KOINZ (PTY) LTD

DISASTER MANAGEMENT AND DATA RECOVERY PLAN

KOINZ (PTY) LTD, Reg no. 2022/235484/07 **DIRECTORS**: LOUISE FOURIE & MARK WEETMAN
Address: Unit 1, Village Corner, 57 via Latina Crescent, Irene Corporate Corner, Irene, Gauteng, 0178
Postal Address: PO Box 61803, Pierre van Ryneveld, Centurion, Gauteng, 0045
Tel: 012 880 3790 Email: info@koinz.co.za Website: www.koinz.co.za

1. PURPOSE OF A DISASTER MANAGEMENT & DATA RECOVERY PLAN

From a business perspective, a disaster may be defined as any accidental, natural or man-made event which threatens or disrupts an organisation's normal operations to such an extent that the organisation fails or is brought to a standstill.

Any sudden and/or drastic crisis or event that disrupts the organisation's core business processes will ultimately have an impact on the organisation's ability to deliver products and/or services and to generate a profit.

Crisis events may be caused by:

- Natural events (for example: fires or floods), or
- Human behaviour, which can be both internal or external. Examples of external crises, could be an outsider committing arson, causing malicious damage to the organisation's property or committing an armed robbery. Examples of internal human behaviour that could cause a crisis include the dishonourable or dangerous conduct by staff members;
- Technological breakdowns (for example: power outages, computer virus attacks or cyber-crime);
- External economic events (such as the financial crisis of 2008).

The purpose of a Disaster Management & Data Recovery Plan is to provide a framework for establishing emergency responses and recovery procedures following a disaster or serious incident.

By following a systematic plan, the organisation will be able to resume its core business functions as quickly as possible thereby minimising the risk of reputational damage and financial loss.

The objectives of a Disaster Management & Data Recovery Plan are to:

- Communicate to all levels of the organisation, the organisation's commitment to transparency and treating customers fairly, even in the face of a disaster
- Plot the procedures and resources required in order to initiate recovery efforts
- Reduce the risk of injury or further harm to the organisation's staff members, clients and other third parties
- Ensure that the organisation recovers from unexpected business disruptions
- Resume core business processes as quickly as possible

- Point out the location of data storage devices and how business data may be retrieved
- Identify clients and other third parties who may be affected and must be notified in the event of a disaster
- Ensure that maximum possible service levels are maintained
- Minimise the likelihood and impact of interruptions
- Minimise the risk of reputational damage and financial loss
- Minimise the external impact of the disaster so as to ensure (as far as possible) the sustainability of financial markets
- Ensure the organisation deals with the disruption in a manner that fosters transparency and trust

2. EMERGENCY CONTACT DETAILS

The following individuals / organisations must be contacted in the case of an emergency:

Name	Contact Details
Mark Weetman	0828188988

Name	Contact Details
Louise Fourie	0731510908

Name	Contact Details
James Weetman	0741468522

The contact details of Emergency Response Services situated closest to the organisation are:

Ambulance	**012 664 6662/671 7211 / 671 0024**
Doctor	**664 0222**
Flying Squad	**10111**
Police	**0126543131/664 0024**
Fire Brigade	**012 310 6300/6400/ 107/671 6211 / 671 7375**
Poison Control	**0126645006**
Electricity	**0124213160/ 671 7536/671 7540**
Water Works	**012 358 9999/080 111 1556**
Telephone Company	**0128803790**

IT Service Provider	**In progress**
Other	

As part of the organisation's disaster recovery and data recovery plan an insurance policies has been put in place.

Policy Name	Coverage Type	Amount of Coverage	Personal responsible for Coverage
(Application in progress)	Civil and crime liability, Directors' and officers' liability	**1 000 000**	**KI and employees**

3. EMERGENCY RESPONSE PROCEDURES

3.1. FIRE

In the event of a fire, and where deemed feasible by the emergency contacts, the following response procedures will be followed:

