Symphony Limited

IT Disaster Management Policy

I. PURPOSE

This policy outlines the procedures for preparing for, responding to, and recovering from IT disruptions that threaten the availability, integrity, or confidentiality of data and systems of Symphony Limited (the "Company").

The purpose of this policy is to –

- ✓ Minimize downtime and data loss caused by IT disasters (natural disasters, cyberattacks, hardware failures etc.).
- ✓ Ensure business continuity during IT disruptions.
- ✓ Protect critical IT infrastructure and data assets.
- ✓ Establish clear roles and responsibilities for disaster response and recovery.
- ✓ Facilitate a swift and efficient recovery process.

A well-defined IT Disaster Management Policy and a comprehensive IT Disaster Recovery (ITDR) Plan are essential for ensuring business continuity and minimizing the impact of IT disasters. By following these guidelines, the Company protects its critical data and systems, and ensures a swift recovery in the event of an IT disruption.

II. SCOPE

This policy applies to all IT infrastructure, systems, applications, and data managed by the Company and used by employees across the Company.

III. ROLES AND RESPONSIBILITIES

The Company's management provides resources and support for ITDR activities and ensures business continuity during disasters.

The Company's IT department leads the development and implementation of the ITDR plan, manages data backups, and coordinates disaster recovery efforts.

The Company's employees follow established procedures during IT disruptions, report incidents promptly, and participate in disaster recovery training.

IV. IT Disaster Recovery (ITDR) Plan

The Company's ITDR Plan outlines the followings:

1. Risk Assessment:
   Identifying potential IT threats and vulnerabilities.

2. Business Impact Analysis (BIA):
   Determining the criticality of IT systems and acceptable downtime for core business functions.

3. Recovery Time Objective (RTO) and Recovery Point Objective (RPO):
   Defining the acceptable time to recover systems and data loss tolerance levels.

4. Data Backup and Recovery:
   Establishing procedures for regular data backups and restoration methods.

5. Disaster Response Procedures:
   Outlining steps for incident identification, notification, containment, and mitigation.

6. Testing and Training:
   Conducting regular testing of the ITDR plan and providing disaster recovery training to IT staff and relevant personnel.

V. REVIEW OF THIS POLICY

This policy and the ITDR plan shall be reviewed and updated periodically to reflect changes in technology, threats, business needs, industry standards, and legal requirements.

***