Loxley Pubic Company Limited

| | |
|---|---|
| Document Title: Information Security Policy | Document Code: LOXLEY-ISMS-POLICY |
| Document Type: Internal Use Only | Revision Number: 00 |
| Implementation Date: May 15, 2023 | Page: **1** of **5** |

# Information Security Policy

## Loxley Public Company Limited

Loxley Public Company Limited and its subsidiaries (as per the attached document), hereinafter referred to as the "Company," have implemented information systems to facilitate, enhance, and improve work efficiency and effectiveness. Additionally, the concept of "GRC" (Governance, Risk, and Compliance) has heightened awareness among organizations regarding "Regulatory Compliance," such as adherence to various laws and regulations. Examples include the Computer Crime Act, the Electronic Transactions Act, the Cybersecurity Act, the Personal Data Protection Act B.E. 2562 (2019), and other relevant laws.

This policy aims to ensure that the Company's services and operations are conducted seamlessly and appropriately, in alignment with the Company's business policies. It also seeks to prevent issues arising from improper use of information systems, whether by users or from internal and external threats, which could potentially harm the Company's business. Additionally, it ensures that the Company's information systems are managed effectively, securely, and reliably, adhering to established standards and best practices for information system security, as well as complying with relevant laws and regulations. To this end, the Company has established the following Information Security Policy as follows:

1. **Organization of Information Security**

   The Company must define the roles and responsibilities of individuals involved in governing, overseeing, and performing duties related to information security. These roles and responsibilities must be clearly outlined and communicated to employees and relevant parties to ensure accurate adherence to policies, regulations, and requirements.

2. **Human Resource Security**

   The Company must establish measures for users or employees to understand their duties, roles, and responsibilities. It should also promote awareness and strict adherence to their information security responsibilities, thereby safeguarding the Company's interests.

**3. Assets Management**

The Company must have measures in place to identify its information assets, as well as assign appropriate responsibilities for the use and protection of these assets. Additionally, the Company must determine suitable levels of protection for its information in accordance with the importance of the data to the Company. This is to prevent unauthorized disclosure, alteration, transfer, deletion, or destruction of the Company's information.

**4. Access Control**

The Company must establish measures to control unauthorized access to its information systems. It must ensure that individuals accessing the information systems can be accurately verified, tracked, and identified. Furthermore, the Company should encourage users to take responsibility for collectively safeguarding the Company's data to ensure the security and optimal efficiency of the information systems.

**5. Cryptography**

The Company must establish measures for encrypting data and guidelines for selecting data encryption standards that are appropriate to the risks that may arise from the data at each level of confidentiality. Additionally, the Company must ensure that these measures are consistently followed and maintained according to the policy and procedures.

**6. Physical and Environmental Security**

The Company must have measures in place to protect, control the use, and maintain the physical security of information assets and information equipment that form the infrastructure supporting the Company's information systems. This includes ensuring that the systems are in a complete and operational condition, as well as preventing unauthorized access to information assets or unauthorized disclosure of information.

**7. Operations Security**

The Company must establish measures to ensure that operations with the Company's information systems are conducted correctly and securely. This includes measures to prevent the loss, unauthorized access, leakage, disclosure, alteration, damage, or destruction of data and computer systems.

8. **Communications Security**

The Company must implement measures to control the management of networks and the transmission of data over computer networks, both internally and externally to ensure its security.

9. **System Acquisition, Development, and Maintenance**

The Company must establish measures to reduce errors in defining requirements, and designing, developing, and testing information systems that are newly developed or modified. This includes measures to ensure that the developed or procured systems comply with the predefined agreements.

10. **Information Security Management with External Service Providers (IT Outsourcing)**

The Company must implement measures and frameworks for managing external service providers in the provision or use of information technology services to ensure that these services are effective, secure, and provide maximum benefit to the Company.

11. **Cyber Security Incident Management**

The Company must define procedures for managing information security incidents, learning from mistakes made from the issues that occurred, and making improvements to prevent similar security incidents from occurring again.

12. **Business Continuity Management**

The Company must implement measures to prevent disruptions or interruptions in the Company's business operations, as well as protect critical business processes from the failure of information systems. This includes procedures for recovering information systems to restore normal operations within a reasonable time frame.

13. **Information System Security Risk Management**

The Company must establish a risk management framework for information technology, covering risk identification, risk assessment, risk management, and control to ensure risks remain within acceptable levels. This includes monitoring and reviewing risks, as well as assigning responsible personnel to manage information technology risks, ensuring that these risks are managed appropriately.

**14. Regulatory and Compliance**

The Company must implement measures and guidelines to ensure that all Company operations comply with relevant laws, agreements, contracts, and security requirements that both the Company and its employees must adhere to. This also includes measures to monitor compliance with the established information security policies.

**15. Information Security Reviews**

The Company must review the Information Security Policy to ensure it remains up to date at least once a year, or when there are significant changes. Additionally, the Company must adjust procedures and operations to align with the updated policy.

**16. Policy Dissemination**

Each department is responsible for announcing and disseminating these policies, as well as supporting and responding to the Company's policy.

**17. Enforcement**

This Information Security Policy applies to employees, temporary workers, and permanent staff of Loxley Public Company Limited, and its subsidiaries (as per the attached document), as well as external individuals and third-party organizations providing services to the Company. It will be effective starting the day after the announcement.