DOUBLE M MEDPRAC SOLUTIONS

ICT Disaster Recovery Policy

Glen Manor Office Park
138 Frikkie De Beer Street
Menlyn
Pretoria
0181
+27 (0) 87 160 0735
danny@mmedprac.co.za
www.mmedprac.co.za

TABLE OF CONTENTS

Glen Manor Office Park
138 Frikkie De Beer Street
Menlyn
Pretoria
0181
+27 (0) 87 160 0735
danny@mmedprac.co.za
www.mmedprac.co.za

Glossary of Business Terms

Alert: Notification that a potential crisis exists or has occurred; direction to stand by for possible implementation of emergency measures.

Alternate Site: A designated location to be used to conduct business when the primary facility is not accessible.

Business Continuity Planning: The process of developing advance arrangements and procedures that enable Double M Medprac to respond to a crisis in such a manner that critical business functions continue with planned levels of interruption or essential change.

Business Impact Analysis: The process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives.

Call Tree: A document that graphically depicts the names and contact information for persons to be called in the event of a crisis.

Command Center: A physical or virtual facility located outside of the affected area used to gather, assess, and disseminate information and to make decisions regarding the response to a crisis.

Contingency Plan: The steps to be followed to conduct a business process without access to the normal operational facility and tools.

Crisis: A critical event, which, if not handled appropriately, could negatively impact Double M Medprac's profitability, reputation, or ability to operate; the period during which a Business Continuity Plan is implemented.

Crisis Management Team (CMT): The key role players responsible for Business DR, who implement Double M Medprac's response to a crisis in an effective, timely manner, with the goal of avoiding or minimizing damage to Double M Medprac's ability to operate.

Disaster Recovery (DR) Plan: The steps needed to be taken to restore Double M Medprac to an acceptable operating condition.

Operational Facility: The place from which business is normally conducted (i.e., the office).

Processor: The employee who conducts or exercises the steps of one of the business processes.

Recovery: The period of time when steps are taken to restore business processes and support functions to operational stability following a crisis.

Recovery Point Objective (RPO): The point in time to which systems and data must be recovered after an outage.

Recovery Time Objective (RTO): The period of time within which systems, applications, or functions must be recovered after an outage.

Glen Manor Office Park
138 Frikkie De Beer Street
Menlyn
Pretoria
0181
+27 (0) 87 160 0735
danny@mmedprac.co.za
www.mmedprac.co.za

ICT Disaster Recovery Policy

1. Overview

It is important to Double M Medprac Solutions to realize that having a contingency plan in the event of a disaster gives a competitive advantage. This policy will manage financial support and diligent attended to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

2. Executive Summary

The purpose of this Disaster Recovery (DR) Plan is to describe the technical activities instituted by Double M Medprac to ensure that the Information Technology (IT) systems meet the recovery protection objectives (RPOs) and recovery time objectives (RTOs) defined by the business to ensure continuity of its operations, the safety of its employees, and physical and intellectual assets in the event of a critical incident at its operational facility. The plan outlines the Disaster Recovery plan for Information Technology once the business has declared a critical incident that impacts the computer facility.

3. Purpose

This policy is to define the need for management to support ongoing disaster planning for Double M Medprac.

4. Scope

This policy applies to all the staff of Double M Medprac Solutions including management and technical staff. (Be it outsourced)

5. **CONTINGENCY PLANS** (details of system backup and disaster recovery plan)

The backup plan, backup register, Disaster Recovery (DR) plan and Business Continuity plan are reviewed at least once annually. Below is a basic overview of the backup and recovery process.

Backups (Computer Emergency Response Plan):

- Daily automated backups of all Servers, databases, Desktop PC's and laptops are performed daily to a cloud backup facility. Data are compressed and encrypted before its uploaded to the cloud backup storage facility.
- The minimum data retention period is 60 days.
- Ntipu Holdings will be contacted, immediately when emergency has occurred. Damage will be accessed and an action plan of which whether a repair or replacement is needed will be taken.
- Sever, switches, router, multi-function Printer, Telephones, UPS, Desktops & Laptops. Our ICT Service Provider provides equipment upon request.

