Business Continuity Plan

Version 02 (SSBCP/0001)
August-2025

SPAR Health (Pty) Ltd. incorporates the following Subsidiaries:

Company Name	Registration Number
S Buys (Pty) Ltd.	1993/001280/07
Malan and Buys (Pty) Ltd.	1997/014298/07
Forefront Info (Pty) Ltd.	1997/014968/07
S Buys Academy (Pty) Ltd.	2001/023449/07

Table of Contents

TITLE / APPROVAL PAGE

Prepared:

Ina Barkhuizen – Legal Representative

Date:

01 August 2025

Signature

Madeleine Malan – Executive Manager

01 August 2025

Signature

The review indicates that quality persons from operational areas have reviewed the content for accuracy, clarity, and the ability to implement it as written.

Reviewed:

Gerry Muller – IT Manager

Date:

01 August 2025

Signature

Dean Jacobs – Maintenance

01 August 2025

Signature

Approval indicates appropriate personnel participated in preparation and review, and that the content is aligned with organization objectives.

Approved:

Jeremy Nicol – Managing Director

Date:

01 August 2025

Signature

REVISION HISTORY

Revision	Description of Change	Author	Effective Date
01	Initial Release (SPAR Health Group)	Ina Barkhuizen & Madeleine Malan	1 July 2024
02	Formatting changes and numbering. Included Clause 2: RACI Matrix; Clause 8.8: Emergency Situation (Refer to existing crisis management plan); Clause 9: Emergency Response and Recovery Procedures; Clause 10: Mitigation of Financial Losses.	Ina Barkhuizen & Madeleine Malan	01 August 2025

1. INTRODUCTION/EXECUTIVE SUMMARY

This BCP establishes procedures and responsibilities to ensure that the organisation can respond effectively to disruptions, safeguard stakeholder interests, maintain critical services, and recover to full operations within acceptable timeframes.

1.1 Information Technology (IT)

The Information Technology (IT) was identified as critical for the Holding Company and its subsidiaries to conduct its business with the minimum disruption perceived by clients, patients, and stakeholders.

Information Technology (IT) includes many components such as networks, servers, desktop and laptop computers, and wireless devices. The ability to run both office productivity and enterprise software is critical.
Servers (either physical or virtual) running SQL Server, have their databases backed up to disk on a Symantec Backup Exec Media Server on a daily basis, should a situation arise where only a database needs to be restored not an entire server. Those servers in turn are also backed up in their entirety, virtual or physical:

- All Virtual Servers are backed up to a Symantec Backup Exec Media Server on LTO Media;
- All Physical Stand-Alone Servers are also backed up to LTO media via Symantec Backup Exec;
- Symantec Backup Exec Servers run Full Backups on each backup run and send detailed success or failure reports to IT staff after each run.

Restoration tests are carried out on a fortnightly basis on all servers. Further to that, hypervisors are left with enough capacity on them to host critical servers on opposing Hypervisors, should a hypervisor fail.

1.2 Power Outage

A power outage plan is important to outline how the business will continue to operate in the event of a power outage. It includes procedures for everything from backup power generation to customer communication.
This plan can help to minimize the impact of unexpected downtime. It can also help to keep customers and employees safe and mitigate the financial losses that can occur when business is interrupted. Power outages can also damage equipment, this plan must assist in protecting the company's investments.
The process of creating and implementing a BCP may reduce the impacts of infrastructure disorder and associated supply chain disruptions. Business continuity preparedness can prevent unnecessary downtime, increase recovery efforts, and protect the financial bottom line.

1. **Key elements of the Power Outage Continuity**
   i. List of critical systems and processes that need to be maintained during a power outage.
   ii. List of backup power generation options, including generators and battery backups.
   iii. Protocol for customer communication, including contact information for key customer service personnel.

iv. Protocols for employee safety, including evacuation procedures.
v. A plan for mitigating financial losses, including insurance coverage and contingency funds.
vi. A plan for recovering lost data and files.
vii. Supply chain/data switching robustness during power outage periods.

2. Power Outage Continuity

2.1 Critical systems and processes that need to be maintained during power outages:

i. All IT software systems (main server) and well as all the electronic switching mechanisms should remain active;
ii. Hardware such as printers and various PCs that are used for data capturing, daily operational/order processing, invoice picking and scanning, parcel dispatch processes as well as the administrational and operational processing of service level agreements and student registrations;
iii. The walk-in cold rooms and well as the walk-in freezer rooms should always have electricity available to ensure that the product cold chain can be maintained at all times;
iv. The facility air-conditioner to ensure that ambient warehouse storage areas remain under the required storage temperature of 25°C;
v. The facility temperature monitoring system should remain active to ensure that the required temperature is maintained;
vi. The security system (both alarm system and cameras) needs to be maintained and fully functional at all times to secure the inventory;
vii. Company switchboard should remain active to ensure that customer inbound and outbound calls can be made and calls recorded; and
viii. Facility lights need to have power to ensure that normal working processes can be performed.

