

# **FCMB Pensions Limited**

## **Business Continuity Management Plan**

Revised

April 29, 2022

**APPROVAL PAGE**

Title of Document:	Business Continuity Management Plan		
Prepared by:	Benedict Ohiovbeunu		
Designation:	Head, Risk Management		
	Date: 28/4/2022	Sign: 	
	Approved by:		
Managing Director/Chief Executive	Christopher .B. Bajowa	Date: 28/4/2022	Sign: 
Chairman Board Risk Management Committee		Date: 28/04/2022	Sign: 
Board Chairman		Date: 28/04/2022	Sign: 

Approval	Date of Last Approval March 4, 2021	Revised April 2022	Renewal Annually
----------	--	-----------------------	---------------------

## TABLE OF CONTENTS

	<b>Page</b>
Approval page	2
Practices, Regulations and Standards	4
Acronyms and Abbreviations	5
<b>1. Section I: Introduction</b>	<b>6</b>
I Objective	6
II Scope	7
III Priorities in a disaster situation	7
IV Conditions	8
V Update/changes to plan	8
VI Plan Distribution List	9
<b>2. Section II: Business Continuity Strategy</b>	<b>10-15</b>
I Relocation Strategy and Disaster Recovery site	16
II Strategy on the phases of Recovery plan	16
III Document Back-up	17
IV Restoration of stored files	17
V On-line Access to FCMB Pensions Branches	18
VI Mails Distribution	18
<b>3. Section III: Recovery Teams</b>	<b>19</b>
I Recovery Team Responsibilities	20
a. General Responsibilities	20-21
b. Specific Responsibilities	22
I Business Continuity Plan Coordinator	22-23
II Business Continuity and Recovery Team	23
III Information Technology Recovery Team	23
IV Corporate Resources Team	24
<b>4. Section IV: Recovery Procedures</b>	<b>25</b>
Phase I: Disaster Occurrence	25-29
Phase II: Plan Activation	30-33
Phase III: Transition to Head Office (Primary Site)	34-35
<b>5. Section V: Plan Testing</b>	<b>36</b>
I Disaster Recovery Test	36 - 38
II Scenario Based Test	38
III Established Responsibilities	38 - 39
<b>6. Section VI: Appendices</b>	<b>40-51</b>

## **PRACTICES, REGULATIONS AND STANDARDS.**

Some of the international best practices, regulations and standards used in the development of this Business Continuity Management Plan were as:

- i. FCMB Pensions Enterprise Risk Management Policy.
- ii. PenCom Risk Management Framework.
- iii. PenCom IT guidelines.
- iv. ISO 22301:2019: Security and resilience- Business Continuity Management Systems.
- v. ISO/IEC 27001-Information security management.
- vi. Business Continuity Institute (BCI) - Provides good practices for business continuity management.
- vii. Disaster Recovery Institute International (DRII) – Provides professional practice for business continuity professionals.
- viii. ISACA-COBIT framework provides guidance on IT controls that are relevant to the business.

## ACRONYMS AND ABBREVIATIONS THAT ARE USED IN THIS DOCUMENT

<b>S/N</b>	<b>ACRONYMS</b>	<b>MEANING</b>
<b>1</b>	BCRT	Business Continuity and Recovery Team
<b>2</b>	BCMP	Business Continuity Management Plan
<b>3</b>	IT	Information Technology
<b>4</b>	DRS	Disaster Recovery Site
<b>5</b>	LAN	Local Area Network
<b>6</b>	RSA	Retirement Savings Account
<b>7</b>	RTO	Recovery Time Objective
<b>8</b>	RPO	Recovery Point Objective
<b>9</b>	PenCom	National Pension Commission
<b>10</b>	ITRT	Information Technology Recovery Team
<b>11</b>	CRT	Corporate Resources Team
<b>12</b>	SLA	Service Level Agreement
<b>13</b>	MD & CEO	Managing Director & Chief Executive Officer
<b>14</b>	ED	Executive Director
<b>15</b>	HODs	Heads of Departments
<b>16</b>	ISP	Internet Service Provider
<b>17</b>	CRM	Customer Relationship Management

## 1. Section I: Introduction

FCMB Pension's Business Continuity Management Plan has been updated to reflect best practices and to give assurance to stakeholders that the company's business activities will continue seamlessly after any unforeseen business disruption. In the event of a disaster which interferes with FCMB Pensions ability to conduct business from its Head Office; this plan is to be used by the company to coordinate the business recovery activities. This plan provides reference to all of the information that might be needed for business recovery in the event of a disaster; it is therefore meant to ensure that normal operations shall be restored quickly within a day.

### I. Objectives

The objective of the Business Continuity Management Plan is to coordinate recovery of critical business functions in the event of disruption or disaster at the Head Office. This include short or long-term calamities that might affect the Head Office which relates to catastrophic events such as fires, floods, earthquakes, explosions, terrorism, extended power interruptions, natural or man-made disasters and Information Technology disruptions.

***In the context of our business management continuity planning a disaster is defined as any event that affects FCMB Pensions operations or interferes with the company's ability to deliver essential business services such as Fund Valuations, Crediting Pension Contributions of Members, Benefit Payments, Rendition of Reports to PenCom, Services to RSA holders, Retirees, Employees and other stakeholders.***

## II. **Scope**

The Business Continuity Management Plan covers business recovery and continuance due to disruptions or unforeseen circumstances of FCMB Pensions business. It also includes procedures for all phases of recovery as defined in the Business Continuity Strategy of this document. This plan is over and beyond the FCMB Pensions Information Technology Disaster Recovery Plan put in place by the IT and Systems Department, which focuses on the recovery of technology facilities and platforms, such as critical applications, databases, servers or other required technology infrastructure.

The scope of this plan is focused on localized disasters that maybe human related, technology disruptions, electrical failures, fires, floods, earthquake, volcanic eruption, thunderstorms and other natural or man-made disasters. *This is detailed in Appendix B: Risk Assessment.*

## III. **Priorities in a disaster situation.**

The priorities in a disaster after activating the BCMP shall be as follows:

- a. Ensure the safety of employees and visitors in the office buildings.
- b. Mitigate threats or limit the damage that threats can cause.
- c. Ensure that critical business functions can continue at the disaster recovery site.
- d. Use documented plans and procedures i.e. BCMP to ensure quick and effective execution of recovery strategies for critical business functions.

