Backup Policy
Recovery and Procedure

<table>
<tr><td rowspan="3">  </td><td rowspan="3">EDUCATION LABOUR RELATIONS COUNCIL</td><td colspan="2">Doc No. IT/PC/009</td></tr>
<tr><td>Date: APRIL 2016</td><td>Rev 0</td></tr>
<tr><td colspan="2">Page: 2 of 11</td></tr>
<tr><td colspan="2">Title: BACKUP POLICY AND RECOVERY</td><td>Document type: POLICY</td></tr>
<tr><td colspan="2">This document has been seen and accepted by the following:
EXECUTIVE COMMITTEE OF THE COUNCIL</td><td>COMPILED/ REVIEWED BY:

DAKALO NEMAVHOINI
IT MANAGER</td></tr>
<tr><td>RECOMMENDED BY:

OCTAVIA MOKOFANE
SENIOR MANAGER: CS</td><td>APPROVED BY:

NOLUSINDISO FOCA
GENERAL SECRETARY</td><td>AUTHORISED BY:

LUVUYO BONO
CHAIRPERSON OF THE COUNCIL</td></tr>
<tr><td colspan="3">DATE OF LAST REVIEW: APRIL 2016</td></tr>
<tr><td colspan="3">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.</td></tr>
</table>

TABLE OF CONTENTS

1. BACKUP POLICY OVERVIEW

1.1 Computer information systems and electronic data are valuable assets to the Education Labour Relation Council (ELRC) and a substantial investment in human and financial resources has been made to create these systems and information and, as such, a formalised policy has been implemented to:

- Safeguard the risk of losing data.
- Safeguard the confidentiality and integrity of information contained within these systems.
- Ensure availability of critical data so that information can be utilised as the valuable asset that it is.
- Reduce business and legal risk.

1.2 Processing in the ELRC is centrally run from the server room. This implies that the data centre is critical to the running of the Council and therefore very reliant on sound and dependable business systems and infrastructure.

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

1.3 The Council's critical data is stored on the File-server, Exchange-servers (mail-box data) and Application-servers. This data can be categorised as: user personal data, business unit data, shared data, application/ system data and Database.

1.4 The Backup policy is necessary to minimise the impact of any possible disruptions to the ELRC's daily business processing capabilities. The Council has approximately 60 staff members connected online, accessing various LAN-based applications locally and remotely and operations would be adversely affected if the data centre had a downtime for an extended period of time.

The objectives of Backup policy are:

1.4.1 To limit the magnitude of loss;

1.4.2 To minimise the extent of the interruption and the severity of disaster;

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

1.4.4 To define alternatives for continuing critical services;

1.4.5 To establish advanced methods of recovery of operations;

1.4.6 To minimise decision making during a crisis;

1.4.7 To rebuild the data processing facility if necessary;

1.4.8 To advice personnel of their responsibilities;

1.4.9 To facilitate the restart of essential operations after a disaster;

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

1.4.11 To ensure that the backup plan is dynamic and an on-going activity.

2. MANAGEMENT COMMITMENT

The ELRC is committed to implementing this Backup policy and is aware that the absence of such a policy places a high risk element on the Council's Business and Infrastructure systems that are required to support the ICT unit. Management is therefore committed to this policy. By approving this Backup Policy, management demonstrate that:

- They are firmly committed to the need to have a sound Backup process to cover business operations during a disaster;
- 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;
- They support the initial and periodic tests associated with data backup and its associated cost;
- They understand that this data backup requires periodic testing and updating in response to information derived from the tests.

3. PURPOSE OF THIS DOCUMENT

3.1 The Backup Policy is critical to ensure that in the event of significant interruptions the Council can effectively recover data and resources that enable operational processes. The policy establishes the framework for developing an 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.