Phase	Procedure	Responsible Persons / Additional Comments
1	If fire or smoke is present, assess the situation and determine the severity of the fire. Remove anyone from immediate danger and call the fire brigade as soon as possible.	
2	In the event of a minor fire, personnel are to attempt to extinguish the fire (e.g. a small paper bin fire).	All personnel must familiarise themselves with the location of the fire extinguishers closest to them.
3	In the event of a major fire, activate the building fire alarm system and call the fire brigade. Provide the fire brigade with your name, the location of the fire and your contact details.	All personnel must familiarise themselves with the location of the fire exits closest to them. Remain calm and do not run.
4	Notify building security.	Contact appropriate personnel to aid in the decision regarding the protection of equipment if time and circumstances

4	Confine the fire by closing all windows and doors if it is safe to do so.	Do not attempt to distinguish the fire if it is unsafe to do so. Remember, safety first. If smoke is present, stay beneath the smoke while evacuating. Closed doors must be tested with the back of the hand for any heat prior to opening. If a door is really hot due to fire on the other side, do not open it and find an alternative route to safety.
5	Evacuate the building and assist all visitors to the nearest fire exits.	Evacuate the building in accordance with your building's emergency evacuation procedures. Use the nearest stairwells. Do not use elevators.
6	Gather at designated assembly points.	Follow the fire marshal's instructions provided and do not wander around or leave the area until instructed to do so. This is important to ensure that all

3.2. FLOODING

In the event of flooding, and where deemed feasible by the emergency contacts, the following response procedures will be followed:

Phase	Procedure	Responsible Persons / Additional Comments
1	If water is originating from above electronic equipment, power down the affected individual devices, provided it is safe to do so.	Do not interact with electronic devices that are in contact with water.
2	Notify all personnel within the building of the situation and cease all affected business operations.	
3	Assess the extent of the flooding and determine whether professional technical services will be required (i.e. minor or major flooding).	Water detected on floor level may have different causes. If water is slowly dripping from air conditioning equipment, contact repair personnel immediately.
4	If water is of a major quantity and flooding beneath the floor, immediately power-down all affected electronic devices at the main switch.	If further danger is imminent, then immediately evacuate the building and follow management's instructions.

5	Contact the local municipal water works department for further instructions.	

3.3. ARMED ROBBERY

In the event of an armed robbery, and where deemed feasible by the emergency contacts, the following response procedures will be followed:

Phase	Procedure	Responsible Persons / Additional Comments
1	Remain calm and avoid any action that may provoke further violence.	
2	Comply with the assailant's instructions, even though it seems that personnel will not be harmed.	Do not try to overpower an armed assailant.
3	Immediately following the incident, establish whether any personnel were injured and contact the police flying squad.	Quickly assess whether any personnel are injured and require medical attention. If you are able to assist them without causing further injury to them or without putting yourself in further danger, then provide what assistance you can and call for help.
4	Close and secure the office until the police arrive.	All personnel involved in the incident should write down their own description of the events.
5	Personnel should receive trauma counselling.	

3.4. COMPUTER VIRUS ATTACKS

In the event of the above, and where deemed feasible by the emergency contacts, the following response procedures will be followed:

Phase	Procedure	Responsible Persons / Additional Comments
1	Isolate the infected computers by disconnecting them from the organisation's internal and external network.	Every employee is responsible

2	Inform the IT department and/or contact the organisation's IT service provider for further instructions.	Every employee is responsible
3	Where computers are still operational, remove malware by running an anti-virus software on the compromised computer.	Every employee is responsible
4	Where computers are not operational, arrange for alternative computers where necessary.	Determine cause of outage and timeframe for recovery.
5	Review anti-virus updates and IT security procedures.	Every employee is responsible
6	In the event of a cybercrime- retain all of the evidence linked to the crime and report the crime to the South African Police Services.	

4. RECOVERY PROCEDURES

4.1. RESPONSIBLE PARTIES

The following individuals are responsible for managing disaster and/or data recovery efforts:

Full Names & Surname	Contact Details
Mark Weetman	0828188988

Full Names & Surname	Contact Details
Louise Fourie	0731510908

Full Names & Surname	Contact Details
James Weetman	0741468522

4.2. RECOVERY ANALYSIS

What are the core business functions that need to be operational as soon as possible following a disaster?
1. Operations Department 2. Finance Department
If so required, can the organisation relocate the business to a temporary location, and if so, where is the most suitable location?
In the event that there is a disaster, every employee is supposed to work from home. There is no alternative work location. All the necessities for working from home shall be provided by Koinz
How will the organisation finance the costs of recovery?
Koinz has an insurance cover that will cover all the necessary costs in the event of a disaster
Does the organisation maintain backups of critical business data, and if so, how and where can this information be retrieved?
The IT service providers will be assisting in this regard.
Is the computer server stored offsite? If so, where is the server located?
It is located on premise on a visible location.

