MANGAUNG
AT THE HEART OF IT ALL

CENTLEC
Reg No. 2003/011612/30

Information and Technology Business Continuity Plan

DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: INFORMATION AND TECHNOLOGY BUSINESS CONTINUITY PLAN	POLICY NO:
REV NO:	REV DATE : 31 MAY 2023
SUB-DIRECTORATE:	BOARD ITEM NO:
SIGNATURE :	
DATE APPROVED:	EFFECTIVE DATE:

1. INTRODUCTION

CENTLEC dependent on information and information technology to operate and continue its business effectively and efficiently. It is thus important to have an information communication technology (ICT) business continuity plan (BCP) to ensure business continuity in the event of a disaster. This document describes the operations and process of CENTLEC ICT systems and the necessary actions required to ensure that the CENTLEC are able to resume normal business functions in the event of a disaster. CENTLEC's information and communication technology sub-directorate focuses on ensuring that ICT systems are working in order as per the overall Business Continuity Plan (BCP).

2. PURPOSE

Business continuity plan is design to help organizations recover from a disruption in service. Specifically, this plan provides policy and guidance to ensure that the CENTLEC ICT can respond effectively to a disruption and restore essential services to the public and employees as quickly as possible.

3. OBJECTIVE

The objectives of this business continuity plan are to:

3.1 Identify advanced arrangements and procedures that will enable the agency to respond quickly to an emergency event and ensure continuous performance of critical business functions.

3.2 Reduce employee injury or loss of life and minimize damage and losses.

3.3 Protect essential facilities, equipment, vital records, and other assets.

3.4 Reduce and mitigate disruptions to business operations.

3.5 Identify managers and other staff who might need to be relocated depending upon the emergency.

3.6 Identify teams, which would need to respond to a crisis and describe specific responsibilities.

3.7 Facilitate effective decision-making to ensure that agency operations are restored in a timely manner.

3.8 Provide support to employees and employee families during an event so that employees know that the safety of their families has been addressed, and that employees will therefore be available to work and help restore agency function.

3.9 Identify alternative courses of action to minimize and/or mitigate the effects of the crisis and shorten the agency response time.

3.10 Quantify the impact of any kind of emergency in terms of money, time, services, and work force.

3.11 Recover quickly from an emergency and resume full service to the public timely

4. ABBREVIATIONS

4.1	BCP	-	Business continuity plan
4.2	ICT DRP	-	disaster recovery plan
4.3	ICTDRT	-	ICT Disaster Recovery Team
4.4	ICT	-	Information Communication Technology
4.5	LAN	-	local area network
4.6	SLA	-	service level agreement
4.7	WAN	-	wide area network
4.8	PC	-	Personal computer
4.9	Disaster	-	A likely hood that an event or risk may occur

5. RELATED DOCUMENTS

This policy is relate to disaster recovery plan, incident procedure that deals with incident plan, backup procedure and change control procedure and may be useful in the event of an emergency.

6. SCOPE

The CENTLEC BCP takes all of the following areas into considerations:

6.1 Business impact analysis for systems failures

6.2 Which service provers are affected?

6.3 Which are the most critical systems affected for business continuity?

6.4 Which Backup systems to restore from in order for business continue its operations?

7. OBJECTIVE

The objectives of this business continuity plan are to:

7.1. Identify advanced arrangements and procedures that will enable the agency to respond quickly to an event and ensure continuous performance of critical business functions.

7.2. Reduce and mitigate disruptions to business operations.

7.3. Identify users and service provider who might need to be rerouted for connection depending upon the emergency.

7.4. Identify systems and services provider who might assist in service restoration.

7.5. Identify teams, which would need to respond to a crisis and describe specific responsibilities.

7.6. Identify alternative courses of action to minimize and/or mitigate the effects of the crisis and shorten the agency response time such as alternative working methods as stated in disaster recovery plan and procedure.

7.7. Recover quickly from an incident and resume full service to the public and internally in a timely manner.

8. BUSINESS IMPACT ANALYSIS DISRUPTION

There are three main scenarios that are addressed with this BCP namely for impact analysis;

8.1 Loss of data due to natural disaster or human triggered disaster

8.2 Loss of data due to disgruntled employee or resigned employee

8.3 Loss of data due to hardware failure or loss

8.4 Loss of Hardware failure or crash

Table 1: Threats Analysis

Possible Threats	**Vulnerability**				**Likelihood**				**Severity Level**
Elements	H	M	L	N/A	H	M	L	N/A	
Earthquake		√					√		**3**
Tornado / heavy winds			√				√		**2**
Flooding	√					√			**4**
Fire	√					√			**4**
Explosion	√					√			**4**
Water pipe break	√					√			**4**
Severe thunderstorm	√				√				**5**
Hazardous material			√				√		**3**
Hail damage		√				√			**3**
Lightning	√				√				**5**
Drought		√				√			**3**

