DIGICALL

DIGICALL BUSINESS CONTINUITY & DISASTER RECOVERY PLAN

DOCUMENT CLASSIFICATION	Internal
VERSION	1.1
DATED	01 August 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSITION	SIGNATURE	DATE
Johan Kriel	Group CIO		28 Nov 2024
Irene Nel	Chief Operations Officer: Business Process Management		28 Nov 2024

This document supersedes and replaces all previous versions of this document.

Revisions

VERSION	DATE	AUTHOR	SUMMARY OF CHANGES
0.1	22.02.2022	Ameet Ranchod	Initial Draft
0.9	22.02.2022	Ameet Ranchod	Final Draft
1.0	21.07.2022	Ameet Ranchod	Version 1.0 of new BCDR
1.1	08.01.2024	Donald Fraser	Updated personnel & roles, removed ContinuitySA, Majuda Added solar generation

Contents

1 Introduction

This document details the Business Continuity and Disaster Recovery Plan (BCDRP) for the Digicall Group. In the event of a disruption impacting the organization's operational capabilities, this plan serves as a critical framework to ensure the business can sustain its financial commitments and fulfil its operational responsibilities.

This plan serves as a guidance document for addressing significant disruptions to business operations. From a business systems perspective, these disruptions can be categorized into two primary scenarios:

Staff Access Impact: Events that hinder employees' ability to access Digicall facilities, potentially affecting their ability to perform tasks.

System Disruption: Events that impair the functionality or availability of business systems, while physical facilities remain operational and accessible.

This categorization enables targeted responses and ensures the continuity of critical business processes under varied conditions.

The Digicall Group acknowledges the growing importance of Information Technology services to its customers. This policy outlines the strategy the organization employs to assess disaster recovery (DR) requirements, and to develop, implement, and continually evaluate a comprehensive Business Continuity and Disaster Recovery (BCDR) solution. This strategy ensures an appropriate response is tailored to the criticality of each service. Our mission is to maintain information system uptime, data integrity, availability, and overall business continuity to support uninterrupted operations on a 24/7/365 basis.

2 Purpose

This document delineates our policies and procedures for recovering from disasters affecting staff's ability to access Digicall facilities, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes the recommended procedures which will come into effect if an actual emergency should arise.

2.1 Management has approved the following:

1. The company shall develop a comprehensive Business Continuity and Disaster Recovery Strategy.
2. This strategy shall contain a comprehensive Business Continuity and IT Disaster Recovery plan.
3. The strategy should differentiate between people and technology.
4. A risk assessment shall be undertaken to determine the requirements for the business continuity plan.
5. The business continuity and disaster recovery plan shall cover all essential and critical infrastructure elements, systems, networks, and people, in accordance with key business activities.

6. The business continuity and disaster recovery plan shall be evaluated at least annually in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
7. All staff shall be made aware of the business continuity disaster recovery plan and their own respective roles.
8. The business continuity and disaster recovery plan shall be kept up to date to consider changing circumstances and shall be reviewed at least annually.

The principal objective of the business continuity and disaster recovery program is to develop, test, and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from a disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

1. The need to ensure that all employees fully understand their duties in implementing such a plan.
2. The need to ensure that operational policies are adhered to within all planned activities.
3. The need to ensure that proposed contingency arrangements are cost-effective.
4. The need to consider implications on other company sites.
5. Business continuity and disaster recovery capabilities as applicable to key customers, vendors, and others.

3 General

Digicall Group responsibility for BCDR provisioning for branches will be limited to ensuring network resilience to maintain continuous access to these services following a disaster level event affecting the Digicall Group computer network.

In preparing this plan the following assumptions have been made:

1. All development work shall cease immediately following a disaster. This will free up Digicall Group resources to execute the BCDR plan.
2. Development staff shall be released to enact the recovery, and development computer resources will be available to be reconfigured to replace lost production services.
3. Systems shall be restored based on the priority as determined by the Group CIO and available as Annexure K.
4. The policy and plan are expected to cater for only one disaster level event at any one time.

4 Scope

Any part of business operations is a potential risk to business-as-usual operations. The list below covers only some of the potential risks that can impact business operations:

1. Loss of incoming calls through a network outage or other service disruption that only affects the technology platform. Staff are still able to access facilities, and only the technology platforms are affected.

2. Loss of network due to a power outage, network interface card failure, cable problem or cable connector problems, cable cut, lightning strike, or trunk interface failure. Staff are still able to access facilities, and only the technology platforms are affected.
3. Loss of the hardware due to a hardware failure, power outage, circuit board failure, software failure, or human error. Staff are still able to access facilities, and only the technology platforms are affected.
4. Loss of the information systems due to a power outage, server failure, or storage element failure. Staff are still able to access facilities, and only the technology platforms are affected.
5. Loss of premises and/or services available on said premises (water supply, electricity) forcing a *Work-from-Home* event, while leaving technology platforms intact.
6. External impact: communicable outbreak or pandemic, Acts of God, or extreme weather, forcing a *Work-from-Home* event, while leaving technology platforms intact.
7. Loss of staff due to civil/political unrest, industrial action, or other unknown threats, forcing a *Work-from-Home* event, while leaving technology platforms intact.
8. Loss of service providers, that does not impact Digicall staff from accessing facilities or technology platforms.

