SECURITY POLICY

ANAPET TAŞIMACILIK ANONİM ŞİRKETİ's Security Policy reflects our commitment to protecting information, people, and assets. We adopt internationally recognized standards to ensure operational safety, business continuity, and compliance with applicable laws. We expect our employees, contractors, and partners to uphold the same level of integrity and diligence in all operations.

1. PURPOSE AND SCOPE

This Security Policy aims to ensure the security of information, facilities, equipment, and personnel across all operations of ANAPET Taşımacılık A.Ş. It applies to employees, contractors, visitors, business partners, and digital systems.

2. CORE PRINCIPLES

2.1. ***Confidentiality:*** All commercial, operational, and personal data are processed confidentially and accessed only by authorized personnel.

2.2. ***Integrity:*** The accuracy of data and systems is maintained, preventing unauthorized changes

2.3. ***Availability:*** Business continuity is ensured, and systems remain operational 24/7.

2.4. ***Compliance:*** All activities comply with applicable regulations (KVKK, ISO 27001, GDPR, etc.).

3. PHYSICAL SECURITY

Facility access is controlled via card or biometric systems. Visitors are escorted. Critical areas are monitored by cameras. Emergency and fire safety plans are regularly executed.

4. INFORMATION SECURITY AND CYBER PROTECTION

System access is limited by personal accounts and strong password policies. Firewalls, antivirus, and IDS systems are active. Email traffic is encrypted. Annual information security training is mandatory for all staff.

5. DATA PRIVACY

Personal data are processed in accordance with KVKK and GDPR. Confidentiality clauses are included in supplier contracts. Sensitive information is shared only on a need-to-know basis.

6. PERSONNEL SECURITY

All employees sign a confidentiality agreement. Access rights are revoked upon role change or termination. Any security breach must be immediately reported.

7. BUSINESS CONTINUITY AND INCIDENT MANAGEMENT

Critical data are backed up regularly. An emergency response plan is activated in case of cyber-attack or system failure. Root cause analysis is conducted after every incident.

Concerns should be reported to the Compliance Department at info@anapet.net ANAPET enforces a strict non-retaliation policy, ensuring that individuals who raise concerns in good faith are protected from any adverse action.

Violations of this policy may result in suspension or termination of business relationships. By working with ANAPET, all business partners acknowledge their responsibility to uphold these principles and commit to continuous improvement in ethics, safety, and sustainability.