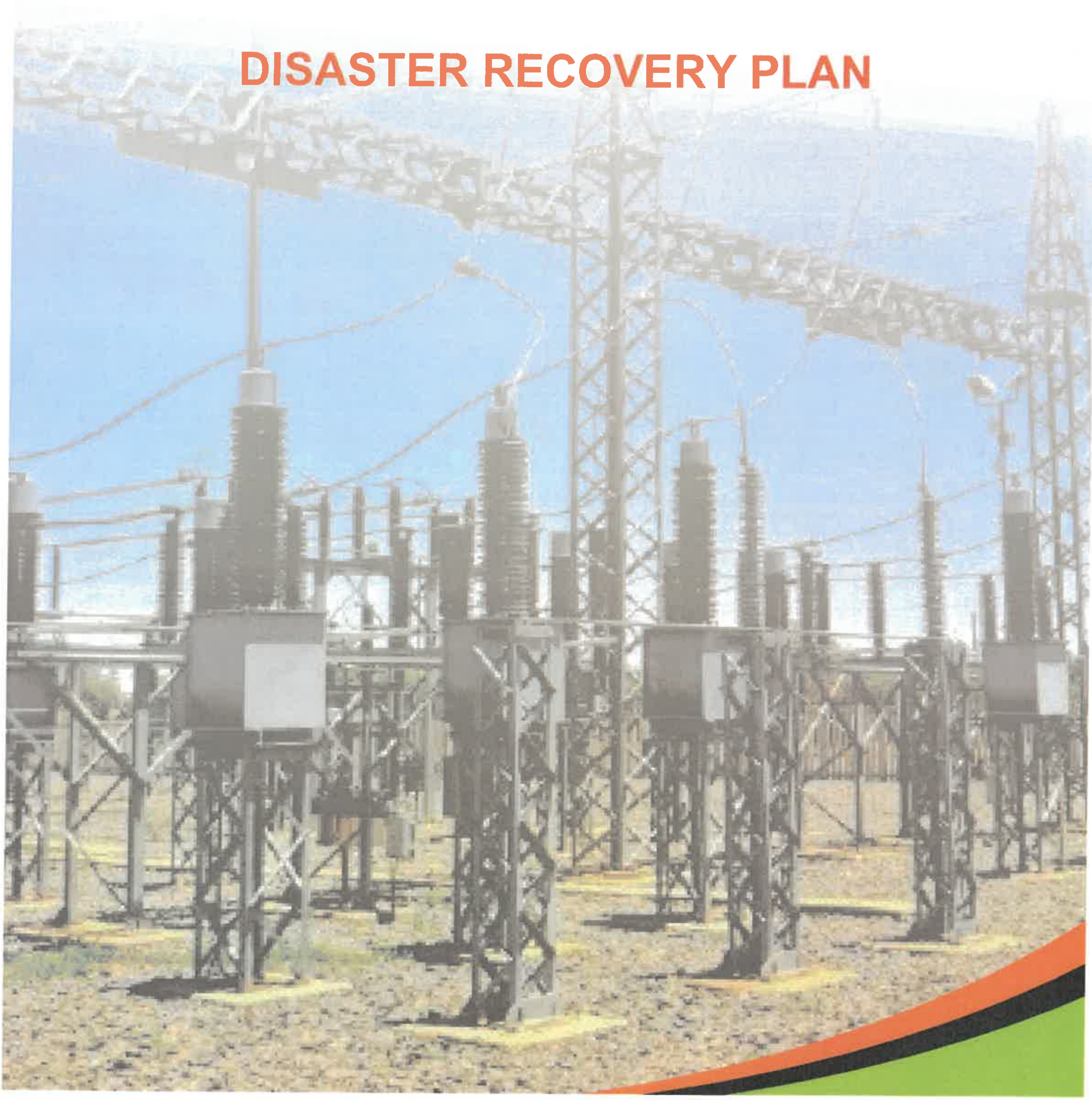
MANGAUNG
AT THE HEART OF IT ALL

CENTLEC
Reg No. 2003/011612/30

DISASTER RECOVERY PLAN



CENTLEC

DIRECTORATE: OFFICE OF THE CEO	
SUBJECT: DISASTER RECOVERY PLAN	POLICY NO:
REV NO: 1	REV DATE: 10 May 2023
SUB-DIRECTORATE: Information Management	BOARD ITEM NO:
SIGNATURE:	
DATE APPROVED:	EFFECTIVE DATE: 01 July 2023

1. INTRODUCTION

CENTLEC dependent on information and information technology to execute its business effectively and efficiently. As a result, information became just as valuable an asset to CENTLEC as all the other physical assets and intellectual property owned and produced by CENTLEC. Most operations are time-dependent and even a short period of missed production can affect CENTLEC in certain areas.

It is thus important to have an Information Communication Technology (ICT) Disaster Recovery Plan to ensure business continuity in the event of a disaster. This document describes the nature and location 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. The CENTLEC's Information Communication Technology Sub-directorate focuses on ensuring that the vital ICT components are restored to working order as per the overall Business Continuity Plan (BCP). It is therefore the CENTLEC's overall Business Continuity Plan (BCP) to migrate towards being compliant with industry best practices, international standards, corporate governance and regulatory requirements.

This document forms the base for recovering all the CENTLEC's business essential applications and services in the event of a disaster.

2. ABBREVIATIONS

2.1	**DR**	-	disaster recovery
2.2	**ICT DRP**	-	disaster recovery plan
2.3	**ICTDRT**	-	ICT Disaster Recovery Team
2.4	**ICT**	-	Information Communication Technology
2.5	**LAN**	-	local area network
2.6	**SLA**	-	service level agreement
2.7	**WAN**	-	wide area network
2.8	**PC**	-	Personal computer
2.9	**Disaster**	-	A likely hood that an event or risk may occur

3. RELATED DOCUMENTS

This policy is relate to standard operational procedure that deals with Incident Plan, Backup Procedure and Change control procedure and may be useful in the event of an emergency.

4. DEFINITIONS

Disaster - ICT disaster recovery is the process for recovering systems following a major disruption. The likelihood of a major disaster or significant disruption is generally low, often remote but the consequences of a system failure that cannot be restored could be significant or even catastrophic.

Disaster recovery - Disaster recovery is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions

Business Continuity Plan - business continuity plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in service. Plans may provide detailed strategies on how business operations can be maintained for both short-term and long-term outages.

Hardware - is the most visible part of any information system: the equipment such as computers, scanners and printers that is used to capture data, transform it and present it to the user as output.

Service Level Agreement - Service Level Agreement (or SLA) is the part of a contract which defines exactly what services a service provider will provide and the required level or standard for those services.