The purpose of the policy is to provide continuity, restoration and recovery of critical data and systems. The IT unit needs to ensure that critical data is backed up periodically and copies are maintained at an off-site storage location

Ownerships of all electronic information residing in any Council computer vests in the ELRC and the Executive Committee. All requests to restore employee data where the data has been deleted or lost, should be directed to the ICT unit.

3.1.1 Backup and Restore Procedure

Backup is the process of copying active files from an online disk to tape or save so that files may be restored to a disk in the event of equipment failure, damage to or loss of data.

Restore - The process of bringing offline storage data back from the offline media and putting it on an online storage system, such as a file server.

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

3.2 Data Backed up

The Council is currently using Commvault backup system to automatically backup data and replicate them to an offside cloud.

System backup includes

a) ELRC file server – IP 10.0.0.16
b) Exchange Server – IP 10.0.0.10
c) Application Server (Pastel Evolution & VIP) - IP 10.0.0.22
d) User personal data
e) Provincial users' computers

3.3 Backup Schedule

- ICT with Pronto IT solution (SP) runs the incremental backup Monday to Thursday and full backup on Friday to ensure the safety of data using Commvault backup system that mirrors to an offsite cloud data centre.
- ELRCFILE, Evolution and Payroll SQL database runs the incremental backup during the day and full backup at night.
- Backups run twice a day at 12:00 and also at 19:00.
- Retention cloud protect data replication is three years
- The Commvault backup system sends a daily report to the IT Manager on backup performed during the day and at night.
- Backup for provincial chambers starts at 15:00.
- To backup - select files to backup, open Commvault system go to the list of servers, choose the server you want to backup, right click the default then properties and select the content and choose file to backup.
- All backups are automated to the local storage and then replicated to the cloud protect data centre.

3.4 Backup Exclusions

The below extension will be excluded from backup on the file server unless the request has been made on official related files.

- ✓ Mpeg
- ✓ Mpa
- ✓ Mp2
- ✓ Mp3
- ✓ Mp3
- ✓ Mp4
- ✓ Wav
- ✓ Wsf
- ✓ Mwa

3.5 Scheduled backup and test days per annum

3.5.1 Backups are incremental and full backups to the storage server and then replicated to the cloud.

3.5.2 The DR test will be done on a quarterly basis (Data Files) and financial systems.

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

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

4. RESTORATION LEVEL

4.1 The backup data held at a defined offsite location 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.

4.3 **Instructions**

To restore data from the file server

- Log into elrcfile server 10.0.0.16/ Commvault backup server 10.0.0.20
- Open the Commvault backup system
- Put in the login details
- Click on the listed server you want to restore from
- Right click and go to browse and restore
- Click on restore
- Select the date and file you want to restore

4.4 Maintaining Disaster Recovery Plan

Pronto and the 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;
c) JHB provincial chambers identified as DR centre.

