elrc

EDUCATION LABOUR
RELATIONS COUNCIL

ICT System Disaster Recovery Plan & Business Continuity

elrc EDUCATION LABOUR RELATIONS COUNCIL	EDUCATION LABOUR RELATIONS COUNCIL	Doc No. IT/PC/004	
		Date: APRIL 2016	Rev 0
		Page: 2 of 11	
Title: ICT SYSTEMS DISASTER RECOVERY PLAN & BUSINESS CONTINUITY		Document type: POLICY	
This document has been seen and accepted by the following: EXECUTIVE COMMITTEE OF THE COUNCIL		COMPILED/ REVIEWED BY: DAKALO NEMAVHOINI IT MANAGER	
RECOMMENDED BY: OCTAVIA MOKOFANE SENIOR MANAGER: CS	APPROVED BY: NOLUSINDISO FOCA GENERAL SECRETARY	AUTHORISED BY: LUVUYO BONO CHAIRPERSON OF THE COUNCIL	
DATE OF LAST REVIEW: APRIL 2016			
DATE OF NEXT REVIEW: APRIL 2018 *NOTE: - This document may be changed before the stipulated period as and when a need arises as guided by the Documentation Policy.*			

FNO LB

TABLE OF CONTENTS

FNG
LB

1. DISASTER RECOVERY PLAN OVERVIEW

1.1 This Disaster recovery is an agreed Business strategy that indicates how quickly the ELRC Data Centre (or portions of the data centre) must be recovered from an outage and plans for the resources required in order to sustain the ELRC systems.

1.2 The processing in ELRC is centrally run from SACE Building. This implies that the data centre is critical to the running of the council and therefore very reliant on sound and dependable Business system and infrastructure environment.

1.3 Increasing dependence of computers and the data increases the importance of plans to safeguard their availability.

1.4 The Disaster recovery plan (DRP) is necessary to minimize the impact of any possible disruptions to ELRC' daily business processing capabilities in the council which users are approximately 60 staff members connected online, accessing various LAN-based applications locally and remotely and would be adversely affected by if the data centre for an extended period of time.

The objectives of DR plan are:

1.4.1 Limit the magnitude of loss;

1.4.2 Minimize the extent of the interruption and the severity disaster;

1.4.3 Determine and define the causes of events that could lead to a disaster;

1.4.4 Define alternatives for continuing critical services;

1.4.5 Establish advanced methods of recovery of operations;

1.4.6 Minimize decisions making during a crisis;

1.4.7 Rebuild the data processing facility if necessary;

1.4.8 Advice personnel of their responsibilities;

1.4.9 Facilitate the restart of essential operations after disaster.

1.4.10 Restore any application or provide a replacement within the period defined (48 hours)

1.4.11 The DR plan is dynamic on-going activity.

FNO LB

2. MANAGEMENT COMMITMENT

ELRC is committed to this DR plan and is aware that the absence of a sound plan places a high risks element on the Council Business and Infrastructure systems that are required to support the ICT department. Management is therefore committed to this plan. By approving this plan management demonstrate that:

- They are firmly committed to the need to have a sound DR process to cover business during disaster situation;
- There is a need to be able to recover to normal operations quickly after a disaster situation and that they support the proposed order of systems recovery and outage periods;
- Support the initial and periodic tests associated with DR plan and its associated cost;
- They understand that this DR plan requires periodic testing and updating in response to information derived from the tests and as the results of changing business organisation.

3. PURPOSE OF THIS DOCUMENT

3.1 The DRP is critical to ensuring that in the event of significant interruptions the council can effectively recover data and resources that enable operational processes. The DR policy establishes the framework for developing IT business continuity and disaster recovery plan. The purpose of this document is to assist with the execution of declared disaster recovery test. Copies of this document will be kept with the data backups

3.1.1 Declaring/invoking a Disaster

A 'Disaster' is an incident which has, or will disable, partially or completely, the central computing facilities, and/or data communications network for a period greater than 48 hours.

The following procedure should be followed to inform ELRC management and the staff of declaration or invocation of a disaster.

Declaration applies to a disaster and is a warning to inform the council that an invocation may be forthcoming in the near future, based on the damage and repair capability assessments underway. A declaration keeps its validity for 4 hours if not renewed it will lose its validity. A declaration can be refreshed not more than twice (maximum of 12 hours in total).

Invocation applies to the recovery of service or the configuration and the request access to Council fall back resources within 2 hours.

LB
FNO

3.2 ELRC recovery responsibilities

During a declared disaster the ELRC DR crisis management team will be responsible for all communication to, and coordination of, the customer community.

a) Inform them of the extent of disaster
b) Start and monitor ELRC disaster recovery procedure
c) Update the community on the status of the disaster
d) Have available users to test connectivity and data integrity
e) Inform users to continue processing.

