Disaster Recovery Plan Policy

1. Overview

Disaster recovery planning is often left until it's too late. Disasters happen rarely, and as such many organisations fail to prioritise their preparation processes until they are affected. Having a contingency plan in the unfortunate event that a disaster occurs is essential to ensure the continuity of business operations throughout and after the disaster, and gives the company a competitive advantage.

Disasters, as defined by this policy, include not only natural disasters such as floods and earthquakes but also any other event that could cause an extended and immediate disturbance or delay to service delivery or business operations.

2. Purpose

This policy defines the development process and implementation steps of a disaster recovery plan for the NIAB. This includes the process for recovering IT systems, applications and data from any type of disaster or major outage.

3. Scope

As this policy details the development and implementation of a disaster recovery plan, its scope extends to the IT management staff who are responsible for developing, testing and updating the plan.

4. Policy

List of Contingency Plans

The following contingency plans must be developed:

4.1. Disaster Recovery Plan

This plan must detail who is to be contacted in the immediate aftermath of a disaster, as well as when and how they are to be contacted. This plan must include specific advice for each of the most likely types of disaster that the Company might face, as well as general guidance.

4.2. Priority Server List

This list must include all the services provided and their order of importance. This list should also include an order of recovery in both the short-term and long-term aftermath of a disaster event.

4.3. Data Backup and Restoration Procedures

This plan must detail which data is backed up, where it is backed up and in which manner it is stored. It should also detail how often the backup is made, and how the data can be recovered.

4.4. Testing

It is essential that after plans have been developed, they are tested to whatever extent is feasible. Time should be set aside to test implementation of each part of the plan as well as the full disaster recovery plan. Reviews should be conducted annually, and the plan must be updated to meet any new requirements or information.

5. Compliance

5.1. Compliance Measurement

The IT team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. Exceptions

Any exceptions to this policy must be approved by the IT team in advance and have a written record.

5.3. Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.