Does the Organisation's insurance policy cover loss of income and damages to property due to a disaster?
Yes, it does

4.3. DISASTER & DATA RECOVERY PROCEDURE

The individuals responsible for managing disaster and/or data recovery efforts will, where feasible, follow the procedures outlined below:

Phase	Procedure	Responsible Persons / Additional Comments
1	Response team to meet as soon as possible.	Receive communication on emergency situation and contact relevant emergency response services where so required.
2	Ensure that the source / event that triggered / caused the disaster or loss of data no longer poses an immediate threat to the organisation, its personnel or other third parties.	The immediate risk of loss of life, health or property must be avoided.
3	Where the organisation's business premises are no longer available, identify a recovery site. Relocate or set up temporary office space.	The temporary site may be moved to various premises depending on the extent of the disaster.
4	Retrieve Business Continuity Plan	
5	Establish basic communication facilities. i.e. telephone / mobile services.	Notify all relevant stakeholders of the crisis situation and how they may reach the response team: 🕐 Personnel and their family members 🕐 Clients 🕐 Media 🕐 Suppliers 🕐 Regulators 🕐 Insurance company 🕐 Service providers Managers will serve as first contact point for their respective departments.
6	Address immediate financial needs of the organisation.	Assess temporary borrowing capability, insurance policies and availability of the organisation's credit cards.

7	Restore basic IT infrastructure i.e. emails / data servers	Retrieve data stored on backup devices.
8	Restore core business services	Assess resources required to restore core business services and coordinate all activities with the response team. Oversee delivery and placement of office supplies.

5. DATA BACKUP PROCEDURES

Proper electronic data backups will minimise the risk of loss of important business information in the event of a disaster.

Permanent loss of data may have a significant impact on the organisation's ability to perform core business functions. It is therefore imperative that backups are made and tested on a regular basis.

The following individuals are responsible for the organisation's data backup procedures.

The below will be the yet to be appointed IT

Full Names & Surname	Contact Details

Full Names & Surname	Contact Details

Data can be stored on any of the following devices:

- Compact Discs ("CDs") / Digital Versatile Discs ("DVDs");
- Flash-drives;
- External hard drives and Tape drives;
- Cloud storage;
- Network Storage or Servers; and
- Offsite backup systems (replication or synchronisation methods).

The frequency and the extent of backups will correspond proportionately with the importance of the data being stored. For example, where client information is of critical importance to the organisation's day-to-day functioning and/or regulatory compliance requirements, the information will be backed-up on a more frequent basis.

The three main types of backup procedures are:

- ***Full Backups:*** A full backup captures all data files on disk. It is the simplest type of backup and provides a complete backup image, making restoring data and functionality easier and faster. The disadvantage of a full backup is that it takes time and uses more storage space than an incremental backup.
- ***Incremental Backups****:* Incremental backups only contain copies of data files that were changed subsequent to the previous backup. This allows for more device storage space and considerably reduces the time it takes to perform a backup.
- ***Custom Backups:*** Custom backups are usually made on an ad hoc basis.

Backups must be tested on a regular basis. Regular testing will minimise the risk of an unsuccessful data recovery exercise following a disaster.

6. DATA BACKUP ROSTER (Will be functional once we have an outsourced IT)

It is recommended that the organisation maintains a data backup roster as per the below.

Data ID	File system description	Backup method	Backup media	Frequency	Schedule	Storage locatio

7. Conclusion:

All representatives of Koinz including key individuals and management are required to be dedicated to upholding the highest level of integrity and ethical conduct in all of their activities and relationships with all stakeholders.

8. Ownership and Accountability

This policy is owned by **Koinz (PTY) LTD**, an authorised financial services provider in terms of the Financial Advisory & Intermediary Services Act (37 of 2002) and subordinate legislation.

As Key Individual of the Provider, I, **Mark Howard Weetman** hereby confirm the adoption of the policy on behalf of the governing body of the Provider. I hereby accept responsibility for the successful training of employees and successful implementation of this Policy.

Signatures **Date**