3.3 Contact listing of key ELRC personnel (ICT Operational Committee)

Name	Telephone	Cell phone
ICT manager: corporate services	012 663 7556	060 546 7608
Senior manager: corporate services	012 663 7556	079 260 5722
Chief financial officer	012 663 7556	063 253 0507

3.4 The Recovery Team (ICT)

This team will ensure the successful recovery at the ELRC site for all services run from the central computing facilities.

a) Ensure the availability of all computer equipment necessary for fall back;
b) Reconstruct the data files that either has been lost through the disaster, or whose integrity or completeness have been affected.
c) Reconstruct data files for planned tests
d) Prepare application software for transfer
e) Plan and prepare the data processing production activities;
f) Execute the production activities and carry out output handling and distribution.

3.5 Scheduled backup & test days per annum

3.5.1 Backups are daily backups (incremental backup) to the storage server.

3.5.2 The test will be done on quarterly basis (Data Files) and full testing once in a year.

3.5.3 The number of test days scheduled for each platform is as follows:

Platform	Test Days
Financial & SCM Systems	1 x 4 days
Network systems	1 x 4 days

FNO LB

4. RESTORATION LEVEL

4.1 The backup data held at a defined offsite locations will generally be the level of data to be restored, however should more recent backup copies have been taken and these later backups are undamaged and accessible then these will be used to affect restoration.

4.2 Recovery will be made to the point of the latest available daily backup copy of the systems, database and application file.

4.2.1 Maintaining this disaster recovery plan

Pronto and ELRC shall ensure safe storage and distribution of the associated procedures as follows:

a) offsite safekeeping of the DR plan;
b) Pronto IT DR consultant;

4.2.2 Test results and any required corrective plans

After six-monthly disaster recovery test a report is produced with all relevant results of the test. Any actions arising from a test are documented in an action plan. The test report, along with any outstanding action plans, can be found in hard copy in the file entitled "ICT System Disaster Recovery Plan".

4.2.3 Location schedule of period and offsite backups

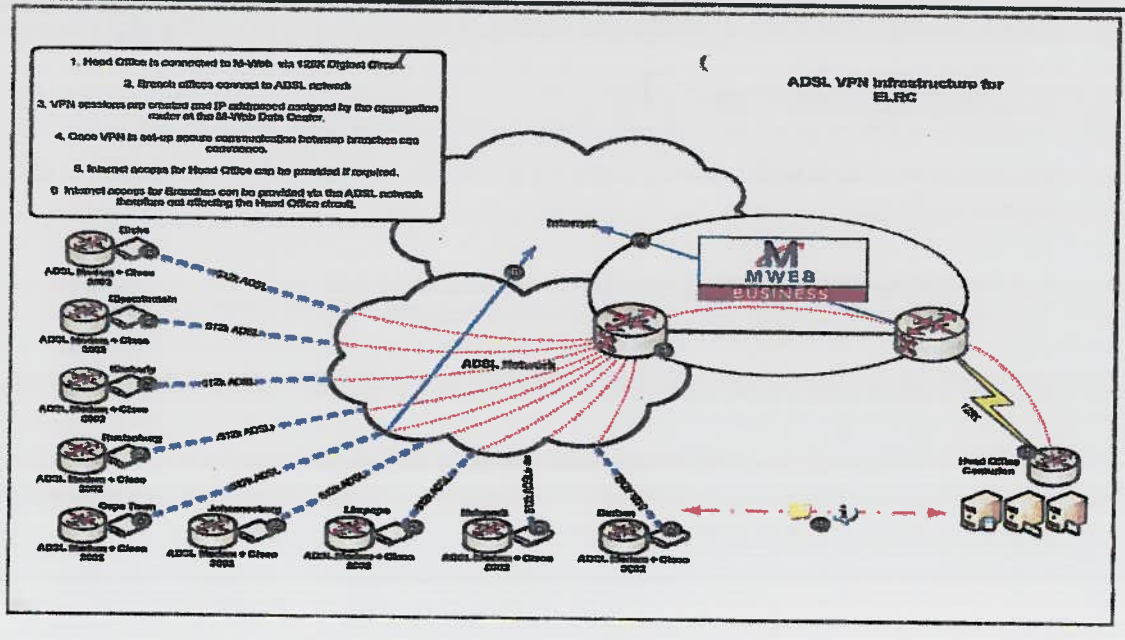
Periodic backups are stored in the datacentre in Samrand of Pronto Solutions

4.2.4 Maintaining printing during a Disaster

ELRC's printing requirements defined as follows:

a) Xerox 5755
b) Xerox 5562
c) Documents must be able to be saved on external media for offsite printing.

5. APPENDIX 1 ELRC NETWORK LAYOUT



LB
FNO

ELRC network Connectivity

ELRC network controls all the traffic between sites and give access to the internet. The sites connect directly with the ASDL and diginets lines to head office. A VPN connection is setup on the router to make this connections available. Mail and website are hosted by Mweb.