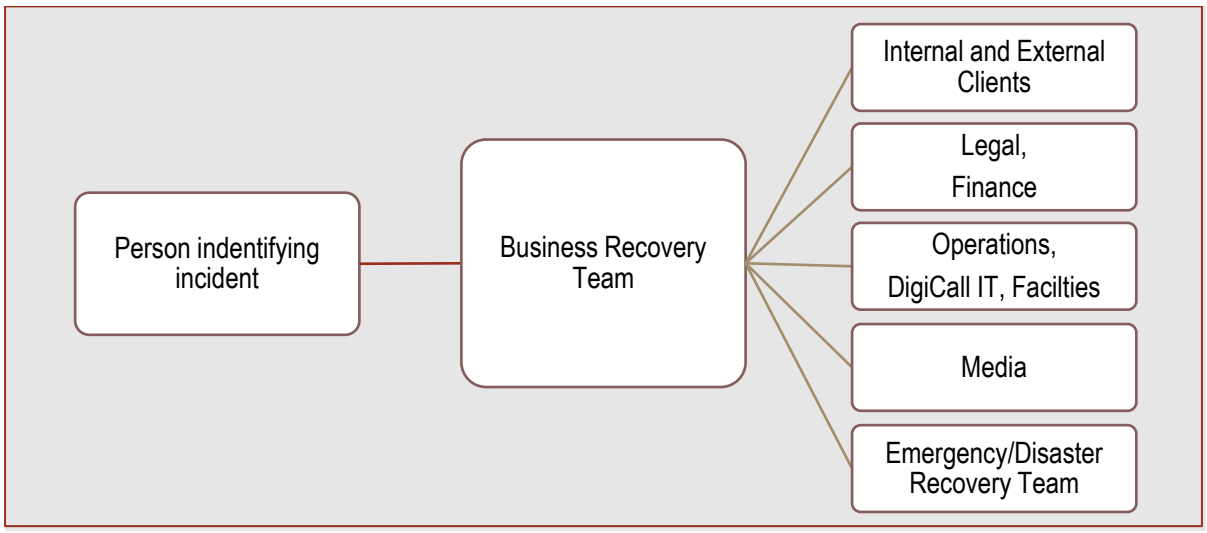
4.1 Abbreviations

Description	Abbreviation
Business Recovery Team	BRT
Business Continuity	BC
Business Continuity & Disaster Recovery Plan	BCDRP
Contact Centre Manager	CCM
Chief Executive Officer	CEO
Chief Information Officer	CIO
Chief Operations Officer	COO
Customer Relationship Management Software	CRM
Direct Inbound Dial	DID
Disaster Recovery	DR
Disaster Recovery Team	DRT
Emergency Recovery Team	ERT
General Manager	GM
Internet Service Provider	ISP
Information Technology	IT
Local Area Network	LAN
Recovery Point Objective	RPO
Recovery Time Objective	RTO
Uninterruptable Power Supply	UPS

4.2 Key Personnel Information

Refer to Annexure A for list of key personnel and contact details.