#### IV. **Conditions**

The viability of this Business Continuity Management Plan is based on the existence of the following conditions:

- a. That a viable and tested IT Disaster Recovery Plan exists and shall be put into operation to restore data center services at the backup site within one to two days.
- b. That this plan has been properly maintained and updated as required.
- c. That each department's critical functions have been identified in the Business Continuity Management Plan.
- d. That all critical physical documents have been scanned in docuWare application.
- e. That the company has a disaster recovery site which serves as recovery alternative site.
- f. That the disaster recovery site has available space for relocation to perform critical functions.
- g. That FCMB Pensions has a "Warm" disaster recovery site.

***WARM SITE is infrastructure that is partially configured in terms of IT, usually with network connection and essential peripheral equipment such as disk drives, tape drives and controllers. The equipment may be less capable than the normal production equipment. Most Current data would need to be loaded before operations could resume at the warm site.***

#### V. **Update/Changes to the Plan**

The Business Continuity Management Plan shall be reviewed and/or updated annually or whenever there is a significant change (Information Technology, People, Processes, and Regulations etc) within FCMB Pensions business. It is the responsibility of the Risk Management



Department to update the plan and should be duly supported by all Heads of Departments.

## VI. Plan Distribution List

The Business Continuity Management Plan document shall be distributed to the following employees:

**Table 1: The distribution list of the BCMP.**

S\N	Location	Staff
1	Head Office Abuja	ED, Operations & Services.
2	Head Office Abuja	Head Financial Control.
3	Disaster Recovery Site (DRS)	Head IT & Systems.
4	Head Office Abuja	Head Corporate Resources.
5	Head Office Abuja	Head Risk Management.

## 2. Section II: Business Continuity Strategy

The strategy to be followed in the event of the disaster at the Head Office is highlighted in this section. The strategy shall depend on the severity of disruption that may affect FCMB Pensions business.

### a. Severity of Impact

In the company's risk assessment strategy, severity shall be ranked as Critical, Major, Moderate and Minor in terms of impact on the business. The table below defined this further.

**Table 2: Severity of Impact**

<b>Severity</b>	<b>Definition</b>
Critical	The disruptions will seriously impact the operations of FCMB Pensions if it exceeds one day.
Major	The disruptions will seriously impact the operations of FCMB Pensions only if it exceeds two days.
Moderate	The disruptions will moderately impact the operations of FCMB Pensions only if it exceeds five days.
Minor	The disruptions will not seriously impact the operations of FCMB Pensions, it would only cause some inconveniences even if it exceeds two weeks.

**b. Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).**

The Business Continuity Strategy is based on Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) of the company.

*Recovery Time Objective (RTO) is defined as how quickly the process must be restored following a disaster. The Recovery Time Objective is an estimate of how long the process can be unavailable.*

*Recovery Point Objective (RPO) is the determination of how much data loss, in terms of time, is tolerable before a process is significantly impacted.*

The company's business solutions recovery strategy is based on RPO and RTO for the business as shown in table 2. IT Recovery Plan is shown in table 3 whilst the severity of natural or man-made risks are captured in table 4.

The RTO and RPO are based on Business Impact Analysis that relates to loss in revenue, increasing operating expenses, loss productivity, loss customer service and loyalty, reputational issues, employees and customer safety and security. *Appendix C-Business Impact Analysis.*

**Table 2: IT solutions recovery strategy based on RPO and RTO**

	Critical Solutions	Maximum Allowable Downtime/Data Loss-RTO and RPO				
		Within 24 hours	1-2 Days	3-5 Days	1-2 Weeks	>2 Weeks
1	EnPower	X				
2	IBS (Moneytor )	X				
3	Sage Evolution	X				
4	Sage- Pastel Payroll and HR		X			
5	Breakdown of LAN Network, Switches and Communication.	X				
6	E-mail service disruption	X				
7	Website		X			
8	Qlikview			X		
9	Legend CRM			X		

**Table 3: IT Solutions and the recovery strategy**

S/N	Solution	Ranking	Impact	Recovery Plan
1	EnPower	Critical	Complete downtime in operation	<p><b>Hard Disk Failure:</b> Redundant hard disk to take over.</p> <p><b>Server Failure:</b> Use offsite backup server.</p> <p><b>Complete loss of data centre:</b> Use offsite server at Disaster Recovery Site currently at UBA Branch Asokoro. Restore last backup from Networker.</p>
2.	IBS ( Moneytor)	Critical	Complete downtime in operation	<p><b>Hard Disk failure:</b> Redundant hard disk to take over.</p> <p><b>Server Failure:</b> Use offsite backup server.</p> <p><b>Complete loss of data centre:</b> Use offsite server at Disaster Recovery Site currently at UBA Branch Asokoro. Restore last backup from Networker.</p>
3.	Sage Evolution	Critical	Complete downtime on company's account management	<p><b>Server Failure:</b> Restore the application on the backup server and restore last data backup from Tape.</p> <p><b>Complete loss of data centre:</b> Use offsite server at Disaster Recovery Site currently at UBA Branch Asokoro. Restore last backup from Networker.</p>
4.	Sage –Pastel Payroll & HR	Major	Complete downtime on HR payroll management	<p><b>Server Failure:</b> Restore the application on the backup server and restore last data backup from Networker.</p> <p><b>Complete loss of data centre:</b> Use offsite server at Disaster Recover Site currently at UBA Branch Asokoro. Restore last backup from Networker.</p>

5.	Breakdown of Network & communication to Vodacom.	Critical	Complete downtime on operations with external stakeholders	Activate the backup network link with (Direct on Data) DOD communications.
6.	Breakdown of particular Servers at FCMB Pensions.	Critical	Complete downtime of connected devices.	Get replacement from Asokoro branch.
7.	Breakdown of LAN Switches	Critical	Complete downtime on internal operations and external stakeholders.	Inform internal Network Engineers.
8.	E-mail service disruption	Critical	Exchange server is completely inaccessible.	Restore the exchange server from offsite server at our Disaster Recover Site currently at UBA Branch Asokoro. Restore last backup from Networker.
9.	Website	Major	Website attack/not working.	Contact vendor immediately and ensure the website is safe and online.
10.	Qlikview	Moderate	Qlikview is not working.	Contact vendor immediately and ensure the website is safe and online.
11.	Legend CRM/IVR	Moderate	Legend CRM/IVR is not working.	Contact vendor immediately and ensure the website is safe and online.