Backups - To make a copy of the data held on the system in case the original data is lost or damaged. Backups can be made onto removable media such as CDs, magnetic tape, removable hard disks and then stored away from the PC. The original data files could then be restored.

Windows integrated security authentication - (often referred to as Windows authentication) is the easiest security mechanism to implement. The basic vision is beautiful in its simplicity: if the user has already logged on to Windows, the browser can silently pass the user's credentials to ASP.NET.

5. PURPOSE

This plan is to assist in recovering the business critical systems/operations that were identified in the business impact analysis in case of a disaster.

The identified ICT systems represent the most critical systems identified to the business, as without them, business cannot continue. This would result in a major impact on CENTLEC if a disaster occurs.

6. SCOPE

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

6.1 Network infrastructure

6.2 Server infrastructure

6.3 Telephone system

6.4 Backup systems

6.5 End-User computers

6.6 Database systems

6.7 Application systems

6.8 Website

6.9 Document management system

7. EXPECTATIONS

The following assumptions have been made in compiling this plan.

All data, systems and applications have been backed up and need to be stored initially internal and eventually externally to the ICT offices.

A worst-case scenario disaster being experienced at the CENTLEC is assumed in the planning process but not initially catered for.

Key CENTLEC ICT critical systems personnel shall be trained in their emergency response and recovery roles and they are available to activate the CENTLEC critical systems ICT DRP. Preventative controls (e.g. generators, environmental controls, waterproof tarps, sprinkler system, fire extinguishers etc.) shall be installed and will be fully operational as the finances become available to supply these. An "Enviro-rack" solution has already been installed at the first identified DR site. Data centre equipment, including components supporting the CENTLEC-critical systems, are connected to a UPS that provides 4Hrs of electricity during a power failure. Service level agreements are maintained with service providers for systems hardware, software and communication providers to support the CENTLEC systems. All production data will be restorable at an alternative site via replication of data to and from the different DR sites. This DR approach applies to CENTLEC server hardware and software and therefore excludes items such as the WAN, PCs, and transversal systems.

Disaster Recovery situations may result in degraded performance of certain services.

A complete copy of this DR Plan is available in the Recovery Kit. This copy of the ICT DRP shall become the default copy for use in the event of a disaster.

CENTLEC General Manager / Executive: ICT coordinates the maintenance of the ICT DRP as contained in the Recovery Kit.

8. THREATS IMPACT ANALYSIS

Table 1: Threats

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**

Possible Threats	Vulnerability				Likelihood				Severity Level
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**

9. BUSINESS IMPACT ANALYSIS

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

1. Loss of premises/facilities;
2. Loss of people; and
3. Loss of systems
4. Loss of Hardware

9.1 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.

9.2 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.

9.3 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.

9.4 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.

10. DISASTER RECOVERY TIME

The recovery time to start and maintain operations is vital to the financial need of CENTLEC. The following recovery point time of objectives in the event of the disaster. These times are defined as the following in tears based on the criticality:

Table 2 – recovery time

Disaster recovery Categories	Recovery Time
Infrastructure Services	0-8 Hours
Critical applications - Tier One	8-24 hours
Business essential operations - Tier Two	48-72 hours

Infrastructure down time

This are the services including the hardware such as switches, servers, and network connectivity.

This technology is very essential for the organization for communication and operations.

1. Recovery time : 0-8 Hours
2. Equipment strategy : equipment spares on site for immediate technology requirements or faster delivery procurement

Table 3- servers down time

Services	Description
Company Servers	VMware for all the Servers
Company network	Switches in all the department
Company network	Firewalls in the server rooms
Company network	Microwaves and Cables for APN

Critical Applications down time

This are the services including the software's such as financial software, Human resource software and historian software.

These applications are very essential for the organization for user access and operations.

1. Recovery time : 8-24 Hours
2. Software strategy : regular check-up on the licensing expiry dates.

Table 4- critical application down time

Services	Description
Exchange mails	Communication operations for internal and external
Internet	Operational connectivity through APN
Financial	SCOA for Financial transaction
Human resource	PAY day for Leaves and payroll
Vending	Prepaid electricity purchase
Telemetry	Scada systems for switching
Active Directory	Authentications

Business essential operation services down time

These are the services including the communications such as telephones, digital radios and Websites

These applications are very essential for the organization for user access and operations.

1. Recovery time : 48-72 Hours
2. Software strategy : regular check-up on the licensing expiry dates

Table 5 :business essential down time

Services	Description
Website	Communication operations
Telephone system	Communication operations
Digital Radio	Communication operations
Service Desk	Communication operations
Call Centre	Communication operations

Services recovery points and priorities

Following is the priority sequence in which systems need to be recovered.

Table 6: Priority 1 Server Sequence

Priority	System/Application	Server Name	Service Provider	Contact
1	Active Directory	Domain Controller	CENTLEC	051 412 2634
1	Exchange Server	Mail Exchange	CENTLEC	051 412 2634
1	Firewall	Firewall	CENTLEC	051 412 2634
1	Solar Systems	Financial Systems	CENTLEC	051 412 2634
1	Vending Systems	Powernet Systems	CENTLEC	051 412 2634
1	Scada	Sacada	CENTLEC	051 412 2634
1	Mimic	Mimic	CENTLEC	051 412 2634
1	Pay Day	Payday	CENTLEC	051 412 2634
1	ESS	ESS	CENTLEC	051 412 2634
1	Website	Webserver	CENTLEC	051 412 2634
1	Intranet Server	Webserver	CENTLEC	051 412 2634

Table 7: Priority Server Network

Priority				
2	Vol 1	File Server	CENTLEC	051 412 2634
2	Vol2	File Server	CENTLEC	051 412 2634

Table 8: Server Start Sequence

Priority				
1	VMware 1	Host Server	CENTLEC	051 412 2634
2	VMware 2	Host Server	CENTLEC	051 412 2634
3	VMware 3	Host Server	CENTLEC	051 412 2634
4	Active Directory	Mail Exchange	CENTLEC	051 412 2634

5	Exchange Server	Firewall	CENTLEC	051 412 2634
6	Solar Systems	Financial Systems	CENTLEC	051 412 2634
7	Vending Systems	Powernet Systems	CENTLEC	051 412 2634

With above sequence it must be noted that many of the recoveries can be done simultaneously.

11. DISASTER RECOVERY 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. This notification can be in the form of email alert or any form of communication. The person responsible for Backups and Business Continuity should engage responsible person. The relevant ICT service providers' SLA's should provide for the replacement of ICT skills when CENTLEC ICT employees are not available. The ICT section should ensure that skills are evenly spread in the unit.

Usually systems fail due to hardware, software, configuration and/or network failures. These are addressed by the CENTLEC IT support staff, and falls more within problem management procedures.