6. APPENDIX 2 – DISASTER RECOVERY HARDWARE & SOFTWARE IN THE EVENT OF DISASTER

Server Name	Configurations
Fijutsi Siemens Server host 1 - DC • EXCH2010 mail server, • Domain controller & DHCP-10.0.0.12 • Hyper-V	IP: 10.0.0.10 OS: windows server 2012 64 bit processor Virtual Machine
Server Name	**Configurations**
Fijutsi Siemens Server host 2 – File Server • Trend micro AV, - 10.0.0.19 • Pastel 2012 -10.0.0.18 • Payroll – 10.0.0.18 • File server – 10.0.0.16 • Attix5 Server- 10.0.0.20 • Hyper-V)	IP: 10.0.0.13 OS: windows server 2012 64 bit processor Virtual Machines

Network Equipment's

- 2 cisco routers
- 2 Telkom Diginet NTU's
- 1 x Rack UPS
- 1 x HP tape drive
- 23 FSC-entry level computers

7. APPENDIX 3 RECOVERY ACTIVITIES

7.1 Servers / Computers / Data

Ordering of replacement equipment. "The equipment and model will depend on the availability of stock". Reconfiguration of new equipment: servers, computers, etc.

7.2 Reconfiguration of the servers will be +/- 4 days

7.2.1 Install and configure MS Windows Server 2012 onto 4 Servers

7.2.2 Install and configure Veritas Backup Exec 9.0

7.2.3 Transfer of data from remote backup to Servers

7.2.4 Setup of MS Exchange 2013

FNO LB

7.2.5 Transfer mailboxes from remote backup to MS Exchange 2013.

7.2.6 Setup of Pastel Partner 2012

7.2.7 Setup of Payroll 2014

7.2.8 Transfer database from remote backup to Server.

7.2.9 Setup security, mappings and sharing on Server folders

7.2.10 Install MS ISA Proxy / Firewall

7.2.11 Configure / test of network and settings

7.3 Reconfiguration of the computers will be +/- 4 days

7.3.1 Install and configure MS Windows

7.3.2 Install and configure MS Office

7.3.3 Configure user profile to customer needs

7.4 MWEB routers- Telkom Line

7.4.1 MWEB will be able to supply new networking equipment and will reconfigure network to be fully operational before disaster.

7.4.2 MWEB will log a call with Telkom and manage the installation/relocation of the Diginet line for the ELRC network.

7.4.3 MWEB will be able to configure a wireless connection for connection purposes while the installation of the Diginet line takes its route with in Telkom.

7.5 Case Management System

Responsible Company
Public Service Coordinating Bargaining Council
260 Basden Avenue
Lyttleton
012 644 8100

7.5.1 PSCBC will need to reconfigure Cisco router for CMS to function correctly.

7.5.2 Telkom need to install Diginet line to be connected with PSCBC offices.

7.6 Offsite Backup

7.6.1 ELRC data is stored on Backup Exchange (Attix 5)

LB
FNO

7.6.2 Offsite storage on raid solution, AES 256 Bit Encryption, 550GB offsite

7.6.3 Data is also stored in two (2) data centres offsite

8. INDIVIDUAL AUTHORISED TO INVOKE/DECLARE A DISASTER (ICT STEERING COMMITTEE)

Name	Telephone	Cell number
GS	012 663 7556	083 555 0917
CFO	012 663 7556	063 253 0507
Senior manager: CS	012 663 7556	079 260 5722
Senior Manager: IA	012 663 7556	082 411 2034
ICT manager	012 663 7556	060 546 7608

9. GOVERNMENT EMERGENCY TELEPHONE NUMBER

City of Tshwane Emergency number (012) 310 6400

10. TERMINOLOGY

10.1 Fallback: The 'fallback phase' is the period during which business operations are transferred to the facility contracted for this purpose.

10.2 Repair phase: The 'repair phase' is the period during which business operations are repaired and continued at the production facility.

10.3 Backup: The process of taking copies of the operating systems and application data at regular intervals, such that the maximum loss of data should never be more than twenty four hours.

10.4 Off-site storage location: An 'offsite storage location' is any off-site place fallback electronic data and/or supplies required by business operation are stored.

10.5 Outage: any period of time (within defined service hours) when the data processing service is not available to users

10.6 Infrastructure: in conjunction with ICT, the term refers to peripheral facilities required by medium computer environments. It includes, for instance air conditioning, water cooling, electrical power, access to communication networks and raised floors.

10.7 Disaster Recovery Mode: The mode of operation employed during the actual recovery. This operation may be characterised by limited service to users and the availability of selected applications only.

FNO LB

10.8 Service level agreement: The contract between two parties, which describes the scope of services, performance and infrastructure.

10.9 Damage assessment phase: is the period after a disaster during which team of technical experts along with trained emergency staff will assess the damage in order to determine whether repair or fallback is necessary.

LB
FNO