**Table 4: Natural or man-made disruptions.**

S/N	Risk Type	Gross Risk Score	Recovery Location
1	Fires	High	Asokoro
2	Floods	High	Asokoro
3	Earthquake	High	Asokoro
4	Volcanic Eruption	High	Asokoro
5	Lightning and Thunderstorm	High	Asokoro
6	Windstorm, Tornadoes and Hurricane	High	Asokoro
7	Snow and Ice Storm	Medium	Asokoro
8	Pandemic	High	Asokoro
9	Terrorist/Insurgency Attack	Very High	Asokoro
10	Power Loss	Medium	Asokoro
11	Kidnapping and Ransom	Very High	N/A
12	Damage to reputation and Brand	High	Asokoro
13	Politics /Office Inaccessible	High	Asokoro
14	Cyber security	High	Asokoro
15	Data Privacy	Medium	N/A
16	Loss of critical Data-Empower, Moneytor, Sage Evolution, Qlikview and Legend CRM etc.	High	Asokoro
17	Loss of data center	High	Asokoro
18	Loss of Network Communication	High	Asokoro
19	Loss of key service providers	High	Asokoro
20	Loss of office building	High	Asokoro
21	Loss of human Life	Very High	N/A

*More details in appendix B: Risk Assessment.*

## I. Relocation Strategy and Disaster Recovery Site

In the event of a disaster or disruption of services at the Head office, the strategy is to recover critical activities or functions by relocating to the company's Disaster Recovery Site.

**Table 4: Primary and Disaster Recovery Site.**

<b>Primary Location(Head Office)</b>	<b>Disaster Recovery Site and Data Back-up site.</b>
207, Zakaria Maimalari Street, Cadestral Zone AO, CBD, Abuja.	No. 1, Julius Nyerere Street, Asokoro. - <b>DRS</b>
	No. 90, Awolowo Way, Ikoyi, Lagos State. - <b>Data Backup site.</b>

The above relocation strategies will be used in the short-term (not more than three months). The long-term strategies will be to acquire/lease and equip new office space in another location.

## II. Strategy on the Phases of Recovery Plan

The activities necessary to recover from a disaster or disruption shall be divided into three phases. These phases shall come sequentially one after the other.

### a) Disaster Occurrence

This phase shall begin after the occurrence of the disaster event and continues until a decision is made to activate the BCMP. Major activities that take place in this phase includes: emergency response, notification of management, damage assessment activities, and declaration of the disaster.

### b) Plan Activation

In this phase, the BCMP is activated. This phase shall continue until the Disaster Recovery Site is occupied, critical business activities or

functions re-established, and computer system services are restored. Major activities in this phase include: notification and assembling of the recovery teams, relocation to the DRS, sitting arrangements at the DRS, the re-establishment of communication lines across all branches and relevant stakeholders.

**c) Transition to Head Office-Primary Site**

This phase consists of any and all activities necessary to make the transition back to the Head Office.

**III. Document Backup (Members RSA forms and other vital documents)**

Important document as it relates to all departments shall be backed up in

DocuWare Application by the concerned departments and shall be done on daily basis or as the need arises. This shall be done by scanning, indexing and uploading the vital document accordingly into the Application. Some of the other files shall be periodically backed up and stored both at the Head Office, DRS and at the offsite location in Lagos by IT and Systems Departments.

**IV. Restoration of Stored Files.**

In the event of Head Office unforeseen disruption, critical files and records of RSA holders may be destroyed or inaccessible. In this case, the last backup of critical files and records in DocuWare Application and DRS shall be activated and used in the restoration process.

The following categories of information can be exposed to loss:

- a. Any files stored in the Head Office in file cabinets e.g. RSA filled forms and underlining document, SLAs with vendors and counterparty and Retirees Files.



- b. Information stored on local personal computer hard drives and networks.
- c. Information stored on departmental network drives.
- d. Work in progress.
- e. Received and un-opened mail.
- f. Other documents and files in Head Office and staff desks.

#### **V. On-line Access to FCMB Pensions Branches.**

In the event of a disruption at the Head Office, the IT Disaster Recovery Plan strategy shall assist in re-establishing connectivity to the company's branches and customers for the resumption of normal services. The services shall include e-mails, phones, mobile apps and other forms of communications across the company.

#### **VI. Mails Distribution**

During the time that FCMB Pensions operations are run from the DRS, Official Mails shall be received at the site. Mails shall be sent by designated courier company to customers and other stakeholders.

### 3. Section III: Recovery Teams

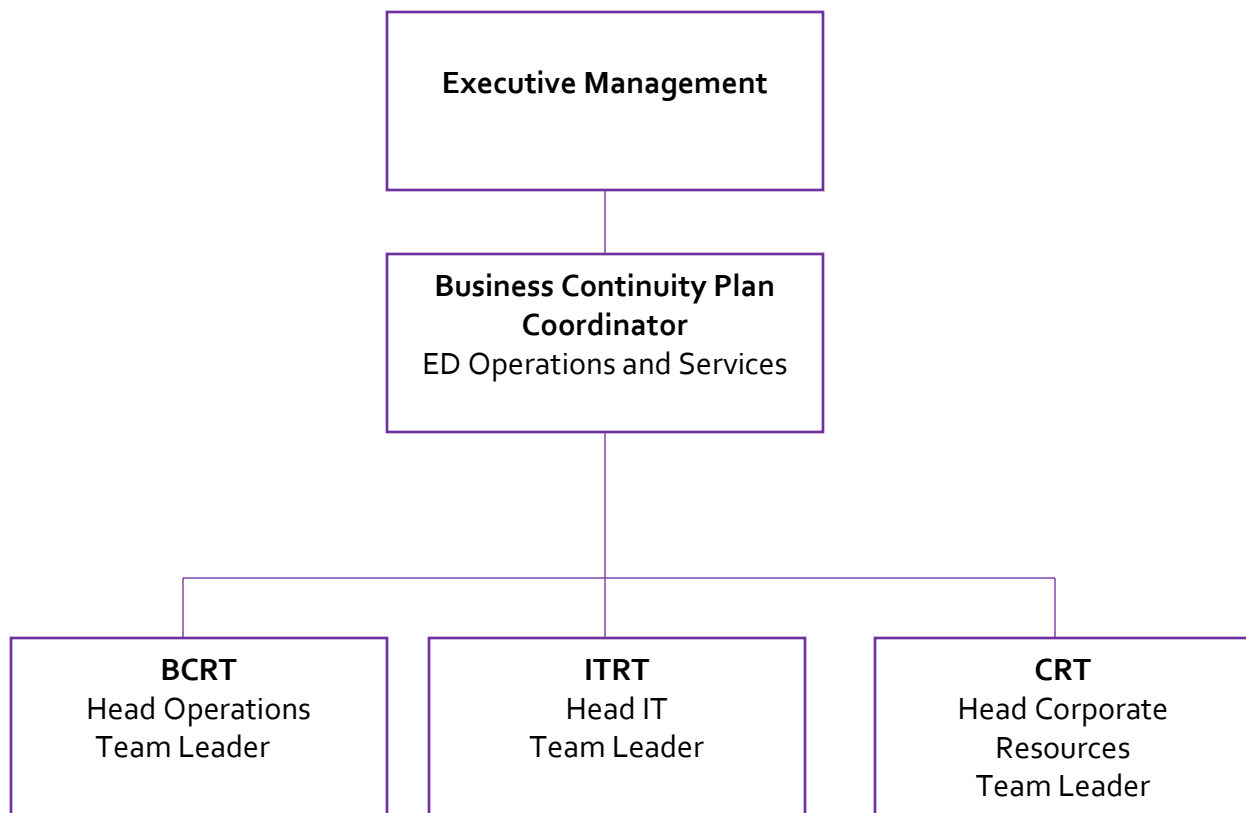
All HODs shall participate in the recovery process of the Business Management Continuity Plan. HODs shall be organized into one or more teams. Each team shall have designated team leader.