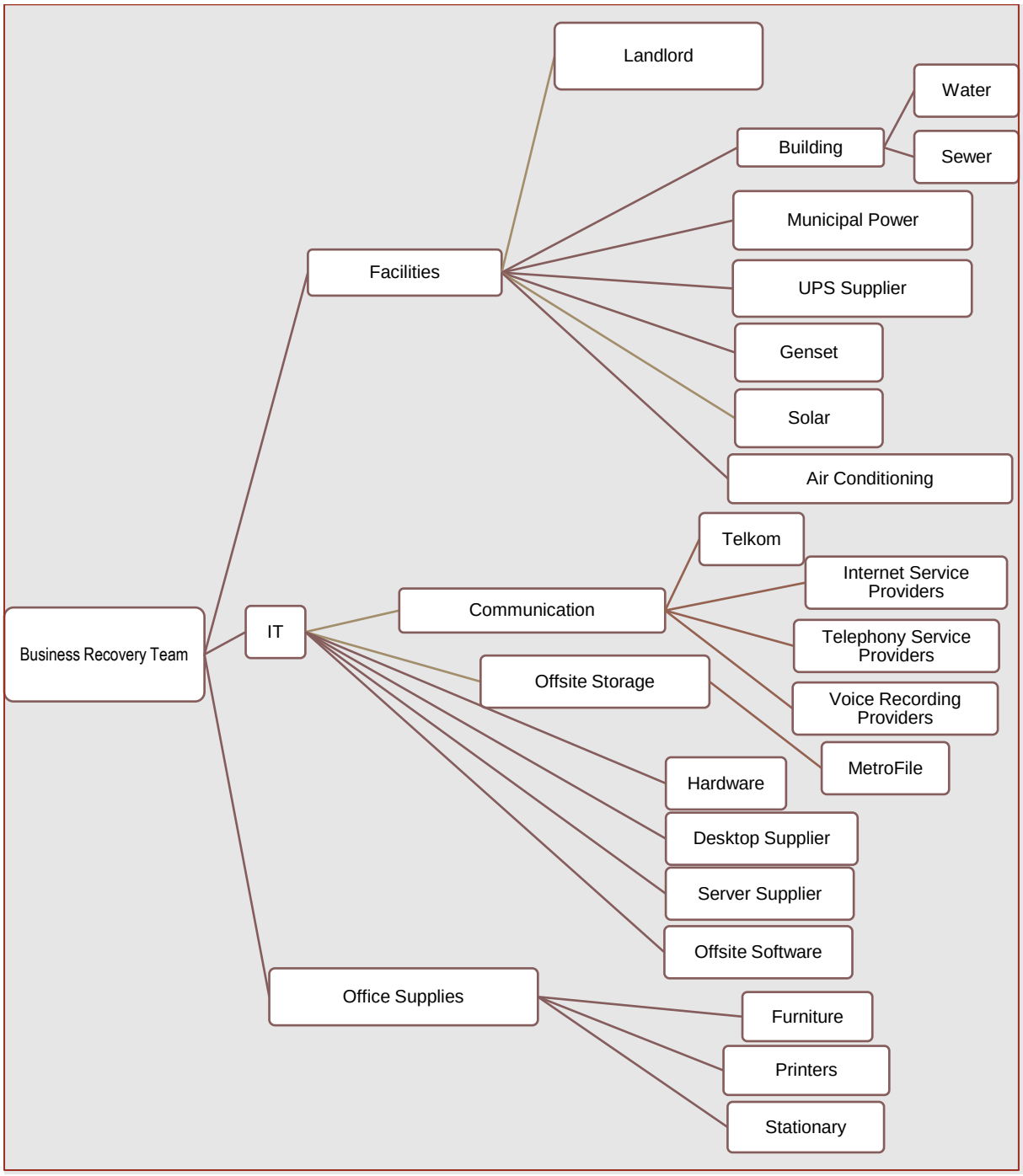
4.3 Internal Notification Process



Refer to Annexure C for Business Recovery Team members.

Refer to Annexure G for internal notification personnel and contact details.

4.4 External Notification Process



Refer to Annexure H for external notification personnel and contact details.

Refer to Annexure D for Disaster Recovery Team members and contact details.

5 Plan Overview

5.1 BCDR Plan Updates

It is necessary for the BCDRP updating process to be properly structured and controlled. Whenever changes are made to the plan, they are to be fully evaluated, and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the Change Manager.

5.2 BCDR Plan Document Storage

1. Copies of this plan will be stored in secure locations as defined in Annexure E.
2. Each member of senior management will have access to the online share where the BCDR plan is located.
3. Printed copies of the BCDR plan, along with the contact lists as per Annexures A and B, will be available in key areas in both buildings as defined in Annexure E.
4. A Master protected copy will be stored on Teams for this purpose.

5.3 Business Continuity Strategy

1. Key business processes and the agreed recovery strategy for each are listed below.
2. The BCDR strategy is divided into the following areas: People & Systems.
3. Where people are impacted, the process is to move staff to Work from Home (WFH) processes.
4. The strategy chosen is for business-critical systems recovery at the various sites is listed below:

Key Business Processes	Recovery Strategy
IT Operations (Systems, Servers)	Recover all affected systems and data using backups. Recovery to primary or secondary datacentre depending on severity of incident.
IT Operations (Hardware)	Recover all affected systems from redundant systems, hospital stock, or suppliers. For example, recover faulty firewall from spare firewall or unit stored offline in dedicated storage.
IT Operations (Staff)	Implement *Work-from-Home* solution where People are affected. Systems to continue as normal.
Email	Login to Mimecast directly.
Call Centre (Systems)	Re-route calls to secondary voice solution.
Call Centre (Staff)	Implement *Work-from-Home* solution where People are affected. Systems to continue as normal.
Building / Facilities	Implement *Work-from-Home* solution for affected departments where People are affected. Systems to continue as normal.

5.4 Roles & Responsibilities

This section describes the expected responsibilities to be conducted by each role in the Recovery Team. The list of responsibilities below is applicable for all Team Members:

1. Complete an initial assessment of the incident.
2. Ensure all relevant members of the BRT and DRT are notified and updated regularly.
3. Assist the implementation of the BCP.

Shift Supervisor on Duty - BRT	
#	**Responsibilities**
1	Informing the / Responding to the decision to activate the BCDRP.
2	Establishing contact with relevant internal / external support contacts.
3	Consult with IT Management to establish a Business Continuity Co-ordination Point (If required).
4	Provide initial impact assessment and evaluation to the CIO/COO, as well as ongoing updates of the recovery.
5	Manage the BRT activities and ensure that all members are briefed and understand their individual and team responsibilities.
6	Communicate to CIO/COO about the business disruption and any implemented alternate working arrangements. Provide regular updates (where applicable).
IT & Infrastructure Manager/Support – BRT & EDRT	
#	**Responsibilities**
1	Coordinate technology resources and equipment throughout the invocation of the plan. Discussions with Internal/External Contacts to invoke manual workaround as required.
2	Responsible for the recovery and resumption of the Digicall IT business processes (where applicable).
3	Engage and consult with any relevant external providers throughout the invocation of the plan.
4	Provide recovery updates to the CIO/COO.
5	Consult with BRT to establish Business Continuity Co-ordination Point (if required).
Shift Supervisor / Manager on Duty - BRT	
#	**Responsibilities**
1	Responsible for the recovery and resumption of the Human Resources business processes.
2	Ensure all members of BRT and EDRT are kept updated regularly.
3	Communicate Business Continuity Co-ordination Point to all staff if applicable.
Sales, Marketing and Legal - BRT	
#	**Responsibilities**

1	Consider legal implications during the incident – specifically as they apply to contractual obligations, applicable, laws and regulations. Engage CEO/COO/CIO.
2	Inform clients of disruption, provide updates, and inform when return to business as usual.
3	Ensure all documentation for follow-up investigation, compensation, insurance, and litigation purposes is collated.

