of the morning after finished backup process.

d. Backup strategy or procedure shall specify the exact time on which the backup is scheduled to start running, and on when the backup copies shall be taken to the safe or storage area.

e. Backup procedures are documented in writing and updated on regular basis as changes are required.

f. There shall be a system administrator assigned to perform the system backups.

g. The system administrator shall inspect the backup log to verify the success of the backup and troubleshoot hardware and or software problem related to backup procedure

h. An electronic log of each backup performed will be created by the system administrator and mailed to ICT Manager monthly for monitoring.

i. Log files shall be analyzed and for any errors, corrective measures shall be taken every time before taking the backup tapes for safe storage.

j. Access to the backup copies in a safe or storage area shall be limited to the system administrators doing the backups.

k. Users shall be responsible for ensuring that all essential business information under their control is backed-up.

l. Monthly backup copies for staff personnel records will be retained for an indefinite time period (five years).

m. Adequate backup facilities should be in place to ensure proper functioning of backup process.

9. EXCLUSIONS

9.1 Restorations are not intended for the following purposes:

a. Personal data such as photos, videos, music and unofficial e-mail accounts.

b. Application programs not officially supported by ICT.

c. Exceptionally large images (scanned or digitized material) and large video files.

9.2 Any lost data not beyond the scope

10. ROLES AND RESPONSIBILITIES

10.1 ICT Division shall ensure essential business information is backed up at appropriate time intervals.

10.2 The system administrator shall ensure information is backed up as regularly as agreed.

10.3 In support of this policy, all the employees must support and comply with the controls that have been put in place by ICT Division.

10.4 Users shall be responsible for saving official files to the specified network shares.

11. Disaster Recovery Strategies

a. ICT shall ensure that every server running municipality applications is backed up regularly.

b. The turnaround time to receive a backup tape for recovery is maximum 2 hours.

c. The system administrator will initiate data recovery processes for the the data that has been destroyed by the disaster.

d. The restoration time will depend on the amount of data to be retrieved

e. A minimum level of backup information, together with accurate and complete records of the backup copies and documented restoration procedures, should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at main site.

f. Backup information should be given an appropriate level of physical and environmental protection, consistent with the standards applied at the main site.

g. Backup media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

h. Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the recovery time that has been allotted in the operational procedures for recovery.

12. INITIATION OF DATA RECOVERY PROCEDURES

12.1 Recovery Actions

a. Prepare a detailed assessment of extent of damage; in particular assess extent of damage to network or telecommunications infrastructure in the server room

b. Locate and validate relevant backup media if Information Systems are affected

c. Call external support contractors (if appropriate) and advise them of extent of damage

d. Assess likely duration of disruption to critical services and consider relocating essential users to an alternative site

e. Ascertain if there is serviceable computer equipment in critical service areas. Locate backup media and schedules

f. Update events log

g. Review initial assessment

h. Make decisions regarding recovery actions or implementation of manual procedures

i. Secure funding if necessary

k. Decide on personnel needed for next phase of recovery

k. Make initial announcement to municipality employees on affected systems

12.2 Full Recovery Actions

a. Continue installation of replacement equipment (if necessary) with assistance as necessary from external service providers

b. Restore from backup media

c. Check that critical areas can access the network and take remedial action as necessary

d. As systems become operational, the ICT division will consult with employees to confirm that systems are fully functional before users are granted access

e. Prepare and release further external statements if service to clients are affected

f. When recovery complete:

   a. prepare final report for senior management
   b. review actions taken and lessons learnt
   c. update plan

13. POLICY REVIEW

This policy shall be reviewed on an annual basis by the ICT Division to:

a. Determine if there have been changes in International, National or Internal references that may impact on this policy.

b. Determine if there are improvements or changes in the ICT process that should be reflected in this policy