INFORMATION TECHNOLOGY GOVERNANCE POLICY
PT Elang Mahkota Teknologi Tbk
("Company")

Introduction

In line with the rapid development of technology, the Company requires a Policy which regulates Information Technology Governance ("**Policy**"). This Policy lays out further regarding Monitoring and Supervision, Information Technology Management Structure, Implementation, Information Technology's Contribution to Business Performance Improvement, Incident Response Procedure, Contingency Plan and Compliance. The Company has also from time to time measured the information technology maturity level and implemented this Policy effectively.

Monitoring and Supervision

In connection with the implementation of this Policy, the Company conducts periodic monitoring and supervision, led by by Yuslinda Nasution as Director of the Company, which has a background in the field of Electrical Engineering majoring in Telecommunication. Currently, she also acts as a member of board of director and board of commissioner within several companies which is part of the Company group, conducting their business in the field of telecommunication and information technology, such as PT Tangara Mitrakom and PT Abhimata Citra Abadi.

Information Technology (IT) Management Structure

The Company's information technology management structure comprised of three main pillars, as follows:

1. Infrastructure, which includes management and monitoring of network devices, servers, storage, access control and security systems, telephony systems, administration of critical applications, as well as data backup, data protection and security.
2. In-house Application Development, for the development of tailor-made internal applications, such as intranet application for employee self service portal, ERP, reporting portal application, management application, as well as archival of file-based assets.
3. IT Support and Helpdesk, which operates 24x7 to handle IT-related matters such as troubleshooting as well as installation of new devices.

Implementation

Implementation of governance related to Cyber Security in the Company:

1. Conduct awareness to all work units in the Company.
2. Require all employees of the Company to participate in e-learning.
3. Sending awareness emails to all employees of the Company.
4. Providing 24/7 IT Support and Helpdesk services responsible for monitoring the Company's Cyber Security systems.
5. Discuss in Board of Directors (BOD) or Board of Commissioners (BOC) meetings related to Information Technology updates and initiatives.

IT System Vulnerability Mitigation

The Company periodically conducts vulnerability assessments to identify and evaluate potential security weaknesses within its information technology infrastructure, including the systems, networks, and applications in use. These assessments are carried out through a combination of automated scanning and manual testing to ensure comprehensive and accurate coverage.

INFORMATION TECHNOLOGY GOVERNANCE POLICY
PT Elang Mahkota Teknologi Tbk
("Company")

Each identified risk will be thoroughly analyzed by the IT team in relation to the infrastructure. High-risk vulnerabilities shall be promptly addressed through appropriate corrective measures, such as the implementation of security patches and system configuration adjustments. All findings from this process shall be integrated as part of periodic evaluations into the Company's risk management framework, as a demonstration of the Company's commitment to strengthening information security and ensuring compliance with applicable regulations and best practice standards.

As part of its broader information security efforts, the Company has initiated a collaborative program involving IT Heads from subsidiaries and affiliated companies within the EMTEK Group. This initiative serves as a platform for sharing best practices in IT governance and in mitigating cybersecurity risks, including threats such as hacking, ransomware, and other cyberattacks. The objective is to promote a consistent and proactive approach to IT risk management across the Group.

In line with international standards, the Company also encourages its subsidiaries and affiliates to pursue globally recognized certifications in information security. These include ISO/IEC 27001 for Information Security Management Systems, as well as other relevant international IT and cybersecurity certifications. Several subsidiaries have obtained ISO/IEC 27001 certification, including PT Tangara Mitrakom, PT Vidio Dot Com, PT Bukalapak.com Tbk, and PT Five Jack. Furthermore, PT Indopay Merchant Services has achieved a Certificate of Compliance with the Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.

Information Technology's Contribution to Business Performance Improvement

In order to further improve employees' productivity and business performance, the Company runs its IT operations by relying on virtualization and setting up private clouds for various applications. This enables the Company to use integrated applications such as Emails, Employee Self Service, Digital Archive System, Storages, etc. The integration of the aforementioned systems allows the Company to conduct its business in a completely transparent manner.

All information systems implemented in the Company's work environment, both at the operational and functional levels, in principle and in practice aim to improve the effectiveness and efficiency of operational activities, which in turn will have a positive impact on the Company's sustainable growth.

Incident Response Procedure

Immediately after becoming aware of a suspicious matter, potential breach or breach of the Company's information technology system, each personnel of the Company is obliged to report such matter to the Company's information technology team ("**IT Helpdesk Team**"), by following such procedure:

1. **Identification** – the relevant personnel delivers the report and explains the issue found to the IT Helpdesk Team through whatsapp chat or through email to helpdesk@sctv.co.id or another email address as may be informed from time to time;

2. **Initial Investigation and Analysis** – the IT Helpdesk Team which receives the report will conduct an initial investigation and analysis towards the issue delivered, to

determine the extent of damage which may be resulted by the issue reported towards the Company's information technology system security;

3. **Rectification** – the IT Helpdesk Team and the personnel delivering the report will work together (as relevant) to conduct necessary rectification after the initial investigation and analysis stage concludes that the issue reported may cause harm to the Company's information technology system.

Contingency Plan
Being aware of the potential disruptions towards the Company's information technology system such as among others disturbances due to global internet connection failure, virus and/or hacker attacks and cybersecurity threat which may potentially disrupt the Company's business and cause leakage of confidential data, the Company has prepared risk mitigations including among others preparing backup on hard disks/laptop/non-online storage, installing anti-virus software in every office computer/laptop, blocking access to suspicious sites, limiting attachments from unknown external emails as well as protecting confidential documents with passwords.

Compliance
Any intentional or unintentional deviation or violation of Company policies, practices or standards will be subject to disciplinary action, up to and including termination of employment or contract and possible civil or criminal action.

All personnel suspected of having committed a security breach or deviation will be entitled to due process, fair treatment, and a full investigation to protect their legal rights.

INFORMATION TECHNOLOGY GOVERNANCE POLICY
PT Elang Mahkota Teknologi Tbk
("Company")

Additional Information related to Breach of Company Information Security

Tahun	Total Number of Information Security Breaches	Total Number of Clients, Customers and Employees Affected by the Breaches
2020	0	0
2021	0	0
2022	0	0
2023	0	0
2024	0	0