Selected teams in the BCMP shall be responsible for various oversight functions relating to the disaster recovery. The recovery operational teams recognized for the purpose of the BCMP shall be as follows:

- a. Business Continuity and Recovery Team (BCRT)
- b. Information Technology Recovery Team (ITRT)
- c. Corporate Resources Team (CRT)

There shall be a BCMP Coordinator who shall be the leader of these teams. With respect to this document, the ED, Operations and Services shall be the company's BCMP Coordinator.

**Team Organogram –Figure 1**



## I. Recovery Team Responsibilities.

The recovery team's responsibility shall be based on both general and specific responsibilities. Identified team roles and the specific responsibilities shall be assigned to each team.

### a. General Responsibilities-Table 5

No	Activities	Description	Responsibility	Support
1.	Coordination of recovery activities.	Overall coordination and management of recovery activities	Business Continuity Management Coordinator.	BCRT
2.	Documentation of recovery activities.	Adequate documentation of all activities involved in recovery process	Head IT/Company Secretary	BCRT
3.	Senior Management Liaison	Communicate with the senior management on the decision of the team	Business Continuity Management Coordinator.	BCRT
4.	Plan Execution	Execution of the recovery exercise.	Business Continuity Management Coordinator.	BCRT/HODs
5.	Staff assignments	Assign staff to various roles during recovery exercise.	Business Continuity Management Coordinator.	BCRT/HODs
6.	Activation of recovery team	Call the recovery team to action whenever the need arise.	Business Continuity Management Coordinator	BCRT/HODs
7.	Communication with system users	Communicate with the system users on the	Head IT	ITRT/HODs

		status of IT infrastructure required for business continuity.		
8.	Vendor Interface	Communicate with various vendors for further support to keep the business up and running.	Head, IT and Head, CR	CFO/CRT
9.	Equipment salvage	Take inventory of the company's equipment after the recovery exercise.	Head, IT and Head, CR	CRT/Team Members
10.	Equipment installation	Install company's equipment required to keep the business running.	Head, IT and Head, CR	ITRT/CRT
11.	Restoration of primary site	Ensure the primary site is back to its normal state prior to the incident	Head, IT and Head, CR	BCRT
12	Obtain system and other documentations.	Provide IT system and other company asset after the incident.	Head, IT and Head, CR	ITRT
13.	Prepare recovery site and command centre for operation.	Ensure the recovery site is up and running to support continuous business operations.	Head, IT and Head, CR	ITRT/CRT
14.	Establish telecommunication network.	Ensure adequate telecommunication is put in place to ensure smooth running of the recovery site.	Head, IT and Head, CR	ITRT/CRT
16.	Workload scheduling	Schedule work activity appropriately among the staff.	HODs	CRT

## **b. Specific Responsibilities**

### **I. Business Continuity Plan Coordinator (ED, Operations and Services)**

In the event of a disaster, the Business Continuity Coordinator shall be responsible for ensuring that the following activities are successfully completed.

He shall:

- i. Work with the FCMB Pensions Executive Management and BCRT to officially declare a disaster, and start the Disaster Recovery/Business Continuation process to recover FCMB Pensions business functions at the DRS.
- ii. Communicate with FCMB Pensions Management that a disaster has been declared.
- iii. Work with FCMB Pensions Executive Management to authorize the use of the DRS.
- iv. Assist in the publication of an official public statement concerning the disaster.
- v. Monitor the progress of all Business Continuity and Disaster Recovery teams daily.
- vi. Present Business Continuity Plan recovery status reports to Executive Management on a daily basis.
- vii. Interface with appropriate management personnel throughout the recovery process.
- viii. Communicate directions received from FCMB Pension's Executive Management to the Recovery Team Leaders.

- ix. Provide on-going support and guidance to the Business Continuity teams and personnel.
- x. Ensure that a record of all Business Continuity and Disaster Recovery activity and expenses incurred by FCMB Pensions is being maintained.

## II. **Business Continuity and Recovery Team (BCRT)**

This team shall be responsible for:

- i. The safety of all employees.
- ii. Inspecting the physical structure and identifying areas that may have sustained damage.
- iii. Providing management with damage assessment reports and recommendations.
- iv. Head Operations, Team Leader to report to the Business Continuity Management Plan Coordinator to declare a disaster.

## III. **Information Technology Recovery Team (ITRT)**

This team shall be responsible for:

- i. Critical data recovery
- ii. IT & systems recovery including LAN Networks.
- iii. Availability of all FCMB Pension's IT systems
- iv. Technical IT & Systems support.

#### IV. **Corporate Resources Team (CRT)**

This team shall be responsible for:

- i. Providing information regarding the disaster and recovery efforts to employees and families.
- ii. Assisting in arranging cash advances if the need arises.
- iii. Notifying employee's Next of kin of employee injury or fatality.
- iv. Ensuring the processing of all life, health, and accident insurance claims as may be required.
- v. Arranging for the availability of necessary office support services and equipment.
- vi. Tracking all costs related to the recovery and restoration effort.
- vii. Taking appropriate actions to safeguard equipment from further damage or deterioration.
- viii. Coordinating the removal, transfer and safe storage of all furniture, documentation, supplies, and other materials as necessary.
- ix. Supervising all salvage and cleanup activities.
- x. Coordinating required departmental relocations to the recovery sites.
- xi. Establishing internal mail delivery procedures and process.

#### 4. **Section IV: Recovery Procedures**

This section focuses on specific activities and tasks that are to be carried out in the recovery process of the company. Given the Business Continuity Strategy outlined in Section II, this section transforms those strategies into a very specific set of action activities and tasks according to recovery phases.

The three recovery phases in the company's BCMP shall be:

- a. Phase I: Disaster Occurrence
- b. Phase II: Plan Activation
- c. Phase III: Transition back to Head Office-Primary Site.

Each activity shall be assigned to one or more of the recovery teams. Each activity shall have a designated team member who has the primary assignment of completing the activity.