5.5 Risk Management

There are multiple potential disruptive threats which can occur at any time and affect the normal business process. Considerations have been made for a wide range of potential threats and the results of deliberations are included in this section. Each potential environmental disaster or emergency has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows for both systems and staff:

Material Impact	Significant	**1**	**2**	**1**	**1**
	Moderate	**2**	**2**	**2**	**1**
	Low/ Negligible	**3**	**3**	**3**	**2**
			3	**2**	**1**
			No Impact	Degraded	No Services
			Ability to deliver services		

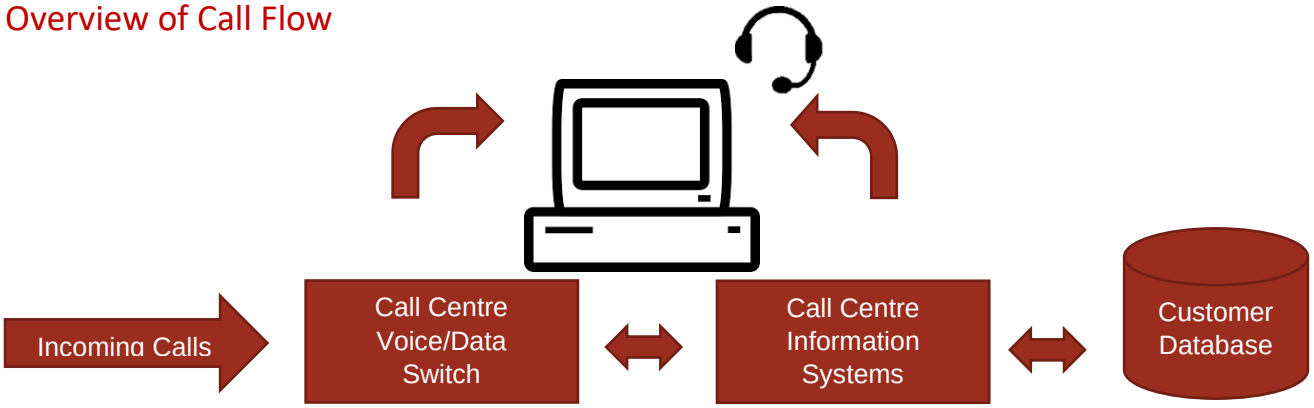
A severity rating of 0 (zero) will be assigned to any situation where essential services, as determined by government, are not available because of a disaster. An event of this nature will be categorised as catastrophic to business, with no contingency plans as the ability to render services will be non-existent during the period of the disaster.

Potential Disaster	Material Impact	Ability to deliver services	Sev	Brief description of potential consequences & remedial actions
Flood	3	3	3	All critical power equipment is located on ground floor and in basement. Move People to WFH.
Fire	3	3	3	Suppression system installed in main computer room. Fire and smoke detectors on all floors. Move People to WFH.
Tornado	3	3	3	Destruction or damage to facilities. Move People to WFH.
Electrical storms	3	3	3	Good grounding of all electrical circuits is essential. Failure of this will jeopardize the equipment to the breaker.
Act of terrorism	3	3	3	Inability of staff to perform services. Move People to WFH.
Act of sabotage	3	3	3	Business systems unavailable, invoke DR processes.
Electrical power Failure	3	3	3	Redundant UPS array, solar generation with battery storage and auto standby generator (n+1) that is evaluated weekly & remotely monitored 24/7.
Loss of communications network services	1	1	1	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience.
Pandemic/Epidemic Outbreak	3	3	3	Viral Outbreak, requiring staff to be quarantined. Remote working will then be enforced for applicable staff, should a site be quarantined. Move People to WFH.
Loss of premises	3	3	3	Offices used to deliver serviced rendered unsafe, move to reduced capacity work from home/remote methods, with the plan to move to resume services at full capacity as determined by the RTO's.
Loss of a major % of staff	2	2	2	Move to reduced capacity work from home/remote methods, with the plan to move to resume services at full capacity as determined by the RTO's
Loss of service providers	3	3	3	Unable to render services to clients.

6 Emergency Response

6.1 Alert, Escalation and Plan Invocation

Overview of Call Flow



6.2 Plan Triggering Events

Key trigger issues at head office where the recovery time is not within 4 hours and will thus lead to activation of the BCDRP are:

- Loss of / denial of access to equipment
- Loss of / denial of access to technology (IT Applications / Voice / Data)
- Significant loss of Human Resources
- Significant and unexpected increase in inbound call volume
- Reduced speed of applications
- Media reports
- Breakdown of communication between any services
- Loss of internet connectivity
- Hardware failure – on premise
- Hardware failure – off premise
- Reduced/revoked access to key operational systems – DAS, FIMS, DPS, Nova, DigiClaim, etc.

