Wison Engineering Services Co. Ltd.

Information Security Management Statement

1. Purpose and Scope of Application

Wison Engineering Services Co. Ltd. ("Wison Engineering" or the "Company") attaches importance to the security of its information, data, engineering design deliverables, client data, and information systems. The information security management statement (the "Statement") describes the Company's establishment of a concise and executable information security framework to protect the confidentiality, integrity, and availability of the Company's information and to support continuous business operations.

The Statement applies to Wison Engineering and outlines the Company's general principles for promoting information security management in subsidiaries over which it has operational control. Each subsidiary implements the relevant requirements based on its business nature, applicable laws and regulations, the Company's degree of operational control, and its existing management systems. The Company also sets forth corresponding information security requirements for contractors, consultants, suppliers, and other business partners who have access to the Company's information or systems where applicable.

2. Information Security Commitments

- Continuous Improvement: Continuously enhance information security management through assessments, training, inspections, incident reviews, and tracking of corrective actions.
- Information Protection: Implement classified protection based on information sensitivity to prevent unauthorized access, disclosure, tampering, loss, or destruction.
- Threat Monitoring and Response: Take appropriate measures to prevent, monitor, and respond to malware, cyber-attacks, mis-sending of information, anomalous access, and other security threats.
- Employee Responsibility: Employees shall comply with information security requirements, protect their accounts, devices, and the Company's information, and promptly report any suspicious matters.
- Third-Party Requirements: Conduct appropriate security assessments of key third parties that have access to the Company's information or systems, and specify requirements for confidentiality, access control, and incident notification in contracts.

3. Key Management Measures

3.1 Risk and Vulnerability Management

The Company conducts an information security risk assessment at least once a year, and updates it as needed after the launch of a major system, a significant change, the integration of a key third party, or a major incident. The Company regularly identifies system weaknesses and prioritizes the remediation of high-risk vulnerabilities; if timely remediation is not possible in the short term, temporary mitigation measures should be taken and tracked until closure.

3.2 Information Classification and Access Control

The Company implements classified protection based on information sensitivity, and approves and periodically reviews access permissions in accordance with the principle of least privilege. When employees are transferred or resign from their positions, their access rights shall be adjusted or revoked in a timely manner.

3.3 Business Continuity

The Company identifies critical business and systems and formulates necessary backup, recovery, and alternative operational arrangements. Critical business continuity or recovery arrangements shall be tested or drilled at least once a year, and any identified issues shall be rectified.

3.4 Information Security Incident Reporting and Escalation

When employees and relevant external personnel discover suspicious emails, loss of equipment, mis-sending of information, anomalous access, malware, or other potential incidents, they should immediately report to the information technology department or the designated information security officer. The Company shall carry out recording, assessment, containment, remediation, and recovery based on the severity of the incident, and shall escalate the matter to management, the legal and compliance department, and the board of directors or its authorized committee as necessary. The Company assesses and fulfills applicable external notification obligations in accordance with laws and contracts.

3.5 Training and Awareness

The Company provides employees with induction and annual information security training, covering topics such as account protection, phishing, information classification, device and mobile office security, data processing, and incident reporting.

3.6 Internal Inspection

The Company conducts an internal information security inspection or review at least once a year. For identified issues, the responsible person, corrective measures, and completion date shall be specified, and the issues shall be tracked until closure. The Company may arrange for independent third-party assessments based on risks and business needs.

4. Governance and Responsibilities

The CEO of the Company is responsible for overseeing the Company's material information security risks and matters and for reviewing the Company's information security strategy. The digitalization department is responsible for the management of information security, including application security and operations and maintenance security.

5. Approval and Review

The Statement is approved by the Company's management and is effective from the date of its public release. The Company shall review the Statement at least once a year, and shall update it in a timely manner in the event of significant changes in laws and regulations, organizational structure, business model, key technologies, or the threat landscape.