The tasks are numbered sequentially within each activity, and this is generally the order in which they would be performed:

##### **PHASE I: Disaster Occurrence**

##### **I. ACTIVITY: Emergency response**

Emergency response activities shall be carried out after a disaster. The activities shall be performed at a designated location at the Head Office. The BCRT shall be responsible for all employees in a disaster situation.

##### **TASKS:**

- a. After a disaster occurs, the BCRT shall quickly assess the situation to determine whether to immediately evacuate the building or not,



depending upon the nature of the disaster, the extent of damage, and the potential for additional danger.

**Note:** If the Head Office is totally lost, not accessible or suitable for occupancy, the remaining activities shall be performed from the DRS, after ensuring that all remaining tasks in each activity have been addressed.

- b. Quickly assess whether any personnel is injured and need medical attention. If the BCRT are able to assist them without causing further injury to them or putting themselves in further danger, then they shall provide the needed assistance and also call for help. If further danger is imminent, then the building shall be evacuated immediately.
- c. If appropriate, the building shall be evacuated in accordance with the building's emergency evacuation procedures.

### **Building's Emergency Evacuation Procedures.**

In the event of emergency evacuation, employees are required to:

- i. Use the nearest stairs.
- ii. Disable the biometric door lock by breaking the green box by the side of the door if not opened already.
- iii. Assemble at the designated **MUSTER POINT** outside of the building.

The expected evacuation time shall be 3 minutes.

Evacuation test during fire drills shall be used for performance evaluation.

- iv. A head count is conducted by Head of Corporate Resources. This is important to ensure that all employees are accounted for. *See appendix F for details.*

**II. ACTIVITY: Notification of Management**

The BCRT leader or any of its Members shall have the responsibility to inform Executive Management and all employees about the disaster. The notification shall be done through any possible means of communication such as telephone calls, emails, sms alert, WhatsApp, Telegram etc.

**TASKS:**

- a. Team leader of BCRT or any of its Members shall inform Executive Management and Staff
- b. Depending on the time of the disaster, staff shall be instructed on what to do (i.e. whether to stay at home, report at the DRS, etc.).

**III. ACTIVITY: Damage Assessment**

The Damage Assessment at the Head Office shall be carried out by the BCRT.

**TASKS:**

- a. The BCRT shall determine the scope, responsibilities and tasks to be performed in the Preliminary Damage Assessment Report.
- b. The BCRT may request for assistance from responsible government agencies in performing the Preliminary Damage Assessment.
- c. The BCRT shall caution all personnel to avoid safety risks as follows:

- i. Enter only areas that are permitted to staff.
  - ii. Ensure that all electrical power supplies are cut off from any area or equipment that could pose a threat to personal safety.
  - iii. Ensure that under no circumstances shall power be restored to computer equipment until the comprehensive damage assessment has been conducted, reviewed, and authority to restore power has been expressly given by the Executive Management.
- d. BCRT shall ensure that the team members do not alter equipment configurations until official approval is given by the Executive Management.
- e. The BCRT Leader shall deliver the preliminary damage assessment status report immediately upon completion.
- f. He shall facilitate the retrieval of items such as contents of file cabinets, Gubabi fire-proof cabinets, petty cash box, security codes, network backup tapes, etc, needed to conduct the preliminary damage assessment.
- g. He shall ensure that administrative support is available, as required.
- h. BCRT shall arrange a meeting with the Executive Management Team and Heads of Department to review the disaster declaration recommendation that results from the preliminary damage assessment and to determine the course of action to be taken thereafter.

#### IV. **ACTIVITY: Declaration of a Disaster**

It is the responsibility of the Executive Management to declare a disaster as recommended by the BCRT from the Preliminary Damage Assessment Report.

#### **TASKS:**

- a. Actual declaration of a disaster shall be made by the Executive Management Team, after consulting with BCRT. HOD's and other Staff shall wait for notification from the BCRT that a disaster has been declared and that Business Continuity Plan has been activated.
- b. The person contacted shall verify that the caller is someone who is authorized to do the notification.
- c. The person contacted shall notify other departmental staff, if they have not yet been contacted.
- d. In the event that the Executive Management cannot be assembled or reached, the Team Leader of the BCRT in-conjunction Heads of Departments shall assemble, gather appropriate information, consult with Management Staff, and make the decision on whether to declare the disaster.
- e. No individual staff shall unilaterally make a decision to declare a disaster. This is the responsibility of the Executive Management.

## **PHASE II: Plan Activation**

### **I. ACTIVITY: Notification and Assembling of Recovery Teams and Employees**

The notification and assembling of recovery teams and employees is the responsibility of BCRT. The team shall ensure that the DRS is functional.

#### **TASKS:**

- a. The team leader of the BCRT shall instructs Recovery Teams on what time to assemble at the DRS.
- b. The BCRT shall contact employees who perform critical functions to assemble at the DRS. *See Appendix H Critical Processes, Application and Staff.*
- c. ITRT and employees who perform critical functions shall move to the DRS.
- d. Employees that perform critical functions shall proceed to the DRS once it becomes obvious. This is to avoid negative impact on FCMB Pensions ability to recover critical services that may occur when there are delays in direct communications.

**II. ACTIVITY: Relocation to the DRS.**

The relocation to the DRS shall be the responsibility of CRT. Transportation and other logistics shall be provided by the CRT. The primary recovery activities at the DRS shall be to ensure that seamless services are offered to our esteemed customers.

**TASKS:**

- a. The BCRT Leader shall instruct the CRT to make arrangements to commute critical employees to the DRS.
- b. The CRT shall consult with the BCRT if access can be gained to the Head Office-primary site to retrieve vital records and other materials. The CRT shall only be allowed access to the primary site if the BCRT grants access. This shall be dependent upon the nature of the disaster and the extent of damage.
- c. If the vital material is small, they shall be given to employees to carry along with them to the DRS. If the material is large, then CRT will make arrangements for transport services and/or overnight courier services.

**III. ACTIVITY: Sitting Arrangements at the DRS**

It shall be the responsibility of CRT to ensure that employees are transported to the DRS and that they seat in the pre-arranged manner according to the distribution list below:

**Table 6: Computer distribution list at DRS**

<b>S/n</b>	<b>Department</b>	<b>Number of staff</b>
1	Financial Control	3
2	Benefits Administration	3
3	Investment	2
4	Operations	7
5	Business Development	1
6	Compliance	1
7	Internal Audit	1
8	Corporate Resources	1
9	Risk Management	1
10	Corporate Strategy and Communication	1
11	Client Services	1
	<b>Total</b>	<b>22</b>

**TASKS:**

- a. On arrival at the DRS, the CRT shall ensure that staff fills in the attendance register.
- b. The CRT shall accompany staff to the respective cubicles as already mapped on the desktop according to departments.
- c. The team shall determine flexible working schedules for staff to ensure that customers and business needs are met. This may require that some employee's work on staggered shifts or may need to work evening or nightshifts and weekends.
- d. The team shall gather vital records and other materials that were retrieved from the Head Office and determine appropriate storage locations.