6.3 Assembly Points

Where the premises need to be evacuated, the BCDRP invocation plan identifies evacuation assembly points in Annexure F.

6.4 Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the BCDRP must be invoked.

1. Responsibilities of the ERT are to:
    1.1. Respond immediately to a potential disaster and call emergency services.
    1.2. Assess the extent of the disaster and its impact on the business, data centre, call centre etc.
    1.3. Decide which elements of the BCDR Plan should be activated.
    1.4. Establish and manage the disaster recovery team to maintain vital services and return to normal operation.
    1.5. Ensure employees are notified and allocate responsibilities and activities as required.
2. Post activation, management and co-ordination of the business recovery is led by the Shift Supervisor on duty and supporting recovery team as directed by the manager. Refer to Annexure C for BRT members and contact information.
3. When the business continuity plan is deactivated by the BRT, the following actions must be completed:
    3.1. All relevant Business Units are informed of the stand-down decision.
    3.2. Internal and External Stakeholders are informed of the stand-down decision.
    3.3. All relevant information is stored, photographed, copied, or duplicated, to be able to evaluate the handling of the business disruption; and
    3.4. Initiate the re-setting of the Business Continuity Coordination Point and its equipment.

6.5 Business Continuity Co-Ordination Point

If the BCP is invoked, the BRT will assemble and coordinate all response activities from a predetermined location called the Business Continuity Coordination Point (BCCP).

The BCCP will be determined by the severity of the disruption and when the BRT have been notified. Refer to Section 5.

The BCCP options are as follows:

Business Continuity Coordination Point Options				
#	**LOCATION**		**CAPACITY**	**AVAILABLE FACITLITIES**
1	People - Work from home provisions		Unlimited	Full Facilities
	DOWNTIME TO SETUP	4 hours	**OUTAGE DURATION**	Unlimited
2	System – Data centre Alternative		0 Seats	
	DOWNTIME TO SETUP	8 hours	**OUTAGE DURATION**	Unlimited
	CRITICAL SYSTEM PRIORITY	Refer to Annexure K		

Further to the above, Recovery Time and Point Objectives (RTO/RPO) are split into distinct levels, dependant on the nature of disaster.

The Recovery Point Objective (RPO) for a local hardware failure (loss of a physical server) is 2 hours where backups are local to the environment.

Recovery Time Objective (RTO) in this scenario is 4 hours to completely restore services.

In the event of a total failure occurring at the hosted data centre site, a Recovery Point Objective (RPO) of 7 days is specified and a Recovery Time Objective (RTO) of 48 hours is specified.

7 Plan Limitations

This plan is limited to the recovery of the business processes. This plan does not outline the approach to rebuild or market the service(s).

8 Summary of Process Recovery and Strategies

The plan has been split into different emergency/disaster scenarios. The scenarios are split according to the issues and incidents raised. These incidents are not inclusive and because this is a “living document” it can and will change as need dictates.

The following table highlights the recovery strategy order for the operations for the first 24 hours for these “high-level” incidents.

The Recovery Team must review the business process recovery order at the time of the incident to confirm the restoration order, in line with the business priorities.

RECOVERY STRATEGY				
Business Asset	**Severity**	**Maximum Acceptable Outage Time (MAO)**	**Contingency 1**	**Contingency 2**
Loss of Building	3	8 hours	Staff operate from home, no change to systems.	Move Staff to alternative site
Loss of Power	3	Less than 5 minutes	Back-up generator, solar. Staff remain at primary site.	UPS / Recall staff to BCCP 1-3
Loss of > 50% Human Resources	3	4 Weeks	Support Staff to assist. Staff remain at primary site.	Remaining 50% of staff will be utilised to facilitate 100% of services, while remaining 50% is re-filled. Staff remain at primary site.
Loss of Technology – Telephony (Primary Platform)	1	2 hours	Inbound calls re-routed to DR system. Staff remain at primary site.	
Loss of Technology – CRM	1	1 hours	Switch to alternative instance. Staff remain at primary site.	Use manual process. Staff remain at primary site.
Loss of Technology – Platform (Physical/Virtual Server)	1	4 hours	Switch to alternative instance. Staff remain at primary site.	Switch to manual operations. Staff remain at primary site.

Loss of Technology – Internet	1	1 hours	Auto failover to backup link. Staff remain at primary site.	Agents to use mobile 4G/5G hotspot. Staff remain at primary site.
Loss of Hosted Data Centre	1	4 hours	Failover to DR data centre. Staff remain at primary site.	Resurrect critical production services in the public cloud. Staff remain at primary site.