People	**H**	**M**	**L**	**N/A**	**H**	**M**	**L**	**N/A**	
Civil unrest	√				√				**5**
Industrial action / strikes	√				√				**5**
Denial of access	√				√				**5**
Computer crime	√					√			**4**
Industrial sabotage		√				√			**4**
Bomb threat / blast		√				√			**4**
Transportation accident	√				√				**5**

Unauthorised access	√					√			**4**
Individuals undocumented knowledge	√				√				**5**

Technology	**H**	**M**	**L**	**N/A**	**H**	**M**	**L**	**N/A**	
Telecommunications failure									
Telephone line failure	√					√			**4**
Network failure	√					√			**4**
Power shortage / failure	√				√				**5**
UPS failure	√				√				**5**
Computer hardware failure									
Workstation failure		√				√			**3**
Server failure	√					√			**5**
Printer failure		√				√			**3**
Computer software failure									
Upgrade compatibility	√					√			**4**
Over customisation	√					√			**4**
Unlicensed software		√				√			**3**
E-mail retention and deletion		√				√			**4**
E-mail content		√				√			**4**
Document loss or destruction									
Legal documents	√					√			**4**
Employee records	√					√			**4**
Service level agreements	√					√			**3**
Data backups & restores	√				√				**5**
Hacking		√				√			**4**
Air-conditioning failure	√					√			**4**
Computer virus attack	√					√			**4**

8.1.1 **Loss of CENTLEC premises/facilities:**

CENTLEC ICT is in the process of establishing an off-site cold disaster recovery site. In the above instance, the worst-case scenario, the main WAN connectivity will be switched to the cold DR site. This would allow primary systems to be functional as soon as they have been recovered.

8.1.2 **Loss of people in the ICT Team:**

In the above instance, full processes and procedures will be developed allowing any suitably qualified person with technical skills and knowledge to be in a position to support the infrastructure in place in the CENTLEC or at the **future recovery premises.**

8.1.3 **Loss of systems:**

Depending on the severity of the system failure, primary servers should be virtualized as well as replicated. This will enable redundancy in terms of CENTLEC business systems within two minutes of failure. This is a dynamic process.

8.1.4 **Loss of hardware:**

Depending on the severity of the hardware failure, primary servers should be virtualized or imaged for physical servers as well as replicated. This will enable redundancy in terms of CENTLEC business systems within two minutes of failure. This is a dynamic process.

9. BUSINESS CONITUINITY IN RECOVERY TIME

The systems recovery time to start and maintain operations is vital to the financial need of CENTLEC.

The activation of the recovery time for business continuity will be followed as per disaster and recovery plan (DRP) in order to activate the services for continuity. In the process, it follow the incident management procedure.

10. BUSINESS CONTUNITY TEAMS & RESPONSIBILITIES

At the time of the disaster, an emergency notifications and alert should be triggered or escalated to relevant personnel or external contractors responsible for the systems or application for disaster recovery plan team (BRP) and business continuity plan (BCP) teams.

This notification can be in the form of email alert or any form of communication.

Business Continuity Teams

This team will receive immediate notification and make decisions related to the business continuity efforts. They will lead the continuity process and provide direction to technical teams to direct the services for business continuity.

Table 1: Business continuity team

Leads Name	Designation	Phone Number	E-mail
Daniel Malokase	IT Manager	051 412 2634	Daniel.malokase@centlec.co.za
Sefale Mokoena	Executive Manager	051 412 2729	Sefale.mokoena@centlec.co.za

Other Business Continuity Team

This team will perform the tasks as identified and outlined in the incident management plan, disaster and recovery plan.

11.1.1 Technical teams to activate the systems as per incident management procedure for business continuity.

11.1.2 Communication teams to communicate the even for business continuity as per disaster and recovery plan and incident management procedure.

11.1.3 Facility team to prepare necessary tools for the sites to active the business continuity as per disaster and recovery plan and incident management plan.

11.2 PLAN ACTIVATION

The activation provide the guidance for business continuity and processes Warning Conditions

11.2.1 **With warning:**

It is expected that in some cases, the first line team will receive a warning related to an event as stated in the incident management plan.

11.2.2 **Identification of potential disaster status**

Criteria for determining whether a particular emergency requires that emergency actions be taken and alternative site to be determined.

9 TESTING

CENTLEC is committed to ensuring that this BCP is ready. The BCP should be tested every week in order to ensure that it is still effective. Testing the plan will be carried out as follows:

13.1 **Walkthroughs** **-** This test provides the opportunity to review a plan with a larger subset or people, allowing the BCP project.

13.2 **Simulations** **-** Use disaster recovery plan together with the required resources to switch off the main site temporarily to continue on the disaster recovery site.