2.2 Back-up Power Generation options available in the Company:

i. SPAR Health Pharmacy at SPAR Distribution Centre including all its subsidiaries is situated in Carletonville and has 2 diesel generators, one large generator that is able to provide electricity to the total building and all the relevant equipment in all departments (CAT generator, 490kW; 1500rpm) as well as a smaller back-up generator (VOLVO, 183kW; 1500rpm).
ii. In addition to the 2 generators, the Distribution Centre is also equipped with a 3 phase 30Kva UPS that is able to provide power (for a maximum period of 15 to 20 minutes) to all the company's computers, printers as well as the servers during the change-over period between ESKOM and the generators. The Server room has an additional 10Kva UPS that can maintain electricity to the server and network equipment for about 45 minutes to an hour to ensure that emergency shutdowns can be performed when required;
iii. Regular maintenance needs to be performed on the generators as well as the UPS systems to ensure that these units are in an optimal functioning condition at all times. Automatic changeover processes should be checked to ensure that changeover will happen without any problems when a power outage occurs;
iv. Preventative maintenance must be carried out on the generator by qualified technicians at intervals of 100 hours of run time under load. The generator

monitoring and information console will indicate the current run time of the generator and the time remaining untill the next maintenance interval;

v. Weekly automated scheduled start-ups and runs under no load conditions must be carried out to ensure that the generator is mechanically sound, and able to auto start and auto shutdown. Any failures or errors during this process should be SMSed via the generator monitoring console to the general factotum and IT personnel so that corrective action can be taken;

vi. Weekly inspection of the generator's battery water levels, oil level, and diesel level must be carried out. Any shortfalls of any of these readings should be corrected immediately;

vii. A daily inspection of the starting state of the generator must be carried out to verify that the generator is in an auto-start state and not a manual start or offline state;

viii. A weekly review of the 30Kva UPS's warning and error log must be carried out to verify that the UPS is operating correctly without errors or under detrimental conditions. If any serious issues are identified in the logs, the relative UPS distributor must be alerted and request a technician to be dispatched;

ix. The area surrounding the UPS must be cleaned weekly and kept free of debris and dust. During periods of rain, the surrounding area should also be inspected for water leaks. Any water leaks must be reported to the general factotum and addressed immediately;

x. Annual servicing and inspection of the UPS must be arranged with the relative UPS distributor;

xi. A sufficient supply of diesel is essential to ensure that the backup generators can provide power during extended periods of power supply outage. The diesel levels of the generators must be monitored continuously by the head of maintenance of the SPAR Health Pharmacy at SPAR Distribution Centre to ensure that the generators never run out of diesel. Special arrangements need to be made with local fuel stations to ensure that diesel will be reserved for the distribution centre during periods of power outage.

3. **Customer Communication:**

i. It is essential that the Company and its subsidiaries ensure that communication will be maintained with customers during extended periods of power outage.

ii. The telephone infrastructure is safeguarded from power outages by the same backup power systems that safeguard the IT infrastructures and server room i.e CAT Generator in turn backed by the Volvo Generator, with a UPS carrying the switchover loads.

iii. The telephone system is VoIP driven and as such the main fibre link is backed by a 'microwave to fibre' fail-over link should the main fibre link fail.

iv. In the event that the cell phone networks are experiencing outages, customers will be contacted via e-mail or 'data call' network options.

1.3 Water interruptions/outage

A water interruption/outage plan is important to outline how the business will continue to operate in the event of an interruption or outage.

It is critical to sustain the water supply to the company during water interruptions/outages. Water supply is not necessarily needed for the operation of the business but it is essential for purposes of health, safety and sanitation.

Ensure continuation of all water-saving interventions. Plan for minimum water demand to ensure that the focus remains on what is critical or not.
Determine the need for essential staff and non-essential staff required at the business premises. If the system cannot supply enough for all employees, the company will map out which functions are critical and which functions can be performed at home.
Develop a schedule of how and when essential staff could access their water allocation from the office.

1. **Key elements of Water Continuity**
   i. List of critical systems and processes that need to be maintained during a water interruption/outage;
   ii. List of backup water options, including storage of water in JoJo tanks, possible reuse of grey water and supply of water from a third party;
   iii. Protocols for employee safety;
   iv. A plan for mitigating financial losses, including insurance coverage and contingency funds; and
   v. Availability of water for fire control.

2. **Water Interruption/Outage Continuity**

2.1 Critical systems and processes that need to be maintained during water interruptions/ outages:

   i. All electronic switching and/or pump mechanisms should remain active in order to keep the supply of water for purposes of sanitation and not for consumption by employees.

2.2 Back-up water options available in the Company:

   i. The Company has installed a 70 000 Litre fresh water reservoir (water for human consumption). The reservoir is fitted with a 2.2 KW pressure pump to ensure consistent water supply to all tenants. The reservoir is filled with water directly from the municipal supply and feeds directly into the main water supply of the building. The water remains fresh and is constantly circulated and replenished. This reservoir is able to supply the entire building with fresh water for approximately a two week period.
   ii. In addition to the water reservoir the company is looking into the possibility of the reuse of grey water, alternatively we make use of a third party to supply water to the company as and when needed.
   iii. Regular maintenance needs to be performed on the electronic switching and/or pump mechanisms to ensure that these units are in optimal functioning condition at all times.
   iv. Preventative maintenance must be carried out on the water supply systems.
   v. Monthly scheduled runs under no water conditions must be carried out to ensure that the water supply systems are functional. Any failures or errors during this process should be reported to the maintenance manager so that corrective action can be taken.

vi. A weekly inspection of the caps/seals for water leaks on the tanks must be done. Any water leaks must be reported to the maintenance manager and addressed immediately.
vii. Annual servicing and inspection of the supply system must be arranged.

1.4 Security Measures and Evacuation Procedures

Security measures are integral to a business. The BCP must make provision for security measures in all departments to ensure the safety of the building and employees which includes prevention, detection, response, cybersecurity, firewalls, access control, security cameras, emergency response plans, security personnel, data encryption, recording of visitors in logbooks, fire extinguishers etc. The building is fitted with an alarm system that is connected to an armed response security company. Armed response is available during office hours should a security situation arise. The building is further enclosed with palisades of which the main gates can be locked if unauthorised people/protestors demand access to the private property.