The CENTLEC ICT currently makes use of the Veem solution to back up systems and data. Business critical systems have been identified, and arrangements are being implemented to replicate all backups made to the secondary DR sites as offsite backup. Critical hardware systems must be placed under next-day-on-site warrantee for 5 years.

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employee of CENTLEC. The different teams and their responsibilities are as follows:

1. Disaster Recovery Lead(s)
2. Disaster Management team
3. Facilities and Environmental team
4. Network team
5. Server teams
6. Applications team

7. Telephone teams
8. Communication network team

11.1 Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at CENTLEC, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in CENTLEC.

Role and Responsibilities

1. Make the determination that a disaster has occurred and trigger the DRP and related processes.
2. Initiate the DR Call Tree.
3. Be the single point of contact for and oversee all of the DR Teams.
4. Organize and chair regular meetings of the DR Team leads throughout the disaster.
5. Present to the Management Team on the state of the disaster and the decisions that need to be made.
6. Organize, supervise and manage all DRP test and author all DRP updates.

Table 1 : Disaster recovery leads

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

11.2 Disaster Management Team

The Disaster Management Team that will oversee the entire disaster recovery process. They will be the first team that will need to take action in the event of a disaster. This team will evaluate the disaster and will determine what steps need to be taken to get the organization back to business as usual.

Role & Responsibilities

1. Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
2. Determine the magnitude and class of the disaster
3. Determine what systems and processes have been affected by the disaster
4. Communicate the disaster to the other disaster recovery teams
5. Determine what first steps need to be taken by the disaster recovery teams
6. Keep the disaster recovery teams on track with pre-determined expectations and goals
7. Ensure that all decisions made abide by the DRP and policies set by CENTLEC
8. Get the secondary site ready to restore business operations
9. Ensure that the secondary site is fully functional and secure
10. Create a detailed report of all the steps undertaken in the disaster recovery process
11. Notify the relevant parties once the disaster is over and normal business functionality has been restored
12. After CENTLEC is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Table 2 : Disaster management team

Leads Name	**Designation**	**Phone Number**	**E-mail**
Nico Moeketsi	Manager OHS	051 412 2499	Nicolas.Radebe@centlec.co.za
Hlomlani Dhlamini	Ass Manager Risk Office	051 412 2779	Hlomlani.Dhlamini@centlec.co.za
Daniel Malokase	Manager	051 412 2634	Daniel.malokase@centlec.co.za
Gerald Nkota	Chief Security Officer	051 412 2207	Gerald.Nkota@centlec.co.za

Facilities Team

The Facilities Team will be responsible for all issues related to the physical facilities that house IT systems. They are the team that will be responsible for ensuring that the standby facilities are maintained appropriately and for assessing the damage too and overseeing the repairs to the primary location in the event of the primary location's destruction damage.

Role & Responsibilities

1. Ensure that the standby facility is maintained in working order
2. Ensure that transportation is provided for all employees working out of the standby facility
3. Ensure that hotels or other sleeping are arranged for all employees working out of the standby facility
4. Ensure that sufficient food, drink, and other supplies are provided for all employees working out of the standby facility
5. Assess, or participate in the assessment of, any physical damage to the primary facility
6. Ensure that measures are taken to prevent further damage to the primary facility
7. Work with insurance company in the event of damage, destruction or losses to any assets owned by CENTLEC
8. Ensure that appropriate resources are provisioned to rebuild or repair the main facilities in the event that they are destroyed or damaged
9. After CENTLEC is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Table 3: Facility Team

Leads Name	Designation	Phone Number	E-mail
Agnes Mosala	Asst Manager Facility	051 412 2383	Agnes.mosala@centlec.co.za
Brian Leserwane	Manager Facility	051 412 2384	Brian.Leserwane@centlec.co.za

11.3 Network Team

The Network Team will responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and telephony connections internally within the enterprise as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

Role & Responsibilities

1. In the event of a disaster that does not require migration to standby facilities, the team will determine which network services are not functioning at the primary facility
2. If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.
3. If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.
4. In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility
5. Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:

    5.1 All members of the DR Teams

    5.2 All manager -level and Executive Staff

    5.3 All IT employees

    5.4 All remaining employees

6. Install and implement any tools, hardware, software and systems required in the standby facility
7. Install and implement any tools, hardware, software and systems required in the primary facility
8. After CENTLEC is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead

summarizing their activities during the disaster

Table 4: Network team

Leads Name	**Designation**	**Phone Number**	**E-mail**
Sipho Twala	IT Support	051 412 2605	Sipho.Twala@centlec.co.za
Ambeswa Ngetu	IT Support	051 412 2384	Ambeswa.Ngetu@centlec.co.za
Ntshepase Sepalo	IT Support	051 409 2358	Ntshepase.Sepalo@centlec.co.za

11.4 Server Team

The Server Team will be responsible for providing the physical server infrastructure required for the enterprise to run its IT operations and applications in the event of and during a disaster. They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

Role & Responsibilities

1. In the event of a disaster that does not require migration to standby facilities, the team will determine which servers are not functioning at the primary facility
2. If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:
3. Assess the damage to any servers
4. Restart and refresh servers if necessary
5. Ensure that secondary servers located in standby facilities are kept up-to- date with system patches
6. Ensure that secondary servers located in standby facilities are kept up-to- date with application patches
7. Ensure that secondary servers located in standby facilities are kept up-to- date with data copies
8. Ensure that secondary servers located in standby facility are backed up appropriately
9. Ensure that all the servers in the standby facility abide by CENTLEC's server policy

10. Install and implement any tools, hardware, and systems required in the standby facility
11. Install and implement any tools, hardware, and systems required in the primary facility
12. After CENTLEC is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Table 5: Server team

Leads Name	**Designation**	**Phone Number**	**E-mail**
Molly Josane	IT Hardware Specialist	051 412 2378	Molly.Josane@centlec.co.za
Mapaseka Maqwara	IT Support	051 412 2637	Mapaseka.Maqwara@centlec.co.za

11.5 Applications Team

The Applications team will be responsible for ensuring that all enterprise applications operates as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

Role & Responsibilities

1. In the event of a disaster that does not require migration to standby facilities, the team will determine which applications are not functioning at the primary facility
2. If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:
3. Assess the impact to application processes
4. Restart applications as required
5. Patch recode or rewrite applications as required
6. Ensure that secondary servers located in standby facilities are kept-up-to-date with application patches
7. Ensure that secondary servers located in standby facilities are kept-up-to-date with data copies

8. Install and implement any tools, software and patches required in the standby facility
9. Install and implement any tools, software and patches required in the primary facility
10. After CENTLEC is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities

Table 6: Application team

Leads Name	Designation	Phone Number	E-mail
Molly Josane	IT Hardware Specialist	051 412 2378	Molly.Josane@centlec.co.za
Mapaseka Maqwara	IT Support	051 412 2637	Mapaseka.Maqwara@centlec.co.za
Ambeswa Ngetu	IT Support	051 412 2384	Ambeswa.Ngetu@centlec.co.za
Ntshepase Sepalo	IT Support	051 409 2358	Ntshepase.Sepalo@centlec.co.za
Ambeswa Ngetu	IT Support	051 412 2384	Ambeswa.Ngetu@centlec.co.za
Thulo Mophethe	Application support	051 409 2433	Thulo.Mophethe@centlec.co.za
Ongezwa Nkomana	Data Analyst	051 409 2261	Ongezwa.Nkomana@centlec.co.za

11.6 Communication Team

This will be the team responsible for all communication during a disaster. Specifically, they will communicate with CENTLEC's employees, clients, vendors and suppliers, banks, and even the media if required.