8.1 Loss Of Building Facilities / Building Evacuation

The following table lists the facilities used by Digicall and their business-required Recovery Time Objective (RTO)

#	Facilities	Business-required RTO
1	Secure office building	< 1 day

The following table identifies the workarounds for building facilities, as identified in the business impact analysis:

Office details			**110 Conrad Drive, Craighall, Johannesburg, Gauteng**		
Workaround description			Temporary movement of office resources and human resources to off-site location or WFH.		
How long can this workaround be performed for?			Unlimited		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
1	Identify need to, and evacuate the premises	Fire Marshals	This may be enacted by any staff member should the need arise after hours.		
2	Notify senior management BCDR Process Enacted	Shift Supervisor	This may be completed by any staff member should the need arise after hours		

3	Contact relevant members of EDRT, request lines be diverted to BCCP location 1-3.	Shift Supervisor	See Annexure B	Yes	
4	Notify Key client contacts of BCDR Process Enacted	KAMS/COO	See Annexure F		Email sent to the key contacts outlining the system issue and potential impact
5	Notify Service Provider Network BCDR Process Enacted	Provider Network Management/Supplier Management team/COO			Email sent to the key contacts outlining the system issue and potential impact
6	Notify all employees of change of location for shift.	Shift Supervisor			Message sent to all staff to advise outage.
7	Arrange transportation of resources including human resources to the agreed BCCP	Shift Supervisor			

In the event of office evacuation, any member of the BRT or EDRT can access the BCDRP by means of:

1. Electronic copy located on the Intranet.
2. Each member of the BRT and DRT can access a copy of the BCDRP on their personal device.

8.2 Loss of Power

Power failures can be classified as external power failures, such as municipal service failure, or internal power failures, such as a short circuit in the wiring within the environment.

8.2.1 External Power Failures:

- Digicall Group generates its own power via the on-site solar plant, this plant is backed up with on-site energy storage.
- We are also equipped with a UPS (Uninterrupted Power Supply) unit, which supplies power to all the servers and relevant equipment in case of power failure.
- Diesel powered generators will supply electricity to the solar plant during an extensive power failure.
- The generator (N+1) has an automatic mains failure panel that will automatically start/stop the generator. The generator must be checked every 2 hours during usage for water, oil, and diesel levels.
- The parties responsible for checking levels during use are the Infrastructure Manager and his team.

The escalation process:

1. Service Delivery Manager / Infrastructure Back-Office Manager
2. Infrastructure Manager
3. CIO
4. Any other ER Team Member

8.2.2 Internal Power Failures:

All internal power failures are to be referred to the list of electricians and service providers as detailed in Annexure H.

The following table lists the facilities used by Digicall and their business-required Recovery Time Objective (RTO)

#	Facilities	Business-required RTO
1	Electrical power supply	< 1 day

The following table identifies the workarounds for building facilities, as identified in the business impact analysis:

Supply details			**Electricity is supplied by municipality/local authority**		
Workaround description			Engagement of the back-up generator, UPS & solar generation. Staff to remain at primary site for as long as backup procedures are operational.		
How long can this workaround be performed for?			If generator fuel and /or sunlight for solar generation is available.		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
When the municipal power supply to the office has failed, the UPS array, along with solar generation and battery storage, will automatically take over the provisioning of electricity. Back-up generators will automatically engage to top up the batteries. The below action would only be required in the event the back-up generators also failed.					
1	Notification of loss of power to the BRT / DRT	Shift Supervisor	This may be completed by any staff member should the need arise after hours		
2	Engage UPS and solar array, inverters, and battery banks from solar plant	BRT	Automatic	Yes	
3	Notify Customer Service Team to use laptops to continue service provision	Shift Supervisor			Message sent to all staff to advise outage.
4	Engage building management and IT on fault and expected recovery time	BRT			
5	Based on the above, decide whether BCCP will be required	BRT	If relocation to BCCP is required, follow contingencies listed in 5.1 Loss of Building.	Yes	
6	Provide regular updates on expected return to normal and when normal power supply is returned.	BRT			Message sent to all staff to advise return to normal.

8.3 Severity Related Actions – External:

Severity	Responsibility and Action
Severity 1	Infrastructure Manager, CIO
Severity level 1 incidents are incidents such as power failures that exceed 8 hours. Once the 8-hour mark has been reached the generator will run out of fuel. Refuelling can be performed by the Infrastructure Manager and his team. Spare diesel fuel is stored on the premises under lock and key. While solar generation is available, is it not designed to fully replace the generator, especially at night when no sunlight is available to recharge the batteries.	Inform City Power as a matter of urgency. Re-fill fuel as the need arises. Invoke DR Procedures.
Severity 2	Any ER Team Member
Severity level 2 incidents are incidents such as power failures that are between 4 and 8 hours. City Power must be informed	Inform Eskom and City Power as a matter of urgency.
Severity 3	Any ER Team Member
Severity level 1 incidents are incidents such as power failures that do not exceed 4 hours. Eskom must be informed of the failure in their service.	Inform Eskom and City Power as a matter of urgency.

8.4 Severity Related Actions – Internal:

Severity	Responsibility and Action
Severity 1	Infrastructure Manager, CIO
Severity level 1 incidents are incidents such as power failures that are expected to exceed 1 hour.	Inform Service Providers as a matter of urgency. Invoke DR Procedures.
Severity 2	Any ER Team Member
Severity level 2 incidents are incidents such as power failures that are expected to last between 30 minutes and 1 hour.	Inform Service Providers as a matter of urgency.
Severity 3	Any ER Team Member
Severity level 3 incidents are incidents such as power failures that are expected to last up to 30 minutes.	Inform Service Providers as a matter of urgency.

Service Provider contacts: See Annexure H for contact details.