Safety drills need to be practiced regularly in case of an emergency for staff to be aware of safety procedures and to remain as calm as possible.

The company has evacuation procedures in place in case of an emergency. The main entrance of the building is controlled by a security guard and electronically operated gates to minimise unauthorised access to the private property of the company.
The IT department also plays an important role in implementing security measures to safeguard the personal information of clients, patients, and stakeholders that is processed by the company.

1.5 Logistics

One of the key operational processes in the company is to ensure that the delivery of medicine to patients, healthcare facilities, and pharmacies are not interrupted.

1. **Key elements of Logistics Continuity**
   i. List of critical suppliers and alternative resources in the supply chain;
   ii. Transportation plans to adapt to changing circumstances;
   iii. Monitor and identify potential risks for late deliveries due to protests;
   iv. A plan for mitigating financial losses, including insurance coverage and contingency funds.

2. **Logistics Continuity**

2.1 Critical systems and processes that need to be in place during a disruption of delivery of medicine:

i. Alternative courier companies to be available to ensure that the delivery of medicine is not interrupted due to an unforeseen event of our current couriers not being able to deliver their usual service.
ii. Ensure clear communication with healthcare providers, facilities, patients, and pharmacies of any late deliveries including the circumstances of the delay.

2. BUSINESS CONTINUITY MANAGEMENT TEAM (BCMT)

2.1 **Purpose**

The BCMT oversees the implementation, testing, and continuous improvement of the BCP. It ensures that continuity measures align with the company's risk appetite and overall strategic objectives. These individuals are part of this team due to the positions they hold. The team meets annually or as per clause 6 of this BCP.

2.2 Roles and Responsibilities

- Chairperson (Jeremy Nicol)
  - Provides overall leadership during a disruption.
  - Authorises activation of the BCP.
  - Communicates with Board of Directors and regulators.

- BCM Coordinator (Madeleine Malan & Ina Barkhuizen)
  - Coordinates BCP implementation.
  - Maintains and updates the BCP documentation.
  - Organises training and testing exercises.

- IT Manager (Gerry Müller)
  - Manages data recovery, cybersecurity incidents, and IT continuity.
  - Oversees restoration of IT services within Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

- HR Executive (Sonica Spamers)
  - Manages employee communication, welfare, and reallocation of staff.
  - Ensures employee training and awareness.

- Logistics Manager (JC Coetzer) and Procurement Specialist (Desire van Lill)
  - Ensures continuity of supply chain and delivery.
  - Coordinates with alternative suppliers and couriers.

- Finance Executive (Dirk van Zyl)
  - Manages insurance claims and contingency funds.
  - Assesses financial impact and ensures timely reporting.

- Communications Officer (Jeremy Nicol)
  - Handles external communications.
  - Ensures stakeholders receive timely, accurate updates.

- Operation Managers of various entities – Wholesaler (Tommie Grobler), Scriptwise (Marisca van Zyl) and Academy (Jalia Meyer)
  - Ensures that business run as effective as possible and oversee that the actual premises & assets are kept secure.

3. RACI MATRIX (Incident Response)

Task	Chair-person	BCM Co-ordinators	IT	HR	Logistics & Procurement	Finance	Communi-cations	Operations
Declare Incident & activate BCP	*A*	*R*	*C*	*C*	*C*	*C*	*I*	*C*
Assess impact of incident	*A*	*R*	*C*	*C*	*C*	*C*	*I*	*C*
Restore IT services	*I*	*C*	*R*	*I*	*I*	*I*	*I*	*C*
Coordinate employee safety & relocation	*I*	*C*	*I*	*R*	*I*	*I*	*I*	*R*
Engage alternative suppliers/logistics	*I*	*C*	*I*	*I*	*R*	*C*	*I*	*C*
Manage insurance claims	*I*	*C*	*I*	*I*	*C*	*R*	*I*	*I*
Draft and send stakeholder updates	*I*	*C*	*I*	*I*	*I*	*I*	*R*	*I*

(*R=Responsible, A=Accountable, C=Consulted, I=Informed*)

4. AIM OF THE BUSINESS CONTINUITY PLAN (BCP)

This plan has been designed to prepare the company and its subsidiaries to cope with the effects of an emergency. It is intended that this document will provide the basis for a relatively quick and painless return to "business as usual" regardless of the cause.

The following scenarios have been identified for which one would have to plan the continuity of business:

- Loss of the use of facilities in the event of fires, extreme weather, vandalism (internal and external) etc.
- Inaccessibility of information and data (patient information and history, script data patient support information, schedules and billing);
- Unavailability of staff;
- Loss of technical resources such as hardware, software, Internet services and communication services;
- Power Outage;
- Water supply;
- Security Measures and Evacuation Procedures; and
- Logistics.

5. OBJECTIVES OF THE BUSINESS CONTINUITY PLAN

The objective of the BCP is to:

- Respond timeously and effectively to a disruptive incident (Incident management);

- Maintain delivery of critical activities/services during an incident (business continuity); and
- Return to 'business as usual' (resumption and recovery).

6. REVIEW AND TESTING OF BUSINESS CONTINUITY PLAN

In addition to an annual review, the company and the subsidiaries will review and modify the BCP:

- After each training drill or exercise;
- After each emergency or major incident;
- Whenever significant changes to personnel or their responsibilities;
- When the layout or design of the facility changes; and
- When key policies or procedures change.

