Information Security Governance Policy

Ngernturbo Public Company Limited ("The Company") recognizes that information technology and network systems are vital mechanisms driving efficient and sustainable financial services. However, technological growth inevitably brings cyber threat risks that could impact business continuity, corporate credibility, and the privacy of customer and stakeholder personal data.

The Board of Directors has therefore established this "Information Security Governance Policy." This policy references and adapts international standards, such as ISO/IEC 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to serve as a systematic and sustainable governance framework for protecting, maintaining, and managing the Company's information technology infrastructure.

1. Scope

- All directors, executives, permanent employees, temporary employees, and contract staff of the Company and all its subsidiaries.
- All information systems, computer equipment, data networks, software, and information technology infrastructure belonging to the Company.
- Outsourced service providers, consultants, business partners, and authorized third parties permitted to access, interact with, or utilize the Company's information systems and data.

2. Governance Structure and Responsibilities

To ensure a rigorous governance system aligned with Corporate Governance (CG) principles, the Company defines the following roles and responsibilities:

- **Board of Directors:** Responsible for approving this policy, ensuring an adequate and appropriate IT risk management structure, and supporting regular IT and cyber threat training for directors and senior executives at least once a year to ensure authentic "Tone at the Top" leadership capabilities.
- **Risk Management Committee:** Responsible for assessing risks, monitoring the IT & Cyber Risk Register, and reviewing the readiness of the IT Business Continuity Plan and Disaster Recovery Plan (IT BCP/DRP) at least once a year, or upon the

occurrence of significant events.

- **Audit Committee:** Responsible for overseeing and monitoring IT Audits conducted by the internal audit department or independent external experts to ensure that IT internal controls are effective, transparent, and compliant with relevant laws.
- C**hief Technology Officer (CTO) / Designated Senior Executive:** Responsible for implementing the policy, developing sub-guidelines, overseeing system security, and reporting system status, cyber threats, and mitigation strategies to the Risk Management Committee at least once a year.

3. Information Security Management According to International Standards

The Company enforces the application of and compliance with the 5 core functions of international information security frameworks: Identify, Protect, Detect, Respond, and Recover.

3.1. Identify

- Maintain an updated IT Asset Inventory and implement a Data Classification protocol based on data sensitivity and importance.
- Conduct an annual IT and cyber risk assessment to analyze vulnerabilities and determine appropriate control measures.

3.2. Protect

- **Access Control**: Adhere to the principles of Least Privilege and Need-to-Know Basis. Review employee access rights at least every 12 months, or immediately upon job rotation or termination of employment.
- **Secure Authentication:** Enforce Multi-Factor Authentication (MFA) for accessing critical systems or when working remotely (Remote Access / VPN).
- **Network Security:** Deploy industry-standard network defense systems, including Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and anti-malware software across all computer endpoints.

3.3. Detect

- Establish a system monitoring and Log Management mechanism compliant

with relevant laws to ensure timely detection of anomalies within information systems.

- Engage independent external experts to perform regular Vulnerability Assessments (VA) and Penetration Testing (Pen Test) on critical operating systems.

3.4. Respond & Board Escalation SLA

- Establish a Cybersecurity Incident Response Plan with clear operational procedures to contain and limit damage to systems and data.
- **Critical Incident Reporting SLA:** In the event of a critical cyber threat or a significant customer data breach that severely impacts the Company's reputation, finances, or operations, management must report the incident to the Risk Management Committee and the Board of Directors within 24 hours from detection or confirmation.

3.5. Recover

- Implement secure Data Backup protocols, including Off-site Backup or secure cloud storage, and conduct regular data restoration tests.
- Formulate and drill the IT Disaster Recovery Plan (IT DRP) at least once a year to ensure that critical IT systems can be restored within defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets during disasters or system failures.

4. Cyber Awareness and Training

- All employees and executives must undergo mandatory Cybersecurity Awareness Training annually to stay updated on modern social engineering tactics (e.g., Phishing, Social Engineering).
- The Company will conduct routine Phishing Simulations to evaluate readiness and mitigate technical attack risks.
- Provide secure reporting channels for employees to report anomalies or system vulnerabilities, supporting a No-Retaliation Policy for Vulnerability Reporting to

protect reporting employees from adverse professional or disciplinary actions.

5. Third-Party Connectivity and Data Security

- When contracting with outsourced service providers or business partners who require access to Company systems or data, a Non-Disclosure Agreement (NDA) and information security terms must always be attached as an integral part of the contract.
- Conduct a Vendor Security Assessment prior to procurement, and immediately revoke or adjust the service provider's access privileges upon project completion.

6. Integration with the Personal Data Protection Act (PDPA)

The design, modification, and security controls of all Company information systems must strictly align with and support the minimum security measures stipulated by the Personal Data Protection Act B.E. 2562 (2019) (PDPA). This ensures that customer and employee data are protected against leakage, loss, or unauthorized access, thereby fully safeguarding Data Subject Rights.

7. Penalties for Policy Violations

Any violation, non-compliance, or intentional act that compromises, risks, or causes severe damage to the Company's information technology systems and security framework shall be considered a grave disciplinary offense. Violators will face disciplinary actions in accordance with Company work regulations, ranging from warnings and suspension to termination without severance pay. Furthermore, the Company reserves the right to pursue civil, criminal, and legal actions under the Computer Crimes Act to the fullest extent of the law.

8. Policy Review and Evaluation

This Information Technology and Cybersecurity Policy shall be reviewed and evaluated for adequacy and appropriateness by the Risk Management Committee and the Board of Directors at least once a year, or immediately following significant changes in laws, international standards, technology, or business models to ensure it remains current and effective.