8.5 Loss of Equipment – End User Equipment

The following table lists the technology used by the Digicall and their business-required Recovery Time Objective (RTO):

#	IT Application/Software Name/Data Terminal	Business-required RTO
1	Primary PC's (All)	< 1 day

The following table identifies the workarounds for IT Applications/Software, as identified in the business impact analysis:

Equipment		Primary PC's			
Workaround description		Use of Laptops / Work from Home Provisions for Staff.			
How long can this workaround be performed for?		> 5 days			
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
1	Activate the Business Continuity Plan	Shift Supervisor			
2	Provide impact assessment and evaluation to the CIO and COO	Shift Supervisor			
3	Substitute data terminal for laptops / direct team members to work from home. Location scheduling to be allocated and team members notified.	Shift Supervisor			
4	Complete incident log forward to BRT Retain record locally.	Shift Supervisor			
5	Investigate / test / repair / replace faulty items	IT & infrastructure Manager/Support		Yes	
6	Log parts / assets replaced and inform BRT of return of asset	IT & infrastructure Manager/Support		Yes	

8.6 Loss of Technology – Platform

The following table lists the technology used by the Digicall and their business-required Recovery Time Objective (RTO):

#	Facilities	Business-required RTO
1	Platform	< 1 day

The following table identifies the email workarounds for IT Applications/Software, as identified in the business impact analysis:

IT Application			Platform		
Workaround description			Perform manually – Engage providers through CRM. Staff to remain at primary site.		
How long can this workaround be performed for?			> 1 day		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required?	Communications Unit Assistance Required?
1	Refresh program, if not refreshed or error message	Customer Service Team			
2	Wait 1 minute and refresh again, if issue not resolved, confirm issue is not isolated to one data terminal – refer to Shift Supervisor (verify system isn't inaccessible due to maintenance)	Customer Service Team			
3	Notify the IT Support team about any issues and implement job dispatch via CRM	Shift Supervisor	Call IT Support		Email sent to the team outlining the system issue and potential impact
4	Manual transactions are processed in when the software is available.	Shift Supervisor / Provider Network Manager		Yes	
5	Establish which invoices are required to be paid over the next 2-3 days.	Office Manager		Yes	

8.7 Loss of Technology – Telephony

Technology			Telephony		
Workaround description			Use alternate telecommunication methods. Staff to remain at primary site.		
How long can this workaround be performed for?			> 5 days		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
1	Notification of loss of telephony to the BRT / DRT	Shift Supervisor	This may be completed by any staff member should the need arise after hours		
2	Escalate incident to IT for investigation.	Shift Supervisor	Call IT Support		Message sent to all staff to advise outage.
3	Staff to use alternative telephony system (hard or softphone, dependant on which system is not available)	All Employees		Yes	
4	Initiate SmartAccess DR process to reroute telephony destination numbers.	IT & infrastructure Manager/Support		Yes	
5	Once landlines or telephony system has been re-established ensure that incoming calls are diverted back to the original numbers	IT & infrastructure Manager/Support		Yes	
6	Testing of all inbound lines to ensure operational	Shift Supervisor / IT Manager/Support		Yes	

8.8 Loss of Technology – CRM

Technology			**CRM (DAS, Destiny, DSA, Digiflow, DPS, Digicall Assist system, FIMS)**		
Workaround description			Bypass of CRM > manual entry. Staff to remain at primary site.		
How long can this workaround be performed for?			> 5 days		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
1	Define and announce an outage?	Shift Supervisor	Anytime CRM is not responding for more than 5 mins and a refresh of internet browser / clear cache has not resolved the issue. Anytime CRM loses key functionality. e.g., not able to affect a service dispatch		
2	Call IT Support	Shift Supervisor			
3	Verify validity using the verification system and aid	Customer Service Team			
4	Requests to be logged on Manual Case Creation doc and Jobs manually posted to the Dispatch Platform	Customer Service Team			
6	Once CRM back online, add all cases to CRM and allocate appropriate providers.	Customer Service Team			

8.9 Loss of Technology - Internet Services

Technology Name			**Internet**		
Workaround description			Manual. Staff to remain at primary site.		
How long can this workaround be performed for?			> 1 day		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
1	Define and announce an outage?	Shift Supervisor	Anytime there is loss of Internet for more than 5 minutes.		
2	Call and inform IT & Infrastructure Manager / external support	Shift Supervisor	See Annexure A + B		
3	Ask agents to use their mobile 4g as internet hotspot	IT & Infrastructure Manager/Support		Yes	

8.10 Loss of Technology – Hosted Datacentre

Technology Name			**Hosted Data Centre**		
Workaround description			Manual. Staff to remain at primary site.		
How long can this workaround be performed for?			> 1 day		
#	Task	By Whom	Notes (Resources/Comments)	IT Assistance Required	Communications Unit Assistance Required
1	Define and announce an outage?	IT & Infrastructure Manager	Anytime there is loss of Datacentre services for more than 4 hours.		
2	Call and inform CIO	Infrastructure Manager	See Annexure A, B & I		
3	Initiate restoration at DR location decided in the BCCP	IT & Infrastructure Manager/Support	See Annexure A, B, I & K	Yes	