Objectives of testing is to:

- Identifying gaps/weaknesses in the Business Continuity Plan;
- Validating and improving the BCP Strategy;
- Keeping the BCP Strategy updated;
- Confirming that your continuity objectives are met;
- Evaluating the company's response to various incidents;
- Improving systems and processes based on test findings;
- Meet compliance and regulator's requirements; and
- Helping reduce recovery time and cost.

The review of the BCP should involve higher-management as well as department heads to analyse and discuss potential improvements, and ensure contact information and recovery contracts are in place. The team should at least conduct a review on an annual basis to ensure it is effective. The focus of the review and test should be on identifying weak areas and accordingly implementing measures to strengthen them.

Testing should consist of:

1. **Business Continuity Plan Review**
   This involves higher-management as well as heads of departments. BCP should be reviewed. Potential improvements should be discussed, as well as making sure contact information is up-to-date, recovery contracts are still in place and effective, and applicable business continuity and disaster recovery scenarios are appropriately covered.
2. **Walk through of BCP**
   A walk-through promotes procedural awareness. A structured walk-through of the BCP with department heads and critical staff will make sure that key points of command and delegation points to internal teams know precisely what to do in an emergency.
   This includes the discussion of disaster scenarios, during which the potential response and procedures will be reviewed and ensure the responsibilities outlined are appropriately handled by the concerned authorities.
   After testing, department team leaders should discuss findings and then draft a unified report on plan efficacy and suggestions for improvement.
3. **Simulation Test**

Simulation Test incorporates actual recovery actions such as restoring backups, live testing of redundant systems, and any other relevant processes. In addition to critical personnel, any employees that would be involved in a BCP event should now be involved in the testing process. A Walk-Through Test may also include validation of response processes/systems, a simulated response at alternate locations, and varying degrees of actual notification and resource mobilization.

4. **Annual Tabletop exercises**
   Senior Management simulates scenarios to test decision-making.
5. **Annual Walkthroughs**
   Department heads ensure team familiarity with BCP.
6. **Post-test reporting**
   Each test followed by a written improvement plan with assigned responsibilities and timelines.

7. BUSINESS PRIORITIES PER SCENARIO

This section identifies the organisation's most urgent functions that must be recovered or maintained during a disruption. It prioritises these functions according to their importance for operational continuity and sets target timeframes for their restoration. The aim is to ensure that the business can respond effectively and in the correct order during emergencies.

What the table describes:
Scenario – a specific type of disruptive event.
Priority – The ranking of each function according to urgency (1 being most urgent)
Critical function – The essential operational task or service that must continue or be restored.
Timeframe – The target period within which each critical function should be operational again.

What the scenarios represent:
The eight scenarios outline different potential threats to operations (like facility inaccessibility) and specify the most urgent actions for each. They serve as a quick response reference to guide recovery efforts and allocate resources effectively.

Scenario 1: Inability to access the facility:

Priority	Critical function	Timeframe
1	Secure temporary facility & re-locate personnel	1 hour
2	Temporary IT set-up with laptops	1 hour
3	Communicate with all key clients regarding temporary arrangements	1 hour
4	Temporarily IT set-up with additional hardware	3-5 days

Scenario 2: Inability to access electronic information and data / Cyberattack

Priority	Critical function	Timeframe

1	Restore from secure back-ups	1 – 4 hours
2	Continue with day to day operations	30 min
3	Implement IT isolation protocols	30 min – 1 hour
4	Notify regulators (POPIA) and affected data subjects	1 – 8 hours

Scenario 3: Unavailability of Staff

Priority	Critical function	Timeframe
1	Allocation of prior trained employees	Immediately
2	Inform Clients with regard to unavailability of staff	Immediately
3	Train newly appointed or allocated employees	2-3 days

Scenario 4: Loss of Telecommunication

Priority	Critical function	Timeframe
1	Use of alternative telecommunication methods	1 hour
2	Inform IT corrective measures	1-4 hours

Scenario 5: Water Availability & Power Supply

Priority	Critical function	Timeframe
1	Activate Backup Generator /UPS	Immediate
2	Backup diesel in bowser for Generators	30 min
3	Initiate fuel supply agreements	30 min
4	Reduce non-critical load	30 min
5	Improve water efficiency / sanitation / cold storage	1 day

Scenario 6: Logistics

Priority	Critical function	Timeframe
1	List of alternative resources in the supply chain	1 hour
2	Use of alternative transportation company (courier) / reroute deliveries	1 hour

3	Back up diesel/petrol in tank for local deliveries	30 min

Scenario 7: National Epidemic / Disaster Announcement:

Priority	Critical function	Timeframe
1	Draft a plan	1 day
2	Communicate the plan to all stakeholders	1 hour

Scenario 8: Emergency situation whereby possible destruction of property (Looting & Civil unrest)

Priority	Critical function	Timeframe
1	Secure facilities with additional armed response	1 hour
2	Draft a plan	4 hours
3	Relocate staff/products to alternate safe premises	1 week
4	Maintain remote operations where possible	3 hours
5	Communicate the plan to all stakeholders	1 hour

8. CRITICAL FUNCTION ANALYSIS AND RECOVERY PROCESS

This section expands on the priorities identified in section 7 by detailing exactly how each critical function will be restored, who or what team is responsible, the resources required, and the specific recovery actions. It ensures that recovery steps are actionable, assigned, and measurable.