Role & Responsibilities

1. Communicate the occurrence of a disaster and the impact of that disaster to all CENTLEC's employees
2. Communicate the occurrence of a disaster and the impact of that disaster to authorities as required
3. Communicate the occurrence of a disaster and the impact of that disaster to all CENTLEC's partners

4. Communicate the occurrence of a disaster and the impact of that disaster to all CENTLEC's clients
5. Communicate the occurrence of a disaster and the impact of that disaster to all CENTLEC's vendors
6. Communicate the occurrence of a disaster and the impact of that disaster to media contacts, as required
7. After CENTLEC is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Table 6: Communication team

Leads Name	**Designation**	**Phone Number**	**E-mail**
Lele Mamatu	GM: Strategic support	051 409 2718	Lele.Mamatu@centlec.co.za
Tseliso Leba	Communications Officer	051 409 2228	Tseliso.Leba@centlec.co.za

11.7 Recovery Facilities

In order to ensure that CENTLEC is able to withstand a significant outage caused by a disaster, it has provisioned separate dedicated standby facilities. This section of this document describes those facilities and includes operational information should those facilities have to be used.

Description of Recovery Facilities

The Disaster Command and Control Centre or Standby facility will be used after the Disaster Recovery Lead has declared that a disaster has occurred. This location is a separate location to the primary facility.

The IT department and the Disaster Recovery teams will use the standby facility; it will function as a central location where all decisions during the disaster will be made. It will also function as a communications hub for CENTLEC.

The standby facility must always have the following resources available:

1. Copies of this DRP document
2. Fully redundant server room

3. Sufficient servers and storage infrastructure to support enterprise business operations
4. Office space for DR teams and IT to use in the event of a disaster
5. External data and voice connectivity
6. Sleeping quarters for employees that may need to work multiple shifts
7. Kitchen facilities (Including food, kitchen supplies and appliances)
8. Bathroom facilities (including toilets, showers, sinks and appropriate supplies)
9. Parking spaces for employee vehicles

11.8 Communicating During Disaster

In the event of a disaster CENTLEC will need to communicate with various parties to inform them of the effects on the business, surrounding areas and timelines. The Communications Team will be responsible for contacting all of CENTLEC's stakeholders.

Communicating with the Contractors

The Communications Team's first priority will be to ensure that the appropriate authorities have been notified of the disaster, providing the following information:

1. The location of the disaster
2. The nature of the disaster
3. The magnitude of the disaster
4. The impact of the disaster
5. Assistance required in overcoming the disaster
6. Anticipated timelines

Table 7 : Contractor team

Contractors	**Services**	**Responsible le Person**	**Phone Number**	**E-mail**
Vodacom	Firewall	Mothibi	084 966 6976	Mothibi.Hlaheng@vcontractor.co.za
Telkom	VoIP PBX	Antonio	082 998 4108	Antonio.Thomas@bcx.co.za
BCX	Solar System	Amanda	072 214 2148	amanda.els@bcx.co.za
Mosima	Vending	Victor	083 2929271	victor.motaung@mosima.co.za

Payday	Payday	Magda	012 803 7730	magda@payday.co.za
LQ Tech	AD and Exchange	Claudius	082 476 5567	claudius@lqtechnologies.co.za

12. DRP ACTIVATION

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

1. That a disaster has occurred
2. The nature of the disaster (if known)
3. The initial estimation of the magnitude of the disaster (if known)
4. The initial estimation of the impact of the disaster (if known)
5. The initial estimation of the expected duration of the disaster (if known)
6. Actions that have been taken to this point
7. Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads
8. Scheduled meeting place for the meeting for Disaster Recovery Team Leads
9. Scheduled meeting time for the meeting of Disaster Recovery Team Leads
10. Any other pertinent information

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management team Lead

13. ASSESSMENT OF CURRENT AND PREVENTION OF FURTHER DAMAGE

Before any employees from CENTLEC can enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

The first team that will be allowed to examine the primary facilities once it has been deemed safe to do so will be the Facilities Team. Once the Facilities Team has completed and examination of the building and submitted its report to the Disaster Recovery Lead, the Disaster Management, Networks, Servers, and Operations Teams will be allowed to examine the building. All teams will be required to create and initial report on the damage and provide this to the Disaster Recovery Lead within 3 days of the initial disaster.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect CENTLEC's assets. Any necessary repairs or preventative measures must be taken to protect the facilities; the Disaster Recovery Team Lead must first approve these costs.

14. STANDBY FACILITY ACTIVATION

The Standby Facility will be formally activated when the Disaster Recovery Lead determines that the nature of the disaster is such that the primary facility is no longer sufficiently functional or operational to sustain normal business operations.

Once this determination has been made, the Facilities Team will be commissioned to bring the Standby Facility to functional status after which the Disaster Recovery Lead will convene a meeting of the various Disaster Recovery Team Leads at the Standby Facility to assess next steps. These next steps will include:

1. Determination of impacted systems
2. Criticality ranking of impacted systems
3. Recovery measures required for high criticality systems
4. Assignment of responsibilities for high criticality systems
5. Schedule for recovery of high criticality systems
6. Recovery measures required for medium criticality systems
7. Assignment of responsibilities for medium criticality systems
8. Schedule for recovery of medium criticality systems
9. Recovery measures required for low criticality systems
10. Assignment of responsibilities for recovery of low criticality systems
11. Schedule for recovery of low criticality systems
12. Determination of facilities tasks outstanding/required at Standby Facility
13. Determination of operations tasks outstanding/required at Standby Facility
14. Determination of communications tasks outstanding/required at Standby Facility
15. Determination of facilities tasks outstanding/required at Primary Facility
16. Determination of other tasks outstanding/required at Primary Facility
17. Determination of further actions to be taken

During Standby Facility activation, the Facilities, Networks, Servers, Applications, and Operations teams will need to ensure that their responsibilities, as described in the "Disaster

Recovery Teams and Responsibilities" section of this document are carried out quickly and efficiently so as not to negatively impact the other teams.

