Information Technology Security Policy

1. Objective and Scope

R&B Food Supply Public Company Limited ("the Company") has established this Policy to define the framework for information security based on three core principles: Confidentiality, Integrity, and Availability. This Policy applies to all directors, executives, permanent employees, temporary employees, and any third parties who access the Company's information assets.

2. Ten Core Control Policies

The Board of Directors requires the Information Technology Management Department to enforce controls and establish Standard Operating Procedures (SOP) covering the following principles:

2.1 Conduct IT risk assessments and policy reviews with experts at least once a year, and consistently promote cybersecurity awareness among employees.

2.2 Maintain a clear separation of duties between the system development group (Developers) and the system administration group (System Administrators) responsible for the production system, to prevent risks of fraud and unauthorized data modification.

2.3 Restrict and record access to the primary and secondary data centers exclusively for authorized personnel, and equip these centers with infrastructure support systems (uninterruptible power supply and fire suppression systems) that meet international standards.

2.4 Information, Network, and System Security:

- Access rights must be granted based on business necessity and confidentiality levels. Transmission of confidential data over public networks must be encrypted at all times.
- User accounts must be assigned strictly on an individual basis. Passwords must be complex, secure, and have an expiration period configured in accordance with IT standards.
- Firewall systems must be installed to control external connections. Anti-malware protection must be maintained and updated every 24 hours, and unauthorized installation of wireless network devices is strictly prohibited.

- All computers and data are considered Company property. Employees must lock their screens every time they leave their workstations, and connecting personal devices to the core business systems is prohibited unless authorized.

2.5 The procurement, development, or modification of computer systems must undergo security testing and User Acceptance Testing (UAT) prior to deployment to the production system.

2.6 Back up business-critical data at a secure off-site location, and conduct IT Business Continuity Plan (IT BCP) drills at least once a year.

2.7 Establish written Standard Operating Procedures (SOP) for IT personnel, and ensure the system maintains computer traffic logs to enable successful retrospective audits.

2.8 IT procurement and outsourcing must include Non-Disclosure Agreements (NDA) and Service Level Agreements (SLA). System access rights must be revoked immediately upon the termination of employment or service contracts.

2.9 Employees must use the internet and electronic mail strictly for the Company's business benefit and in full compliance with the Computer Crimes Act and other relevant legislation. The installation or use of unlicensed or illegal software within the organization is strictly prohibited.

3. Penalties and Enforcement

Any violation of or failure to comply with this Policy, whether intentional or through negligence, shall be deemed a serious disciplinary offense under the Company’s Work Rules and Regulations. If such violation causes damage to the Company, the Company shall pursue civil and criminal legal actions to the fullest extent of the law. Supervisors who neglect their oversight duties shall also be held jointly responsible.

Note: Technical specifications and in-depth operational procedures shall be governed by the Standard Operating Procedures (SOP) approved by the Management.

This Policy was reviewed and approved by the Board of Directors at Meeting No. 5/2025 on November 7, 2025, and shall come into full force and effect from November 10, 2025 onwards.