9 Business Continuity Communication Plan Tree

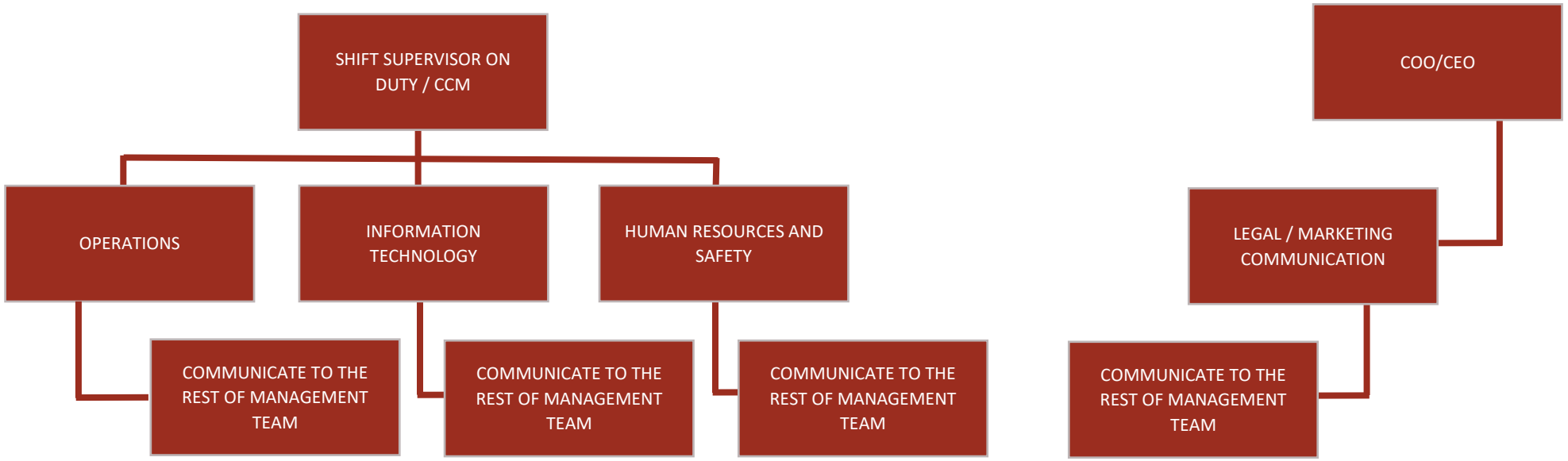
Employees and contracted partners must be contacted in the event of an emergency or disruption to business processes. On instruction from any member of the BRT, communication of the disruption must be sent to all members of the BRT.

This will be done via phone and/or WhatsApp groups which will allow for more efficient delivery of the message to all members of the team. Where the communication is required for the BRT or EDRT, WhatsApp will be the preferred channel of Communication. Communication of the disruption to specific members of the Customer Service Team can be done via phone call, WhatsApp, or the scheduling program.

Use the BCP communication tree to:

- Establish employee whereabouts and status;
- Provide information, directions, and actions;
- Arrange future communications protocol (channel / times / regularity).

Communication Tree Process should represent business as usual reporting lines. If an employee cannot be reached after 3 minutes, move onto the next person. Keep trying to reach un-contactable employee(s) on 5 minutes intervals (all numbers) until they are located.



10 Readiness Testing

Tests should be conducted annually and should cover at least two of the above scenarios. Test dates and results are to be recorded with a summary of the remediation required and timeframe for remediation.

11 Responsibilities

The IT Security and Compliance Manager is responsible for maintaining this policy and providing support and advice during its implementation in line with the IT Risk Management Policy

All Managers are personally responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

12 Policy Compliance Monitoring

12.1 Compliance

Group IT will verify compliance to this policy through various methods, including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

If any user is found to have breached this policy, they may be subject to the Digicall Group's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

12.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

12.3 Non-compliance

All users (employees, contractors, vendors) are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

12.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity, criticality, and impact, opportunities may be provided to correct identified non-compliance. This corrective action will be

evaluated on a case-by-case basis and timelines will be imposed and strictly enforced to ensure timeous remediation.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Human Resources Department or the IT Security and Compliance Officer.

13 Policy Compliance Monitoring

The following table identifies who within the Digicall Group is **Accountable, Responsible, Informed** or **Consulted** with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	**IT Security and Compliance Manager**
Accountable	Group Chief Information Officer
Consulted	IT Infrastructure Manager, Regional IT Infrastructure Managers, General Managers
Informed	All Employees, All Temporary Staff, All Contractors, All Vendors and All Suppliers

14 Audit and Review Process

This policy, and compliance there to, will be audited and reviewed internally at least once every 12 months depending on the changes or requirements within the group which will be reviewed by Management. For Group companies' pursuing certification, policies are required to be audited externally at least once in a 36-month cycle or sooner depending on changes or requirements within the group. Any employees or contractors with suggestions should refer these to their line manager in the first instance so they can be considered for implementation. Whenever changes are made to this policy the final draft will be shared with the Group CIO, IT Infrastructure Manager, and the IT Security & Compliance Manager for review and approval before publication.

IT Security and Compliance Manager will undertake annual policy review.

The COO and CIO will annually perform management reviews together with the Infrastructure Manager and IT Security & Compliance Manager after the annual tests have been performed.

15 Appendices

Business Impact Analysis

Business Continuity Disaster Recovery Policy Annexures