People driving this section:

Executive Managers – Overall decision-making and escalation.
Heads of Departments (HODs) – Operational coordination in their respective areas.
IT / Maintenance & Operational Managers – Technical, facility, and logistical recovery.
Program Managers/Coordinators – Communication with clients and internal teams.
Support Personnel – Assist in implementing recovery measures across departments.

What the detailed tables describe:

Responsibility – Who is accountable for the recovery of that function.
Potential Impact – The severity of the effect on the organisation if the function is disrupted.
Likelihood – The probability of the event occurring.
Total Recovery Timeframe – The overall maximum time expected to resume normal operations.
Priority – The urgency order in which recovery actions should be performed.
Resources Required – Staff, systems, equipment, and information needed to recover the functions.
Action Required – Specific steps to restore the function.
Recovery Timeframe – How long it should take to complete the recovery actions.

Purpose of these details:

By documenting responsibilities, required resources, and step by step actions, this section ensures that everyone knows their role, has access to what they need, and can execute recovery actions within predefined deadlines. This reduces confusion and improves the speed and effectiveness of the response.

8.1 Inability to access the facility

Scenario 1:	**Inability to access the facility**
Responsibility:	Executive Manager
Potential impact on organisation if interrupted:	Major
Likelihood of interruption to organisation:	Highly unlikely
Total recovery timeframe:	3-5 days

Priority: 1	**Critical function:**	**Secure temporary facility & re-locate personnel**
Resources required for recovery:		
Staff		Operational Manager
Data / systems / equipment		• Cell phone • Contact numbers for re-location facility

		• Contact numbers for personnel
Action required		• Secure temporary facility where personnel can be relocated to • Re-locate personnel to facility • Inform IT Manager of location of temporary facility
Recovery timeframe		2 hours
Priority: 2	**Critical function:**	**Temporary IT set-up with laptops**
Resources required for recovery:		
Staff		IT Manager
Data / systems / equipment		• Managers laptops • 3G dongle • Wi-Fi networks
Action required		Set up on SPAR Health VPN and Network Access.
Recovery timeframe		2 hours
Priority: 3	**Critical function:**	**Communicate with all key clients and patients regarding temporary arrangements**
Resources required for recovery:		
Staff		Program Manager and/or Coordinators
Data / systems / equipment		• Laptops • Pharmacy Systems • Program / Patient databases
Action required		• Listing of active patients to be generated from the patient database • SMS sent to inform about temporary arrangements for communicating with Scriptwise • Key clients to be informed telephonically and/or via email
Recovery framework		2 hours
Priority: 4	**Critical function:**	**Temporary IT set-up with additional hardware**
Resources required for recovery:		
Staff		IT Manager
Data / systems / equipment		• Desktops • Software • Printers • WIFI hot spot • Telephones

Action required	• Source hardware and noted above • Set up on SPAR Health VPN
Recovery time	3-5 days

8.2 Inability to access electronic information and data / Cyberattack

Scenario 2:	**Inability to access electronic information and data**	
Responsibility		HOD in every department
Potential impact on organisation if interrupted		Major
Likelihood of interruption to organisation		Likely
Total recovery timeframe:		1 – 3 hours
Priority 1	**Critical function:**	**Restore from secure Back-ups**
Resources required for recovery:		
Staff		IT Manager
Data / systems / equipment		Virtual servers and system back-ups
Action required		• Restoration of Back-ups
Recovery timeframe		1-3 hours
Priority 2	**Critical function:**	**Continue with day to day Operations**
Resources required for recovery:		
Staff		Support personnel
Data / systems / equipment		• Hard copy documents
Action required		All interactions capture manually on paper source documents and then transcribed into an electronic format suitable for analysis and reporting. In the event of a server being offline, staff will be able to continue manually and transfer the data into the database once the server is online again
Recovery timeframe		No interruption in service

	Re-capturing on restored database might take between 1-3 hours.
Priority 3	**Implement IT isolation protocols**
Resources required for recovery:	
Staff	IT Manager, Cybersecurity Specialist, HODs
Data / systems / equipment	Hyperivisors, VM Servers, Servers, Backups
Action required	• Disconnect compromised devices from network • Disable compromised user accounts and change all relevant passwords • Segregate affected servers and workstations
Recovery timeframe	Relative to magnitude of incident (1 hour – 1 day)
Priority 4	**Notify regulators (POPIA) and affected data subjects**
Resources required for recovery:	
Staff	Deputy Information Officer & Support personnel
Data / systems / equipment	• Laptops • SOPHOS • Patient/customer database • WIFI
Action required	Critical evaluation and description of the breach to draft a notice letter to affected individuals with the required elements and report online to the Information regulator.
Recovery timeframe	No interruption in service 1- 8 hours

8.3 Unavailability of staff

Scenario 3:	**Unavailability of staff**
Responsibility	HOD in every department
Potential impact on organisation if interrupted	Minor
Likelihood of interruption to organisation	Likely

Total recovery timeframe		1 day
Priority 1	**Critical function:**	**Allocation of a prior trained employee as temporarily measure**
Resources required for recovery:		
Staff		HOD in every department
Data / systems / equipment		Program Handover Checklist
Action required		• Review of Checklist to ensure that employee received all required training in order to continue with PSP or other program
Recovery timeframe		1 hour
Priority 2	**Critical function:**	**Inform key client with regard to temporarily arrangement**
Resources required for recovery:		
Staff		Staff in every department
Data / systems / equipment		• Email
Action required		Inform client with regard to the temporarily arrangements
Priority 3	**Critical function:**	**Train newly appointed or allocated employees**
Resources required for recovery:		
Staff		HOD of every department
Data / systems / equipment		• Program Handover Checklist • SOPs • Training Guides
Action required		All newly appointed or allocated employees to receive training prior to the start of participation with PSP or other programs
Recovery timeframe		2 – 3 days