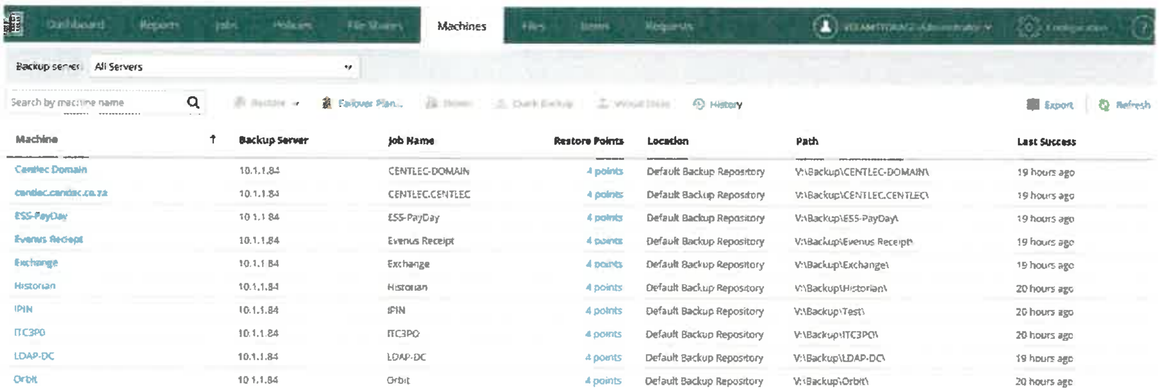
15. RESTORING IT FUNCTIONALITY

Should a disaster actually occur and CENTLEC need to exercise this plan, this section will be referred to frequently, as it will contain all of the information that describes the manner in which CENTLEC's information system will be recovered.

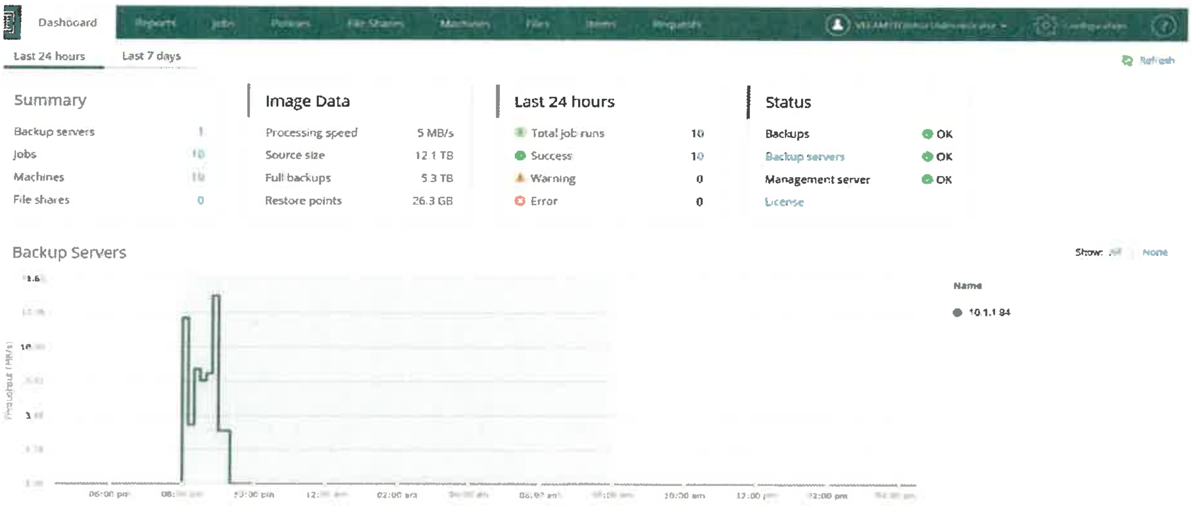
15.1 Repair & Rebuilding of Primary Facility

Before the enterprise can return operations to Primary Facilities, those facilities must be returned to an operable condition. The tasks required to achieve that will be variable depending on the magnitude and severity of the damage. Specific tasks will be determined and assigned only after the damage to Primary Facilities has been assessed.

15.2 Current System Architecture



Machine	Backup Server	Job Name	Restore Points	Location	Path	Last Success
Centlec Domain	10.1.1.84	CENTLEC-DOMAIN	4 points	Default Backup Repository	V:\Backup\CENTLEC-DOMAIN\	19 hours ago
centlec.centlec.co.za	10.1.1.84	CENTLEC.CENTLEC	4 points	Default Backup Repository	V:\Backup\CENTLEC.CENTLEC\	19 hours ago
ESS-PayDay	10.1.1.84	ESS-PayDay	4 points	Default Backup Repository	V:\Backup\ESS-PayDay\	19 hours ago
Evenus Reciept	10.1.1.84	Evenus Receipt	4 points	Default Backup Repository	V:\Backup\Evenus Receipt\	19 hours ago
Exchange	10.1.1.84	Exchange	4 points	Default Backup Repository	V:\Backup\Exchange\	19 hours ago
Historian	10.1.1.84	Historian	4 points	Default Backup Repository	V:\Backup\Historian\	20 hours ago
IPIN	10.1.1.84	IPIN	4 points	Default Backup Repository	V:\Backup\Test\	20 hours ago
ITC3PO	10.1.1.84	ITC3PO	4 points	Default Backup Repository	V:\Backup\ITC3PO\	20 hours ago
LDAP-DC	10.1.1.84	LDAP-DC	4 points	Default Backup Repository	V:\Backup\LDAP-DC\	19 hours ago
Orbit	10.1.1.84	Orbit	4 points	Default Backup Repository	V:\Backup\Orbit\	20 hours ago