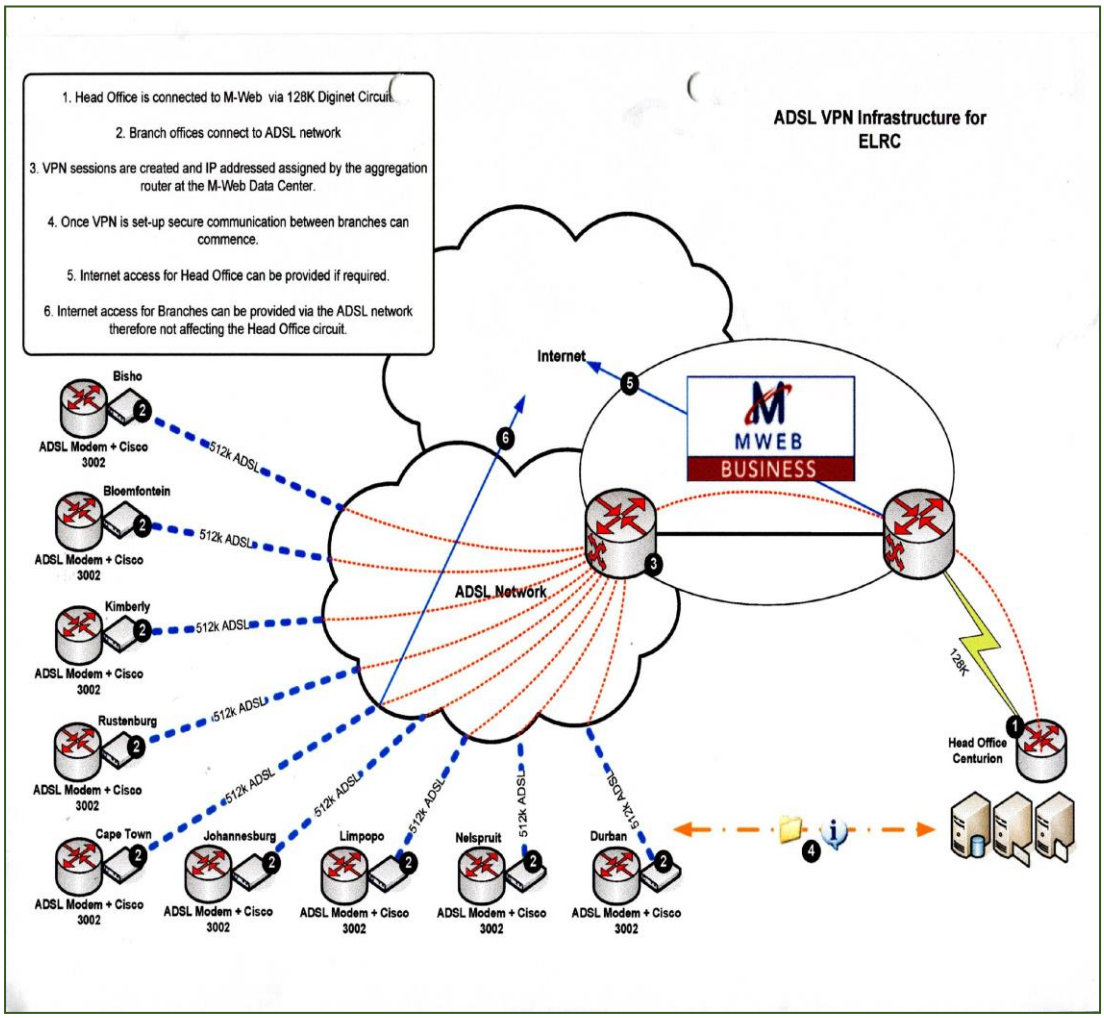
4.5 Test results and any required corrective plans

After six-monthly disaster recovery testing, 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”.

4.6 Location schedule of period and offsite backups

Periodic backups are stored in the datacentre in Samrand at Pronto Solutions.

5. APPENDIX 1 ELRC NETWORK LAYOUT



ELRC network Connectivity

The ELRC network controls all the traffic between sites and gives 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 these connections available. Mail and the ELRC website are hosted by Mweb.

6. APPENDIX 2 – DISASTER RECOVERY HARDWARE AND 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

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 Attix5 backup system

7.2.3 Transfer of data from remote backup to Servers

7.2.4 Setup of MS Exchange 2010

7.2.5 Transfer mailboxes from remote backup to MS Exchange 2013.

7.2.6 Setup of Pastel Partner/ Evolution

7.2.7 Setup of Payroll/ VIP

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 in a cloud protected data centre.

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

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

8. INDIVIDUALS 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 24 hours.

10.4 **Offsite storage location:** An ‘offsite storage location’ is any off-site place where fallback electronic data and/or supplies required for business operations, 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.

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 a team of technical experts along with trained emergency staff, will assess the damage in order to determine whether repair or fallback is necessary.

11. POLICY REVIEW

The policy shall be reviewed annually or as and when the need arises, with the permission of the General Secretary.