Thinking of Tomorrow

Symphony Limited

Cyber Security Policy

I. PURPOSE

This policy outlines the guidelines and procedures to protect information assets, technology infrastructure, and overall digital security posture of Symphony Limited (the "Company"). It is applicable to its employees, including contract workers and contractors, and anyone authorized to access assets and technology infrastructure.

The purpose of this policy is to –

- ✓ Safeguard sensitive information and company data.
- ✓ Ensure the confidentiality, integrity, and availability of the Company's IT systems and networks.
- ✓ Minimize the risk of cyber threats.
- ✓ Promote a culture of cyber security awareness and responsibility among all employees of the Company.
- ✓ Comply with relevant industry regulations and data privacy laws.

II. ROLES AND RESPONSIBILITIES

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

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

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

III. ACCEPTABLE USE

1. Company Devices and Resources:
   The Company mandates use of its devices and resources for authorized business purposes only, limiting their personal use complying with this policy.

2. Passwords:
   The Company mandates setting and updating strong and unique passwords for its accounts and system as per prevailing guidelines. Password sharing is strictly prohibited.

3. Data Security:
   The Company mandates users for safeguarding sensitive data and adhering to data classification protocols. Downloading unauthorized software or transferring data to unapproved devices is strictly forbidden.

4. Email and Communication:
   The Company mandates its employees to exercise caution with email attachments and links from unknown senders. Confidential information must be shared through encrypted channels only.

5. Internet Browsing:
   The Company mandates its employee to avoid visiting malicious website or downloading files from untrusted sources.

IV. SECURITY MEASURES

1. Access Controls:
   The Company grants access to its system and data based on the principle of least privilege (granting only necessary access).

2. Software Updates:
   The Company's devices are being kept up to date with the latest security patches and software versions.

3. Firewalls and Anti-Virus:
   Firewalls and anti-virus software are being installed and maintained on the Company's all devices.

4. Mobile Devise Security:
   The Company's employees using personal devices for work purposes must comply with specific mobile device management (MDM) policies.

5. Incident Reporting:
   The Company's employees must report any suspected security incidents (phishing attempts, malware infections, data breaches etc.) to the IT department of the Company immediately.

V. SECURITY AWARENESS AND TRAINING

The Company provides regular security awareness training to educate employees on cyber threats, best 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.

***