Glen Manor Office Park
138 Frikkie De Beer Street
Menlyn
Pretoria
0181
+27 (0) 87 160 0735
danny@mmedprac.co.za
www.mmedprac.co.za

5.1. Succession Plan:

In the event where in-house ICT support is unavailable, a call will be logged to Ntipu Holdings to attend the matter shortly.

5.2. Data Study:

Double M Medprac Solutions and Clients Data will be stored in our in-house sever. Executive Manager, CEO and appointed personnel will have access to that data.

5.3. Criticality of Service List:

Debt Collection and Finance

5.4. Data Backup and Restoration Plan:

Double M Medprac's and its Clients Data will be stored in a centralised in-house sever. Every Midnight from Monday to Friday, data will be uploaded to the cloud sever as back-up. Should anything happen to our in-house sever, whether theft or fire, data will be restored from cloud server to a new machine immediately.

6. Placing Plans into Action

Management will set aside time to test implementation on every quarter. During these tests, issues that may cause the plan to fail will be discovered and corrected in an environment that has few consequences.

- The first step of the recovery process is to determine the scope of damage to the servers, workstations, systems, or databases that needs to be restored or recovered.
- Database recovery can be done within short time (Max 2 Hours), restoring data from the replicated slave server or on-site backups.
- If the on-site backup server is intact the previous day's backup is restored in +/- 30 minutes. If the offsite backup needs to be used it will be downloaded and restored in +/- 1:30.
- If consultants' workstations are corrupted or stolen, new computers will be connected to the terminal and expected to be operational in a few minutes from time of re-installation.
- If the main server is broken a new server is ordered from suppliers or existing company server is used.
- The new server is then configured and all needed software is installed. Backups of the previous main server are then restored on the new server.
- If a workstation is not functioning anymore, we replace it with a new device that is most of the time available on site, if not we backup and restore the existing workstation box.

Glen Manor Office Park
138 Frikkie De Beer Street
Menlyn
Pretoria
0181
+27 (0) 87 160 0735
danny@mmedprac.co.za
www.mmedprac.co.za

6.1. Updating Plans

Review all plans annually so changes in Double M Medprac's situation can be incorporated.

6.2. Enforcement

Any employee that violates this policy may be subject to disciplinary action up to and including termination of employment.

6.3. Revision History

A history of revisions to this Plan will be maintained by Executive Manager quarterly or annually

7. Organizational Test and Maintenance Plan

The CMT will conduct a test of this DR Plan on an annual basis or more frequently, as directed by the Business DR Lead.

7.1. Purpose of the test:

Annual testing allows the organization to link together and validate individuals and teams' actions under the DR Plan. All testing in stills confidence in the participants, which will ensure a more effective response to an actual emergency. Client requirements and industry regulations often mandate testing. Testing provides the most realistic and effective training possible. Not testing creates the risk that, in an actual emergency, our plans will fail.

7.2. Goal of the test:

Test the accuracy and effectiveness of the DR Plan components to provide input for continually improving the plan. The goal of the test is not to measure whether the Plan "passes" or "fails." Failure of the plan components is a positive result since failure provides the most valuable source of input to improve the plan.

7.3. Test Scenario:

Prior to the actual test exercise, a scenario will be agreed upon by the CMT, including a "disaster" to be simulated during the exercise, a conference room or other location to be designated as the "Command Centre," and other easily accessible location(s) to serve as the "alternate site(s)" for the individual process Contingency Plans to be tested.

The backup plan, backup register, Disaster Recovery (DR) plan and Business Continuity plan are reviewed at least once annually. Below is a basic overview of the backup and recovery process.

Implementation of policy

This policy shall be deemed effective as of 1 November 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.