13.3 **Full-Interruption Testing-** if the test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due

diligence with respect to previous DRP phases cannot be overstated.

10 DR SITE NECESSITIES

Items available at the Disaster Recovery Site for Business Continuity

The following items need to be ready for use at each of the DR sites for Business Continuity

14.1 PCs, Printers, LAN connectivity, Servers, other computer hardware, etc.

14.2 Telephones, Photocopiers, etc.

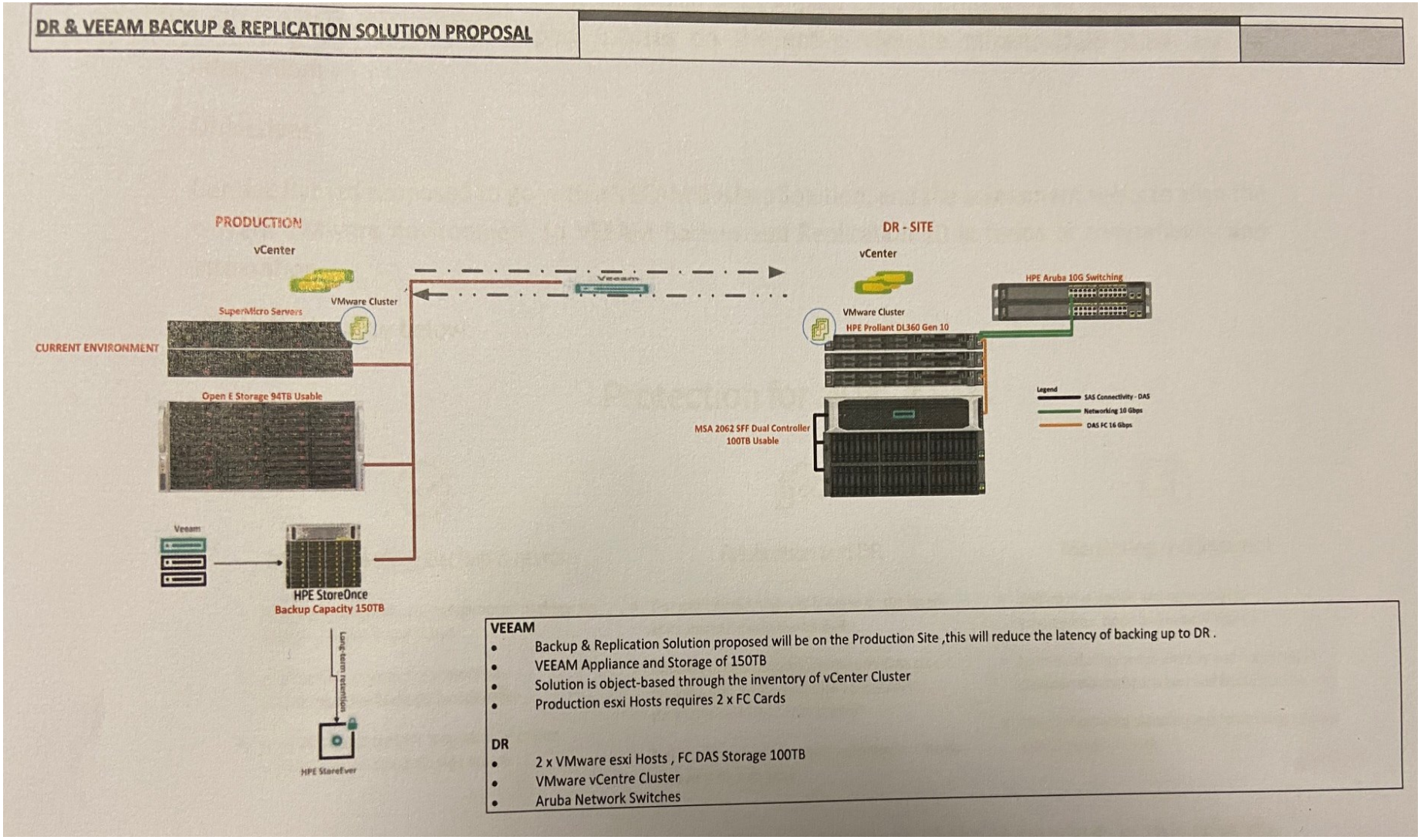
14.3 Power points, standby power, air-conditioning

14.4 Heat detectors

14.5 Fire suppressors

14.6 Batteries and UPS

11 BUSINESS CONTINUITY NETWORK TOPOLOGY



12 REVIEW AND APPROVAL

This Plan and underlying strategies will be reviewed at least annually, or as necessary, to ensure its continued application and relevance.

Prepared by:

Signed:_____

Act Executive Manager: Engineering Retail

Date:_____

Supported by:

Signed:_____

Chief Executive Officer

Date:_____

Approved by:

Signed:_____

Chairperson of the IT Governance Committee

Date:_____