**IV. ACTIVITY: Establishment of Communications with Customers and other Stakeholders.**

It shall be the responsibility of BCRT and ITRT to perform this activity.

**TASKS:**

- a. ITRT shall reroute telephone communications to the DRS.
- b. ITRT shall ensure that Head Office phone numbers are transferred to the DRS.
- c. BCRT shall give directions on how customers shall be notified.
- d. BCRT shall provide the staff with scripts and guidance on how to discuss the disaster with customers and other stakeholders in order to provide assurance on their confidence in FCMB Pensions.

*See appendix H: Information Cascade System*



### **PHASE III: Transition back to Head Office-Primary Site.**

i. **ACTIVITY: Relocation to the primary site. i.e. Head Office.**

After the unforeseen incident and the Head Office have been restored; it is the responsibility of the Executive Management and the BCRT to see to the successful restoration of services and relocation to the Head Office.

**TASKS:**

- a. The BCRT shall coordinate the ITRT and CRT relocation to the primary site, i.e. Head Office.
- b. ITRT shall ensure the restoration of all IT and Systems solutions from the DRS to the Head Office.
- c. ITRT shall verify that data communications are rerouted accordingly.

ii. **ACTIVITY: Termination of DRS Procedures**

The BCRT shall establish that the Primary Site, that is the Head Office functions have been fully restored as it were prior to the incident.

**TASKS:**

- a. The BCRT shall determine when to suspend or discontinue operating procedures at the DRS.
- b. The BCRT shall communicate the changes in procedures to all affected staff.
- c. The BCRT shall determine if additional procedures are needed upon return to the Head Office.

iii. **ACTIVITY: Relocating Personnel, Records, and Equipment to Primary Site i.e. Head Office.**

The Corporate Resources Team shall be responsible for relocating personnel, records, and equipment back to the Head Office.

**TASKS:**

- a. In conjunction with other teams the CRT shall be responsible for relocating staff to the Head Office based on an approved schedule by Executive Management.
- b. The CRT shall communicate this schedule to all staff.
- c. The CRT shall take inventory of critical records, equipment and other materials which need to be transported from the DRS back to the Head Office.

## 5. **Section V: Plan Testing.**

Disaster recovery testing helps ensure that the FCMB Pensions can recover data, restore business critical applications and continue operations after an interruption of services at the Head office. The test exercise shall be carried out bi-annually.

### I. **Disaster Recovery Testing**

Test of critical activities shall be carried out at DRS by departmental representatives. The departments and critical activities to be tested shall be as follows.

#### a. **Fund Accounting**

**Critical Activities:** Valuation of Funds, download of bank statement, call-up shared drive/work file and send instructions to the custodians.

#### b. **Benefit Administration**

**Critical Activities:** Call up Benefit Tracker – Upload benefit tracker, call up Empower application, access the company's network drive, e-mail access to PenCom, instruction to custodians, fund movement, access to DocuWare application and generate Standard Notice of Retirement.

#### c. **Business Development Department**

**Critical Activities:** Call up departmental files, access EnPower application to print customers PINs/RSA statements, generate schedule, access to PenCom website for employer code and access shared folder on company's network.

d. **Operations Department**

**Critical Activities:** Capture a new RSA form – Enrollment, data recapture, PIN generation, call up EnPower application, make a demo chat communication, demonstrate movement of RSA holders from one fund to another fund, process contributions, access RSA contributions for the day, access RSA statement and update of forms.

e. **Legal Department**

**Critical Activities:** View shared folders on the company's network.

f. **Investment Department**

**Critical Activities:** Carry out trading, access FMDQ- Pen Dealer; call up departmental folders, access E-mails and access Moneytor Plus application.

g. **Compliance Department**

**Critical Activities:** View shared folders on the network, access to EnPower and access DocuWare.

h. **Internal Audit**

**Critical Activities:** Call up IBS/Business Intelligent Software, access to DocuWare, call up EnPower, reconcile accounting unit, view shared folders on the company's network and access CTS Validator.

i. **Corporate Resources Department.**

**Critical Activities:** Call up departmental files, Prepare demo payroll, call-up Sage payroll application and demonstrate LPO in Sage.

j. **Company Account**

**Critical Activities:** Post transactions into the Sage application, view shared folders and check report on FCMB platform.

k. **Risk Management Department**

**Critical Activities:** View shared folders, call up Moneytor Plus and EnPower applications and access DocuWare.

II. **Scenarios Based Plan Test**

Apart from the general plan test we shall also consider scenario based plan test. This will be based on scenario events as highlighted in the scope of the BCMP or as may be determined from time to time.

III. **Established Responsibilities**

Specific responsibilities in respect of the BCMP and testing the disaster recovery shall be assigned to the following departments:

a. **Head Risk Management Department Responsibilities**

The Risk Management Department shall be responsible for:

- i. Periodically reviewing the adequacy and appropriateness of the company's Business Continuity Management Plan.
- ii. Coordinating and supervising the disaster recovery test.
- iii. Keeping BCRT current on the disaster recovery test report.
- iv. Communicating all BCMP changes to the BCRT.

b. **Head Corporate Resources Department Responsibilities**

The Corporate Resources Department shall be responsible for:

- i. Coordinating logistics of evacuating staff to the disaster recovery site
- ii. Ensuring the safety of company's assets at the disaster recovery site
- iii. Keeping the DRS clean at all times.

c. **Head IT and Systems Department Responsibilities**

The Head IT and Systems Department shall be responsible for:

- i. Keeping and updating the company's IT Disaster Recovery Plan as the need arises.
- ii. Providing technical support to staff during disaster recovery testing.