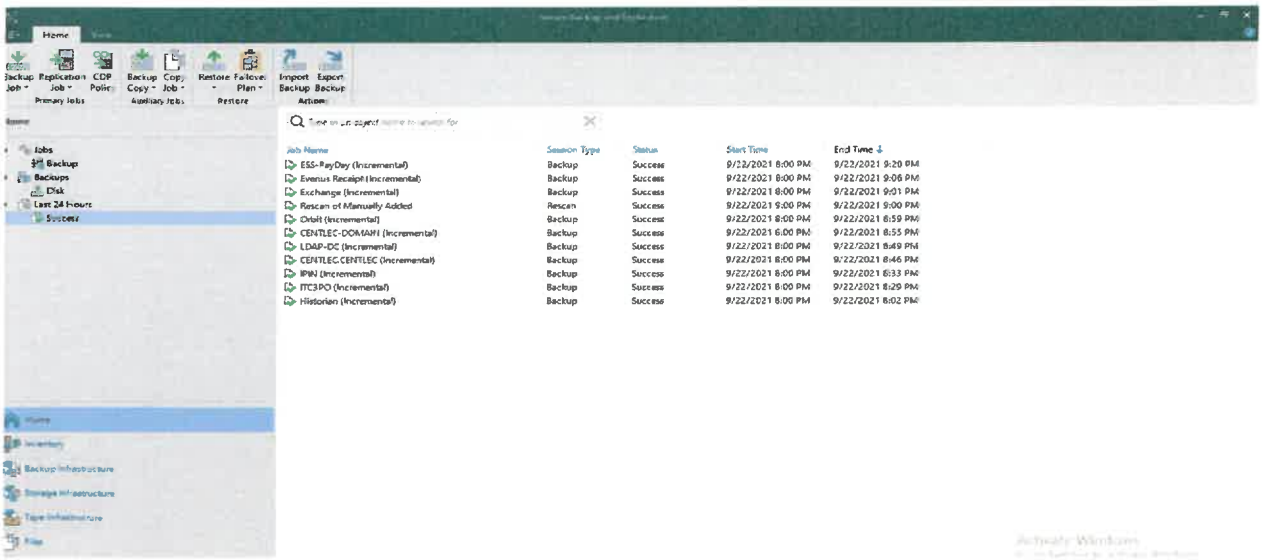


Summary	
Backup servers	1
Jobs	10
Machines	10
File shares	0

Image Data	
Processing speed	5 MB/s
Source size	12.1 TB
Full backups	5.3 TB
Restore points	26.3 GB

Last 24 hours	
Total job runs	10
Success	10
Warning	0
Error	0

Status	
Backups	● OK
Backup servers	● OK
Management server	● OK
License	



Job Name	Session Type	Status	Start Time	End Time
ESS-PayDay (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 9:20 PM
Evenus Receipt (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 9:06 PM
Exchange (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 9:01 PM
Rescan of Manually Added	Rescan	Success	9/22/2021 9:00 PM	9/22/2021 9:00 PM
Orbit (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 8:59 PM
CENTLEC-DOMAIN (Incremental)	Backup	Success	9/22/2021 6:00 PM	9/22/2021 8:55 PM
LDAP-DC (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 8:49 PM
CENTLEC.CENTLEC (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 8:46 PM
IPIN (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 8:33 PM
ITC3PO (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 8:29 PM
Historian (Incremental)	Backup	Success	9/22/2021 8:00 PM	9/22/2021 8:02 PM

15.3 **Primary** Site Procedure and Business Site recovery procedure Person identifying disaster should immediately contact the DR Leaders. Define any other protocols you may find necessary for this person after identifying a disaster. Once the disaster recovery team gets to work, this team should be notified by contact stated in the service provider contacts. Disaster team will also notify the employee by means of telephone broadcast message.

The ICT team should decide which business processes are required to provide an emergency level of service to your cu stomer meaning which type of service and impact for each system identified.

Services should be restore from the main site within 1HR. The switchover t transition from the main site to DR should be the failover of a split second not to lose data.

15.4 **Recovery** Level Objective (RLO):

This allows the operations for non-operation. Readiness preparations should be done in terms of emergency level. Which key business process will be launch during the disaster? CENTLEC should insure that tool of trades for the users and other environment is working. This includes the network and other communication systems.

15.5 **Recovery** Time Objective (RTO):

Level of services such as Email other than the full exchange server is better to recover a bit of data at point in time. The systems should be able to cater for such incident.

15.6 **Recovery** Point Objective (RPO):

The recovery point objective is the point back in time to which you wish to restore from. The most recent backup is the main priority to return to normal operations that is to say the most recent backups. If ICT want to look at an h our before the disaster then you should be backup data every hour. The way you set your RPO will dictate how often you should perform backups. However this could be different for each file system; those, which are mission critical, should be backed up continuously or very often. Less important, or non-mission critical, files can be backed up less frequently.

16. MAINTENANCE

The DRP will be updated frequently to effect the upgrade or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.
Maintenance of the plan will include (but is not limited to) the following:

1. Ensuring that call trees are up to date
2. Ensuring that all team lists are up to date
3. Reviewing the plan to ensure that all of the instructions are still relevant to the organization
4. Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals
5. Ensuring that the plan meets any requirements specified in new laws
6. Other organizational specific maintenance goals

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

17. TESTING

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

17.1 **Walkthroughs** - Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset or people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).

17.2 **Simulations** - A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyses the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

17.3 **Parallel Testing-** A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

17.4 **Full-Interruption Testing-** A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and t therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.

18. DR SITE NECESSITIES

Office space for critical staff and management must be made available at secondary CENTLEC sites. All secondary sites are already interconnected via wireless wan. All workstations must have connectivity to the internet and e-mail. Operating software including security software must be stored in the Recovery Kit.

Access to a high-capacity colour Multi-Function Copier is essential for all workstations connected to the network.

Provision must be made for printing from all relevant information systems including transversal systems.

All system documentation, configuration documentation, system images, system ghosts, duplicate software (including licences) must be available in Recovery Kit.

18.1 Backups, vital records and systems

All weekly back-ups are kept ICT Offices currently and proposed offsite namely (Harvard Substation) in Qwakafontein.

18.2 Recovery Kit Contents and Devices

The contents of the Recovery kit to be stored at the above locations shall include:

18.2.1 A copy of the ICT Disaster Recovery Plan

18.2.2 All keys to locks for physical access to ICT sites including high-sites and computer/server rooms.

18.2.3 All Administrator account passwords including SQL database usernames and passwords.

18.2.4 Copies of all relevant software packages stored centrally on magnetic media (solid-state External Hard disk)

18.2.5 Latest Monthly backups of information systems.

18.2.6 All software licensing information

18.2.7 Service provider details and contacts

18.2.8 Health and Safety information and details

18.2.9 Security information and details

18.2.10 Communication details

18.2.11 Backup and incident procedure

18.3 Items available at the Disaster Recovery Site

The following items need to be ready for use at each of the DR sites when it is finalised:

