Symphony Limited

Data Security Policy

I. PURPOSE

This policy outlines the guidelines and procedures to protect the confidentiality, integrity, and availability of the Company's data assets. It is applicable to all employees of Symphony Limited (the "Company"), including contract workers and contractors, and anyone authorized to access or process the Company's data.

The purpose of this policy is to –

- ✓ Safeguard sensitive information and company data.
- ✓ Put in place optimal security controls basis data classification.
- ✓ Ensure the appropriate use, storage, and transmission of data.
- ✓ Minimize risk from data breaches, unauthorized access, and other security threats.

II. ROLES AND RESPONSIBILITIES

The management of the Company is responsible for establishing and enforcing this policy, allocating resources for data security measures, and ensuring employee training.

The IT Department of the Company is responsible for managing and maintaining data security systems, monitoring network activity, and responding to suspected data breaches and security incidents promptly.

The employees of the Company are responsible for following this policy, protecting the Company's data, reporting suspicious activity, and completing data security awareness trainings.

III. DATA SECURITY PRACTICES

1. Access Controls:
   The Company implements strong access controls to restrict access to data based on the principles of least privilege (granting only necessary access).

2. Data Encryption:
   The Company encrypts sensitive and confidential data at rest and in transit to ensure confidentiality.

3. Data Storage:
   The Company stores data on authorized servers or cloud storage solutions with robust security measures.

4. Data Transfer:
   The Company follows secure protocols for transferring data electronically.

5. Data Backups:
   The Company maintains regular backups of data for disaster recovery process.

6. Data Disposal:
   The Company securely disposes of data that is no longer needed, following appropriate procedures to prevent unauthorized access, in compliance with applicable laws and regulations.

7. Incident Reporting:
   The Company's employees must report any suspected data breaches or security incidents to the IT department of the Company promptly.

IV. SECURITY MEASURES

1. Access Controls:
   The Company implements firewalls, intrusion detection systems, and anti-malware software to protect the Company's network and systems.

2. Vulnerability:
   The Company periodically assesses and addresses vulnerabilities in systems and applications.

3. Data Loss Prevention (DLP):
   The Company implements DLP solutions to prevent unauthorized data exfiltration.

4. Logging and Monitoring:
   The Company's IT department monitors data system activity for suspicious behaviour and maintains data access logs for auditing purposes.

V. SECURITY AWARENESS AND TRAINING

The Company provides regular data security awareness training to educate them about best data security practices, and contents of this policy document.

VI. VIOLATION OF THIS POLICY

The Company takes violation of this policy seriously. Its violation by any of its employees results in disciplinary action, up to and including termination of employment.

VII. REVIEW OF THIS POLICY

This policy shall be reviewed and updated periodically to reflect changes in technology, industry standards, and legal requirements.

***