## **6. Section VI: Appendices**

**Appendix A- List of Vendors**

**Appendix B- Risk Assessment**

**Appendix C- Business Impact Assessment**

**Appendix D- Executive Management and Recovery Teams**

**Appendix E- DRS Inventory- Hardware, Software, Equipment and Furniture**

**Appendix F- Building Evacuation Instructions**

**Appendix G- Emergency Contact Telephone Numbers.**

**Appendix H: Critical Processes, Application and Staff.**

**Appendix I: Information Cascade System (Notification Tree).**

**Appendix J: Crisis Management Reporting Template.**

## Appendix A- List of Vendors

S/No	LIST OF VENDORS	CONTACT	PHONE NUMBER	SERVICE PROVIDED
1.	Foxfire Limited	Tabs Odukwe	08028801602	Electrical Power
2.	Chuks Azogu & Co	Chuks Azogu	08187206558	Sage Evolution
3.	Realtech Business Solutions	Yetunde Adeleye	08059194415	Dynamics NAVISION
4.	Jugenic Consult	Eugene Odiaga	08037273663	Docuware
5.	Simplex Business Solution Limited	Femi Adeniyi	08022235852	IBS and Business Intelligent.
6.	Staunch Technologies Limited	Mcumar Abdulraham	08060509183	Domain Hosting and Mobile App.
7.	Direct on Data DoD	Amodu idowu	08129999188	Backup Internet ISP
8.	Intuitive Technology Service INTL	Gbolade Adewole	08023193959	IVR Solution/Legend CRM
9.	Vodacom Business Nig	Sonia Dodo	08173349057	Primary Internet ISP.
10.	Accord Customer Care Solution (ACCS)	Folarin Banigbe	08035200347	Data Domain/EMC Networker
11.	TISV Digital Limited	Olowojoba Omotolani	07045555908	Website Maintenance
12.	Airtel Networks Limited	Joana Kay-Olawale	08022228022	Intercom and CUG
13.	TRANEX Plc	Henrietta Onyeador	09074272075	Courier Services
14.	Pacific Solution and Technology	Practul Kamar	08050693333	CYBEROAM
15.	Copworks Limited	Joy Rowland	09098301599	Penetration Testing
16.	Soft Solutions Concept Limited	Ayorinde Banjo	08020923914	HR SOFTWARE (HR WORKPLACE)



## Appendix B- Risk Assessment

### Risk parameters and Interpretation

Probability	
Rating	Descriptive
5	Will Happen
4	Likely to Happen
3	Might Happen
2	Unlikely to happen
1	Not Expected

Impact	
Rating	Descriptive
Red	Catastrophic
Amber	Significant
Yellow	Minor
Green	Negligible

S/N	Risk Type	Probability	Impact Rating
1	Fires	2	Amber
2	Floods	1	Red
3	Earthquake	2	Amber
4	Volcanic Eruption	2	Amber
5	Lightning and Thunderstorm	1	Amber
6	Windstorm, Tornadoes and Hurricane	1	Red
7	Snow and Ice Storm	1	Red
8	Pandemic	1	Red
9	Terrorist/Insurgency Attack	2	Red
10	Power Loss	2	Red
11	Kidnapping and Ransom	2	Red
12	Damage to reputation and Brand	2	Amber
13	Politics /Office Inaccessible	2	Amber
14	Cyber security	2	Red
15	Privacy and Security of Data	2	Amber
16	Loss of critical Data-Empower, Moneytor and Sage Evolution	1	Yellow
17	Loss of data center	1	Yellow
18	Loss of Network Communication	2	Red
19	Loss of key service providers	1	Yellow
20	Loss of office building	2	Red
21	Loss of human Life	1	Red

## Appendix C- Business Impact Assessment

Business Impact Assessment				
Quantitative Loss	Description	RTO Categories	RPO Categories	Financial Impact Estimate =N=
Loss Revenue	This is disruption of the business process/activity that impacts the revenue stream of FCMB Pensions as the company cannot service its customers.	1. 0-24 Hours 2. 1-48 Hours or Less 3. 2-5 Days and Less 4. 3-Greater than Five Days	1. No Data Loss 2. Less than Four Hours Data Loss 3. 24 Hours Data Loss	8.4 17m 42m 42m plus 8.4m daily.
Increase in Operating Expenses	The disruption of the business/activity will increase the FCMB Pensions day- to- day operating costs.	1. RTO0-24 Hours 2. 1-48 Hours or Less 3. 2-5 Days and Less 4. 3-Greater than Five Days	1. No Data Loss 2. Less than Four Hours Data Loss 3. 24 Hours Data Loss	3.5m 7m 17.5m 17.5m plus 3.5m daily
Penalties, Fines, Sanctions	The disruption of the business process/activity will impact the ability of FCMB Pensions to meet business, financial, performance/regulatory obligations leading to potential penalties, fines and/or sanctions.	1. 0-24 Hours 2. 1-48 Hours or Less 3. 2-5 Days and Less 4. 3-Greater	1. No Data Loss 2. Less than Four Hours Data Loss 3. 24 Hours	100,000 102,0000 105,000

		than Five Days	Data Loss	105,000 plus 1,000 daily
Loss of productivity	The disruption of the business process/activity will impact FCMB Pensions employees' ability to continue day - to- day operations, requiring the company to pay for time not being worked.	1. 0-24 Hours 2. 1-48 Hours or Less 3. 2-5 Days and Less 4. 3-Greater than Five Days	1. No Data Loss 2. Less than Four Hours Data Loss 3. 24 Hours Data Loss	2.7m 5.4m 27m 27m plus 2.7m daily.
<b>Qualitative Loss</b>				
Customer Service & Loyalty	Loss of the business process /activity that will impact FCMB Pensions ability to service the customer and customer loyalty to the company.			
Operations and other Services Impact	Disruption of the business process/activity that will impact FCMB Pensions routine operations and services, causing delays in one or more parts of the business.			
Public Goodwill, Image & Reputation	The disruption of the business process/activity will impact FCMB Pensions public confidence and trust in the company.			
Employee and Customer Safety & Security.	Disruption of the business process /activity that will impact FCMB Pensions safety and security of employees and customers.			

## Appendix D- Executive Management and Recovery Teams






S/N		MEMBERS	NAME	PHONE NUMBERS
1	EXECUTIVE MANAGEMENT	MD/CEO	Christopher .B. Bajowa	08033023844
		ED BUSINESS DEVELOPMENT AND INVESTMENT	Mai Moustapha Muhammad	08023580099
2	BUSINESS CONTINUITY RECOVERY TEAM (BCRT)	HEAD FINANCIAL CONTROL	Lawrence Keshiro	08034143496
		HEAD OPERATIONS	Segun Ogunsanya	08141233107
		HEAD IT AND SYSTEM	Lukman Yusuf	08037817002
		HEAD INVESTMENT	Olatunji Odesanya	08060867912
		HEAD RISK MANAGEMENT	Benedict Ohiovbeunu	08020637150
3	INFORMATION TECHNOLOGY RECOVERY TEAM (ITRT)	HEAD IT AND SYSTEMS	Lukman Yusuf	08037817002
		SYSTEMS ADMINISTRATOR	Thompson Ugbo	08050562074
		DATABASE ADMINISTRATOR	Timothy Agbele	09038853016
4	CORPORATE RESOURCE TEAM (CRT)	COMPANY SECRETARY	Halima Umar	08077814774
		HEAD COMPLIANCE	Olalekan Fadimine	08038898651
		HEAD CORPORATE RESOURCES	Victor Odumodu	08033385377
		HEAD ADMIN	Bashir Lawal	08069591343