8.4 Loss of telecommunication (Internet of phone)

Scenario 4:	**Loss of telecommunication (Internet or phone)**	
Responsibility		HOD in every department & IT Manager
Potential impact on organisation if interrupted		Major
Likelihood of interruption to organisation		Likely
Total recovery timeframe		1 hour
Priority 1	**Critical function:**	**Use of alternative telecommunication methods**
Resources required for recovery:		
Staff		All employees
Data / systems / equipment		Email / Fax machines / SMS / Phone calls
Action required		Certain processes are critical and can be disrupted if there no telecommunication available. This includes but is not limited to: • Reporting of adverse events or product complaints • Delivery arrangements Alternative communication channels to be used such as faxes and mobile phones.
Recovery timeframe		1 hour
Priority 2	**Critical function:**	**Inform IT for corrective measures**
Resources required for recovery:		
Staff		IT Manager
Data / systems / equipment		Email / Fax machines / SMS / Phone calls
Action required		Follow-up and correct reason for telecommunication failure. Assist with alternative measures.
Recovery timeframe		1-4 hours

8.5 Water availability & Power Supply

Scenario 5:	Water availability & Power Supply	
Responsibility		Maintenance Manager
Potential impact on organisation if interrupted		Major
Likelihood of interruption to organisation		Likely
Total recovery timeframe		1 hour
Priority 1	**Critical function:**	**Use of alternative methods of power: Generator/UPS**
Resources required for recovery:		
Staff		Maintenance & IT
Data / systems / equipment		Generators & UPS
Action required		Refer to paragraph 1.2 Use Alternative Power source for example, UPS and Generator to provide power to at least the mission critical equipment during extended power outages. Management should maintain an ample supply of fuel on hand and have arrangements for replenishment. It is also important to ensure alternative power supplies receive periodic maintenance and testing to maintain operability.
Recovery timeframe		Immediate
Priority 2	**Critical function:**	**Water Availability**
Resources required for recovery:		
Staff		Maintenance/Operations
Data / systems / equipment		JoJo Tanks
Action required		Refer to paragraph 1.3 Ensure continuation of all water saving interventions. Plan for minimum water demand to ensure that focus remains on what is critical or not.

	Determine the need for essential staff and non-essential staff required at the business premises. How many people can you supply for should the water mains be switched off (direct and sanitation use)? If the system cannot supply enough for all employees, map out which functions are critical and which functions can be performed at home. Develop a schedule of how and when essential staff could access their water allocation from the office. Ensure water security for fire safety -check that your fire extinguishers are in legal working condition. If possible, increase the number of fire extinguishers. Store and provide access to bottled drinking water for staff and clients. Water bottles allocated for Sanitation & basic Hygiene.
Recovery timeframe	1 day
Priority 3	Initiate fuel supply agreements
Resources required for recovery:	
Staff	Maintenance & Risk Managers
Data / systems / equipment	Supplier contract list, bowser compliance permit
Action required	• Contact fuel suppliers to confirm emergency • Activate standing fuel supply agreements • Confirm delivery or pick up schedule
Recovery timeframe	30 min to initiate
Priority 4	Reduce non-critical load
Resources required for recovery:	
Staff	Maintenance, external electrician & IT Manager
Data / systems / equipment	Servers, Client Ends, Network Equip
Action required	• Identify and shut down all non-essential electrical loads • Prioritise essential operational systems (IT servers/refrigeration and security etc.)

Recovery timeframe	30 min
Priority 5	**Improve water efficiency / sanitation / cold storage**
Resources required for recovery:	
Staff	Maintenance Manager and staff / External water tanker service
Data / systems / equipment	Water tanks, refrigeration equipment
Action required	• Implement water-saving measures (low-flow fixtures, controlled usage schedules) • Ensure sanitation facilities remain functional for staff and visitors • Optimise refrigeration usage to preserve cold chain.
Recovery timeframe	1 day

8.6 Logistics

Scenario 6:	Logistics	
Responsibility		Operations and Dispatch Manager
Potential impact on organisation if interrupted		Major
Likelihood of interruption to organisation		Likely
Total recovery timeframe		1 hour
Priority 1	**Critical function:**	**Use of alternative delivery company / reroute deliveries**
Resources required for recovery:		
Staff		Dispatch
Data / systems / equipment		Courier Company (own external plans in place) and SPAR Health delivery vehicles
Action required		Refer to paragraph 1.5

		Use alternative courier company/who is able to take the load of all deliveries to patients, healthcare facilities and pharmacies. If there is a fuel shortage, arrange backup fuel for SPAR Health delivery vehicles.
Recovery timeframe		Immediate
Priority 2	**Critical function:**	**Use of alternative supplier**
Resources required for recovery:		
Staff		Operations Manager
Data / systems / equipment		Telecommunication and e-mail
Action required		Refer to paragraph 1.5 Use alternative resources in the supply chain if there was looting of a supplier building and/or blockage of road by protestors. (suppliers/generics)
Recovery timeframe		1 day
Priority 3		**Back up diesel/petrol in Bowser for local deliveries**
Resources required for recovery:		
Staff		Maintenance Team
Data / systems / equipment		Bowser and PPE
Action required		• Maintain emergency fuel reserves in the bowser • Rotate stored fuel to ensure quality • Activate supply channels if fuel reserves run low
Recovery timeframe		30 min