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

18.3.2 Telephones, Photocopiers, etc.

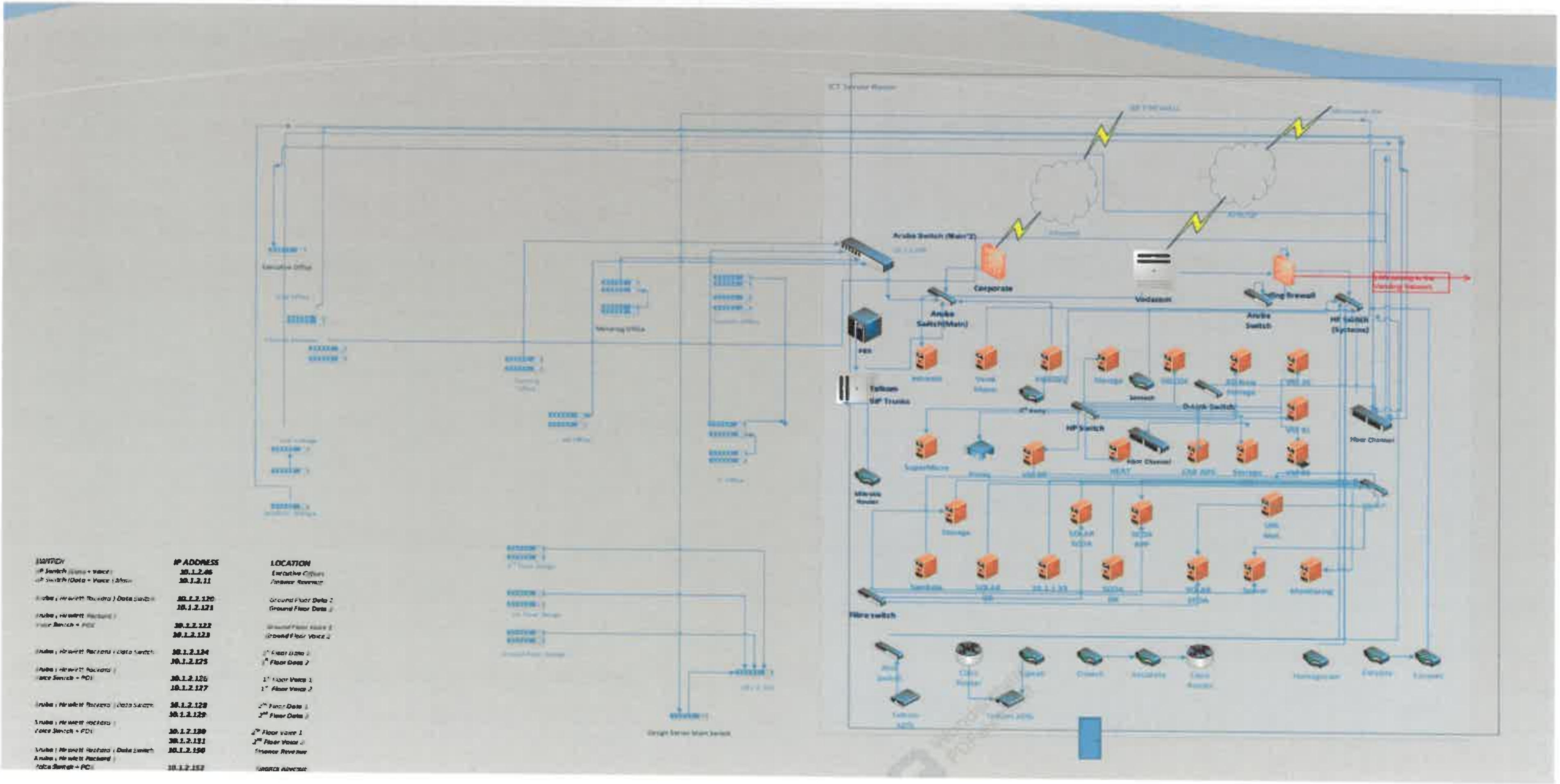
18.3.3 Power points, standby power, air-conditioning