### Appendix E- DRS Inventory-Hardware, Software, Equipment and Furniture

S/N	NAME	TYPE	TOTAL
1	HP Blades Servers	Hardware/Server	3
2	HP Desktop Computers , Key boards and Mouse	Hardware	20 Set
3	EMC Data Domain	Hardware	1
4	HP Tape Recorder	Hardware	1
5	EMC Networker	Software	--
6	Ms Exchange	Software	--
7	Moneytor/IBS	Software	--
8	EnPower	Software	--
9	DocuWare	Software	--
10	Sage (Evolution and HR)	Software	
11	SAN Storage	Hardware	1
12	CISCO Switches	Hardware	2
13	FM 200 Fire Extinguishers	Equipment	1
14	Air Conditioners	Equipment	6
15	Table workstation cubicles	Furniture	20
16	Office Table	Furniture	1
17	Office Chairs	Furniture	21

18	Fire Extinguishers	Equipment	2
19	Stabilizer	Equipment	1
20	Luminous Inverter Batteries	Equipment	8
21	Inverter	Equipment	1
22	Cameras	Equipment	3
23	Temperature Gadget	Equipment	1
24	Vodacom Router	Equipment	1
25	Uninterruptable Power Supply (UPS)	Equipment	1
26	Gubabi Fire-Proof Cabinet.	Equipment	1

## Appendix F- Building Evacuation Instructions-Fire Incidence.

S/N	SIGNS	DETAIL
1		<p>Any person discovering a fire should:</p> <ul style="list-style-type: none"> <li>• Raise the alarm to alert occupants to escape.</li> <li>• Evacuate the building.</li> <li>• Do not panic.</li> <li>• Close all doors behind as you leave; this will delay the spread of the fire.</li> </ul>
2		<ul style="list-style-type: none"> <li>• Never try to pick up valuables or possessions.</li> <li>• Do not pull or push others.</li> <li>• Do not run but work out quickly, smartly and calmly.</li> <li>• Use the nearest stairs.</li> <li>• Fight the fire with any available fire extinguisher.</li> </ul>
3	 <p><small>shutterstock.com • 1428431288</small></p>	<ul style="list-style-type: none"> <li>• Follow the emergency exit nearest to you.</li> <li>• Assemble at a designated MUSTER POINT</li> <li>• Make roll call to ensure no one is left in the building.</li> <li>• Call for the fire service immediately.</li> </ul>
4		<ul style="list-style-type: none"> <li>• Never go back to the building until declared safe to do so by the BCP Coordinator.</li> <li>• Offer any assistance if possible and necessary.</li> </ul>
5		<p>EMERGENCY LINES ARE 09-2906118 OR 112</p>

### Appendix G- Emergency Contact Telephone Numbers.

S/N	Government Agency	Contact Address	Telephone Number
1.	Nigeria Emergency Management Agency (NEMA)	8 Ademola Adetokunbo Crescent Maitama Abuja	08022556362
2.	FCT Fire Service	Mohammadu Buhari way Area 10 Garki Abuja	08032003557 07003283473 09-2906118 09-6711371
3.	Nigeria Police	Shehu Shagari Way Force Headquarters Louis Edet House Central Business District, Area 11, Abuja.	08038305707 092340898 092341709 092340756 07057337653 08061581938 08032003913
4.	PenCom	174 Adetokumbo Ademola Crescent wuse 2, Abuja.	0700-225-573-6266 +234-94603930.
5.	a)UBA Pensions Custodian Limited	3 <sup>rd</sup> Floor, Plot 22b, Idowu Taylor Street VI, Lagos	+234-1-2702627.
	b)Zenith Pensions Limited Custodian	Civil Tower (4 <sup>th</sup> and 5 <sup>th</sup> Floors) Ozumba Mbadiwe Road VI, Lagos.	+234-1-2712793.



## Appendix H: Critical Processes, Application and Staff.

	Critical Process	Critical Application	Critical Staff	Phone Number	Back up staff	Phone Number
1	Enrolment Processing	Enpower	Malachy Aniuha	08032670347	Sufyan Abdulrahman	08031521521
2	Contribution Processing	Enpower	Suleima Yusuf	08032798577	Adaeze Okoli	07038015995
3	Contribution Reconciliation	Enpower	Omolara Oyekanmi	08033016453	Friday Musa	07067305015
4	CRM/Schedule and Collection Unit	Schedule and Funding File	Ibikemi Adetoye	07017365507	Harira Yuguda	08039146070
5	Benefit Administration: <ul style="list-style-type: none"> <li>• Lump sum Programmed Withdrawal and Refunds</li> <li>• Death benefit, 25% and other payment</li> <li>• Document Management unit</li> </ul>	Enpower	<ul style="list-style-type: none"> <li>• Caleb Ndackson</li> <li>• Leah Ajiboye</li> <li>• Ruth Okpara</li> </ul>	<ul style="list-style-type: none"> <li>• 08095494979</li> <li>• 08051129708</li> <li>• 08059580002</li> </ul>	<ul style="list-style-type: none"> <li>• Yusuf Agabi</li> <li>• Iyanuoluwa Loyinmi</li> <li>• Fatima Sadiq</li> </ul>	<ul style="list-style-type: none"> <li>• 08033736396</li> <li>• 07031591473</li> <li>• 08095559412</li> </ul>
6	Investment	IBS Moneytor plus	Maryam Odewale	07032727667	Ugwoke Somtochukwu	07038249055
7	Fund Accounting	IBS Moneytor plus – General Ledger ( GL)	Ali Mansur	08034411925	Edidiong Sunday	07030574160
8	Company account and payroll	Sage Evolution	Abiodun Akande	08139029555	Rahila Fakorede	08103730182
9	E-mail Services	Microsoft Exchange	Thompson Ugbo	08050562074	Akeem Ahmed	08053418543
10	Database Administration	Database	Timothy Agbele	09038853016	Oyinkansola Oyefunmibi	07041119278

11	Corporate Strategy and Communication	Enpower Benefit Tracker CTS Validation Olikview Legend Content Management System	<b>Corporate Strategy</b>  Marvin Silong	08033380225	<b>Corporate Communication</b>  Bimpe Enoyi	08036434666
12	Customer Services	Enpower Legend Enrolment Login	Joy Olorundare	09099660125	Oluwaseun Onipede	07033275492

## Appendix I: Information Cascade System