8.7 National Epidemic / Disaster Announcement

Scenario 7:	National Epidemic and/or Disaster Announcement
Responsibility	Executive Managers
Potential impact on organisation if interrupted	Major

Likelihood of interruption to organisation	Likely
Total recovery timeframe	2 days
Priority 1	**Secure facilities with additional armed response**
Resources required for recovery:	
Staff	Maintenance & Risk Managers, CPI
Data / systems / equipment	• Armed response SLA & emergency numbers • Access control system • CCTV, alarm system, panic buttons, generator supply to security systems • Two-way radios, charged spare batteries, mobile phones • First aid kits, fire extinguishers, temporary signage (no entry), perimeter barriers (CPI) • Site plan, staff contact lists
Action required	• Appoint site leads • Call armed response (patrol vehicles and guards at entry points) • Secure external doors, suspend visitor access
Recovery timeframe	1 hour to establish
Priority 2 **Critical function:**	**Draft a plan**
Resources required for recovery:	
Staff	All the Department Managers
Data / systems / equipment	• Details regarding the Disaster or Announcement • Group plan • Year plan • IT • Maintenance
Action required	• Determine the impact day-to-day functions • Take national guidelines into account • Draft plan on action to be taken • Communicate plan to stakeholders and employees
Recovery timeframe	1 day
Priority 3	**Relocate staff/products to alternate safe premises**

Resources required for recovery:	
Staff	Operations & Logistics Manager, Security Personnel
Data / systems / equipment	Vehicle fleet, inventory records, alternative facility
Action required	• Identify and prepare alternate facilities • Arrange secure transport for products • Ensure necessary utilities and IT access at new location
Recovery timeframe	5-7 days
Priority 4	**Maintain remote operations where possible**
Resources required for recovery:	
Staff	IT Manager, Head of Departments, HR Executive
Data / systems / equipment	• Laptops • SOPHOS • WIFI
Action required	• Enable remote access to systems for all relevant staff • Provide training or guides on remote work protocols • Monitor productivity and data security remotely
Recovery timeframe	2 – 4 hours
Priority 5 **Critical function:**	**Communicate the plan to all stakeholders**
Resources required for recovery:	
Staff	Operations/Administration Manager
Data / systems / equipment	Telecommunication, e-mail, SMS Portal, WhatsApp
Action required	• Arrange meeting with all staff and communicate the plan • Send out the necessary info to clients, patients, pharmacies, students etc.
Recovery timeframe	2 hours

8.8 Emergency Situation (Refer to existing crisis management plan)

Scenario 8:	**Emergency situation whereby possible destruction of property (Looting)**	
Responsibility		Executive Managers
Potential impact on organisation if interrupted:		Major
Likelihood of interruption to organisation		Highly Likely
Total recovery timeframe		3 – 7 days
Priority 1	**Critical function:**	**Secure temporary facility & relocate personnel**
Resources required for recovery:		
Staff		HOD in every department
Data / systems / equipment		• Cell phone • Contact numbers for potential re-location facilities • Contact numbers for personnel
Action required		• Secure temporary facility where personnel can be relocated to • Re-locate personnel to facility • Inform IT Manager of location of temporary facility
Recovery timeframe		1 hour
Priority 2	**Critical function:**	**Temporary IT setup with laptops**
Resources required for recovery:		
Staff		IT Manager
Data / systems / equipment		• Laptops • Dongle
Action required		Set up on SPAR Health VPN
Recovery Timeframe		2 hours
Priority 3	**Critical function:**	**Secure building of DC**
Resources required for recovery:		

Staff		Maintenance Manager
Data / systems / equipment		Security
Action required		• Arrange security guards; and • Set up perimeters
Recovery timeframe		Immediately
Priority 4	**Critical function:**	**Temporary IT setup with additional hardware**
Resources required for recovery:		
Staff		IT Manager
Data / systems / equipment		• Laptops • Desktops • Printers • Software • WIFI • Telephones
Action required		Source hardware and set up on SPAR Health VPN
Recovery Timeframe		2 - 3 days
Priority 5	**Critical function:**	**Communicate with all stakeholders**
Resources required for recovery:		
Staff		HOD of every department
Data / systems / equipment		• Email, WhatsApp, SMS Portal, Telecommunication.
Action required		• Arrange meeting with all staff and communicate the plan • Send out the necessary info to clients, patients, pharmacies, students etc.
Recovery timeframe		2 hours

9. EMERGENCY RESPONSE AND RECOVERY PROCEDURES

This section outlines the critical procedures to be followed in the event of emergencies or disruptions that may impact people, facilities, or essential business operations. It provides guidance on protecting life and safety, safeguarding vital assets and records, and ensuring

effective communication with stakeholders to support the organisation's rapid recovery and continuity of services.

Fatal or serious injuries/illness procedure

Any fatality/serious injury must immediately be reported to the HOD, whereafter the department First Aider will be notified to attend to the individual. The injured person should not be moved unless he/she is not at risk of being further hurt. The first responder must check that the injured person and other employees aren't in any further danger, and, if possible, make the situation safe. The HOD will notify the HR department to arrange an ambulance and if necessary the police. The HR Department will further call the emergency contact that was listed by the injured employee. All incidents must be properly recorded by our Health and Safety representative and the necessary Compensation for Occupational Injuries and Diseases documents have to be completed and submitted.

