KONRUT TARIM A.Ş.

INFORMATION SECURITY POLICY

1. PURPOSE AND SCOPE

Konfrut Tarım A.Ş. and its subsidiaries ("Konfrut" or the "Company") recognize corporate information and the continuity of business operations as among their most valuable assets. The purpose of this Policy is to protect the Company's reputation, reliability, and information assets; ensure compliance with the Capital Markets Board of Türkiye Communiqué No. VII-128.10 on Procedures and Principles Regarding Information Systems Management; and safeguard the Confidentiality, Integrity, and Availability of corporate information.

This Policy applies to all employees (permanent, temporary, and interns), members of the Board of Directors, suppliers, and third-party service providers who access, use, manage, or process the Company's information assets and information systems.

2. MANAGEMENT COMMITMENT AND APPROVAL

This Policy has been approved by the Board of Directors of Konfrut Tarım A.Ş. in accordance with the Capital Markets Law and applicable regulations.

The Board of Directors and Senior Management are committed to:

- Ensuring that the information security strategy is aligned with business objectives;
- Identifying risks related to information assets and maintaining an effective risk management process;
- Monitoring information security incidents and allocating the necessary resources, including financial and human resources;
- Ensuring full compliance with applicable laws and regulations, including CMB regulations, the Personal Data Protection Law (KVKK), and the Turkish Commercial Code;
- Promoting information security awareness through regular employee training and awareness programs.

3. ROLES AND RESPONSIBILITIES

3.1. BOARD OF DIRECTORS

The Board of Directors is responsible for establishing the information security strategy, approving this Policy, and overseeing its implementation. The Board shall appoint an Information Security Officer.

3.2. INFORMATION SECURITY OFFICER

The Information Security Officer, appointed in accordance with applicable regulatory requirements, is responsible for monitoring the implementation of this Policy, coordinating risk assessments, investigating security incidents, and reporting directly to Senior Management.

The Information Security Officer shall not perform any executive or operational duties related to the day-to-day management of information systems.

3.3. EMPLOYEES

Regardless of their position, all employees are responsible for safeguarding the confidentiality of Company information, protecting their assigned access credentials (including usernames and passwords), refraining from sharing such credentials with others, and promptly reporting any suspicious activities or security concerns.

4. MAIN INFORMATION SECURITY PRINCIPLES

4.1. ASSET MANAGEMENT AND CLASSIFICATION

The Company shall maintain an inventory of its information assets, including hardware, software, and data. Information assets shall be classified according to their criticality and sensitivity, and appropriate security controls shall be implemented accordingly.

4.2. RISK MANAGEMENT

Information security risk assessments shall be conducted at least annually. Acceptable risk levels shall be defined for identified risks, and risk mitigation measures shall be implemented following Senior Management approval.

4.3. ACCESS CONTROL

Access rights shall be granted based on the principles of "need-to-know" and "least privilege." The use of multi-factor authentication (MFA) is mandatory for remote access solutions (such as VPN connections) and critical systems.

4.4. LOGGING AND MONITORING

Audit trails and log records relating to critical system activities, authorization changes, and attempted security breaches shall be maintained in a manner that preserves their integrity. Such records shall be securely retained for the legally required retention period, and in any case no less than five (5) years.

4.5. OUTSOURCED SERVICES

Contracts with third-party service providers engaged in information systems services shall include provisions governing confidentiality, data security, and service level requirements.

4.6. PHYSICAL AND ENVIRONMENTAL SECURITY

Unauthorized physical access to areas hosting critical information systems, including server and system rooms, shall be prevented. These facilities shall be protected against environmental threats such as fire, flooding, and power outages, and all access activities shall be appropriately monitored and recorded.

5. REVIEW OF THE POLICY

This Policy shall be reviewed at least annually and updated, subject to Board approval where necessary, to reflect changes in business requirements, technological developments, applicable regulations, and the risk landscape.

6. VIOLATIONS AND SANCTIONS

Violations of this Information Security Policy are treated seriously, as they may result in commercial losses, reputational damage, and regulatory consequences for the Company.

Any breach of this Policy shall be assessed in accordance with the Company's Human Resources Practices and Disciplinary Procedures. Depending on the nature and severity of the violation, disciplinary measures may include termination of employment and the initiation of civil and/or criminal legal proceedings where applicable.