18.3.4 Heat detectors

18.3.5 Fire suppressors

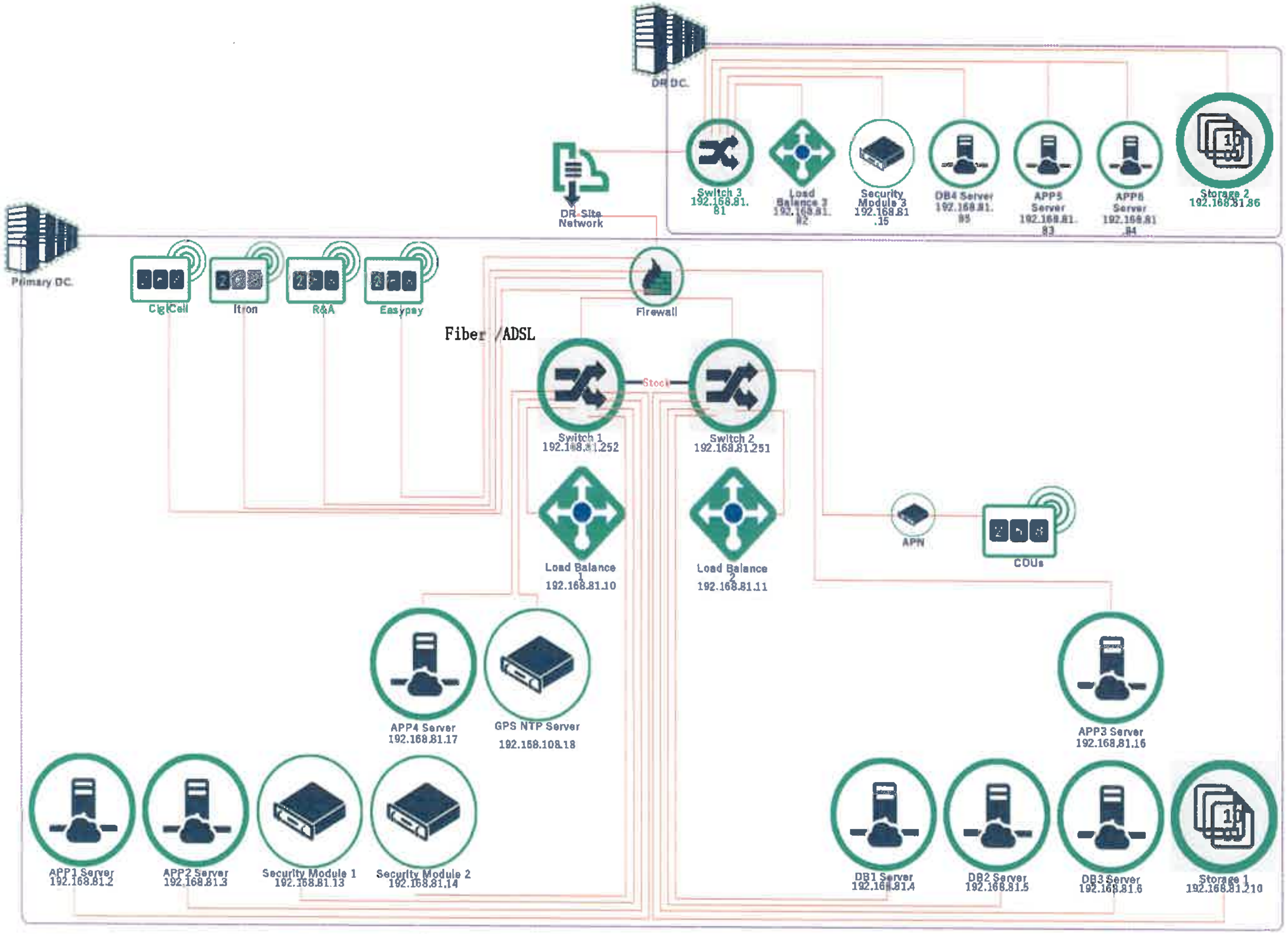
18.3.6 Batteries and UPS

19. NETWORK INFRASTRUCTURE

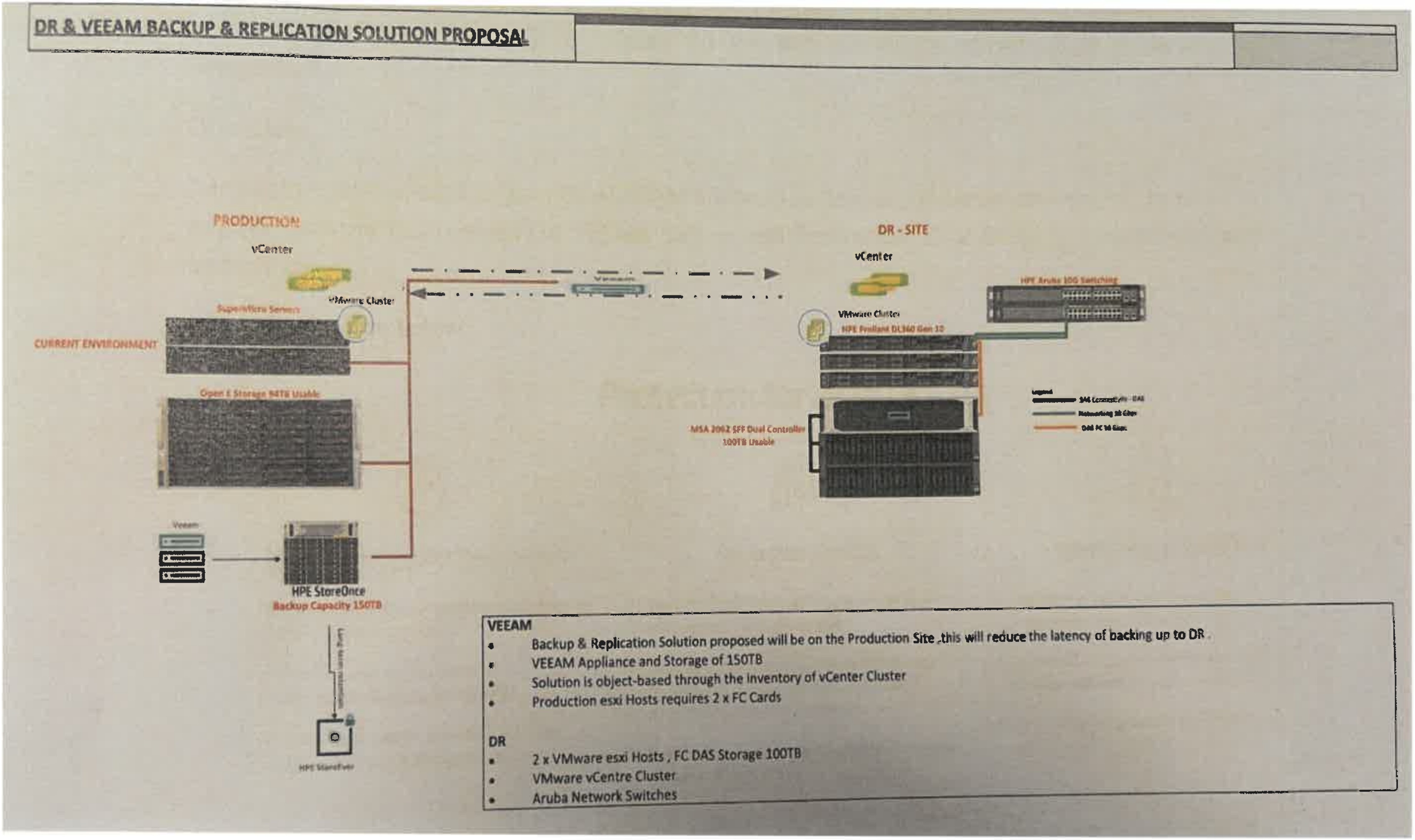


SWITCH	IP ADDRESS	LOCATION
IP Switch (Data + Voice)	10.1.2.46	Executive Offices
IP Switch (Data + Voice) Main	10.1.2.11	Finance Revenue
Aruba (Hewlett Packard) Data Switch	10.1.2.120	Ground Floor Data 1
	10.1.2.121	Ground Floor Data 2
Aruba (Hewlett Packard) Voice Switch + POE	10.1.2.122	Ground Floor Voice 1
	10.1.2.123	Ground Floor Voice 2
Aruba (Hewlett Packard) Data Switch	10.1.2.124	1st Floor Data 1
	10.1.2.125	1st Floor Data 2
Aruba (Hewlett Packard) Voice Switch + POE	10.1.2.126	1st Floor Voice 1
	10.1.2.127	1st Floor Voice 2
Aruba (Hewlett Packard) Data Switch	10.1.2.128	2nd Floor Data 1
	10.1.2.129	2nd Floor Data 2
Aruba (Hewlett Packard) Voice Switch + POE	10.1.2.130	2nd Floor Voice 1
	10.1.2.131	2nd Floor Voice 2
Aruba (Hewlett Packard) Data Switch	10.1.2.150	Finance Revenue
Aruba (Hewlett Packard) Voice Switch + POE	10.1.2.152	[illegible]

20. VENDING INFRASTRUCTURE



21. DISASTOR AND RECOVERY NETWORK TOPOLOGY



DR & VEEAM BACKUP & REPLICATION SOLUTION PROPOSAL

VEEAM

- Backup & **Replication** Solution proposed will be on the Production **Site** ,this **will reduce** the latency **of backing up to DR** .
- VEEAM Appliance and Storage of 150TB
- Solution is object-based through the inventory of vCenter Cluster
- Production esxi Hosts requires 2 x FC Cards

DR

- 2 x VMware esxi Hosts , FC DAS Storage 100TB
- VMware vCentre Cluster
- Aruba Network Switches

22. REVIEW AND APPROVAL

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

Revised by:

Signed:______________________
Manager: Information Management
Date: 22 / 05 / 2023

Supported by:

Signed:______________________
Act Executive Manager: Engineering Retail
Date: 22 / 05 / 2023

Approved by:

Signed:______________________
Chief Executive Officer
Date 22 / 05 / 2023