Should it come to light that an individual in the building has a deadly highly contagious illness, it must be reported to the HOD and HR. The specific department will be placed under lockdown and everyone will have to wear a face mask depending on the circumstances. A general practitioner will be contacted to assist with a protocol to be implemented depending on what the illness is. After following the newly implemented protocol for the circumstances at hand, the maintenance team will disinfect the department before anyone is allowed to enter. Health and Safety representative has to investigate the matter and act to prevent the same or something similar from happening again.

Natural Disaster procedures

We will follow the directions of the national, provincial, and municipal spheres of government in the event of a natural disaster which may include extreme weather events, civil unrest, land degradation, etc. The EmCom will get together, provide direction, and confirm who will be responsible for drafting plans and upcoming tasks.

We will further unplug all electrical appliances, turn off the main electricity and water supply to the building depending on the situation at hand. Move all furniture and electrical equipment to the upper floor to prevent any further water damage.

Communication lines must be kept open at all times between management, HR, and employees to ensure that everyone is aware of what is expected of them. Depending on the circumstances and the instructions from the EmCom, employees will work together to evacuate the building and set up the necessary workspace at the directed location.

We have stormwater drains throughout the business park that are regularly cleaned. This will assist with getting rid of excess water on the premises. SPAR Health installed a freshwater reservoir to be used sparingly as a provision for a water crisis.

Stakeholder Communication

Communication to stakeholders will be drafted per emergency situation. Functional Heads must provide a comprehensive, graded list of stakeholders to be contacted in the specified order.

Vital assets and workspace

Should it become necessary to create alternate working places for those who are unable to work from home, the minimum requirements regarding vital assets are as follows:

Asset Requirements	Quantity
Personal Computers (Normal)	
Laptops	
Printers	
Telephones	
Cellphones	
Office furniture consisting of desks	
Fax machines	
Office furniture consisting of chairs	
Photocopying machine – Access to photocopying machine	
Physical office space required in m2	
Add as required.....	

Retrieval of vital records

At least 60% of documentation is kept in an electronic format. Electronic copies are stored in the SPAR Health server, backed up to the data domain.

If not stored offsite, paper documents must be kept in fire-resistant filing rooms with closed doors.

Designated Persons

Name	Work Phone Number
IT Manager	018 788 2075

Vital Paper Record Storage

Regarding critical documentation, the following should be adhered to:
Immediate contact should be made with the relevant Service Provider Companies to recreate documents.

Part of the documents should be typed into computer files. The files should be saved on the network. NB: This should be done as soon as possible.

If possible, a fire-resistant (SABS Group 3) Record Protection Cabinet should be purchased. The most critical documentation should be stored in the above-mentioned cabinet.

Designated Persons

Name	Work Phone Number
Maintenance Manager	018 788 2075

10. MITIGATION OF FINANCIAL LOSSES

i. Insurance Cover:
SPAR Health has insurance policies to cover losses from natural disasters, property damage, liability, and other potential risks, including business interruption insurance. For example, this type of insurance will help cover lost income and extra expenses caused by a power outage.

ii. Contingency Funds:
All reserves from after-tax profits for the last five years have been retained to fund potential growth and help SPAR Health weather unexpected financial losses without borrowing or depositing operating funds.

iii. Developing Mitigation Strategies:
We are investing in new equipment and technology to reduce energy consumption, such as using energy-efficient equipment and additional backup power and water solutions.

iv. Reviewing and updating insurance coverage:
We review the insurance coverage regularly to ensure that it is still adequate and that the business is not overpaying for coverage it does not need.

v. Diversification of investment and revenue streams:
SPAR Health continue to diversify its investment (Pharmacy at SPAR) and revenue streams to help spread out risk and reduce the impact of financial losses.

11. EMERGENCY NOTIFICATION CONTACTS

11.1 SPAR Health:

Managing Director
Jeremy Nicol
Tel: 079 504 5386
Email: jnicol@sbuys.co.za

Finance Executive
Dirk van Zyl
Tel: 082 827 8377
Email: dvzyl@sbuys.co.za

Risk, Legal and Compliance Executive
Madeleine Malan
Tel: 082 567 7254
Email: mmalan@sbuys.co.za

IT Manager
Gerry Muller
Tel: 082 780 7453
Email: gmuller@sbuys.co.za

Risk & Legal
Ina Barkhuizen
Tel: 072 391 3623
Email: ibarkhuizen@sbuys.co.za

Maintenance
Dean Jacobs
Tel: 082 569 6164
Email: djacobs@sbuys.co.za

11.2 Scriptwise and Pharmacy at SPAR Park:

Executive Manager (Project Manager) SW
Nadine Grobler
Tel: 083 776 4404
Email: ngrobler@sbuys.co.za

Responsible Pharmacist SW
Marisca van Heerden
Tel: 071 606 9128
Email: mvanheerden@sbuys.co.za

Responsible Pharmacist (Park)
Elsje Le Grange
Tel: 082 933 5721
Email: sbpark@sbuys.co.za

11.3 Academy:

Executive Manager
Estelle Victor
Tel: 082 775 2972
Email: evictor@sbuys.co.za

Training Manager
Jalia Meyer
Tel: 082 779 0583
Email: jmeyer@sbuys.co.za

11.4 Wholesaler:

Executive Manager
Eric Pickering
Tel: 082 440 6446
Email: epickering@sbuys.co.za

Operations Manager / RP
Tommie Grobler
Tel: 082 446 0883
Email: tgrobler@sbuys.co.za

11.5 Dispatch

Executive Manager
Eric Pickering
Tel: 082 440 6446
Email: epickering@sbuys.co.za

Dispatch Manager
JC Coetzer
Tel: 079 674 6531
Email: jccoetzer@sbuys.co.za