POLICY 08 • KRB-POL-08

Confidentiality and Information Security Policy

DOCUMENT NAME	DOCUMENT NO	PUBLICATION DATE
Confidentiality and Information Security Policy	KRB-POL-08	03.03.2025
REVISION NO / DATE	**PREPARED BY**	**APPROVED BY**
1 / 11.08.2026	Legal and Compliance Department	Board of Directors

8.1 Purpose

The purpose of this Policy is to define the principles, rules and responsibilities for the protection of confidential information, trade secrets, intellectual property assets and personal data owned by Karub Enerji or entrusted to it by third parties, and to safeguard the confidentiality, integrity and availability of information.

For Karub Enerji, as an R&D-intensive technology company, information such as cell and module production recipes, process parameters, test data, design files and customer information is among its most valuable assets.

8.2 Scope

This Policy covers all information owned or controlled by the Company, regardless of the medium in which it is held (printed, electronic, verbal or visual), and all employees, managers, interns, consultants, suppliers and business partners who have access to this information. The obligations continue after the end of the business relationship.

8.3 Legal Basis

- Law No. 6698 on the Protection of Personal Data and its secondary legislation, and the decisions of the Personal Data Protection Board
- Standard contracts, binding corporate rules and explicit consent mechanisms for transfers abroad under Art. 9 of Law No. 6698
- Law No. 5651 on the Regulation of Publications on the Internet
- Art. 396 (non-competition) and the provisions on unfair competition (Art. 54 et seq.) of the Turkish Commercial Code No. 6102
- Art. 396 (employee's duty of loyalty) and Arts. 444–447 (non-competition) of the Turkish Code of Obligations No. 6098
- Arts. 135–140 (offences relating to personal data) and Art. 239 (disclosure of information constituting trade secrets) of the Turkish Penal Code No. 5237
- Industrial Property Law No. 6769 and Law No. 5846 on Intellectual and Artistic Works
- The EU General Data Protection Regulation (GDPR) — to the extent it applies
- ISO/IEC 27001 Information Security Management System standard

8.4 Definition and Classification of Confidential Information

Confidential information is any information that is not publicly available and whose disclosure could harm the Company, its employees, customers or business partners. This includes in particular: production recipes and process parameters, technical drawings and designs, R&D project outputs and test results, inventions not yet the subject of a patent application, cost and pricing data, bid and tender information, customer and supplier lists, contract terms, financial data and business plans, employee personnel and salary information, and security information relating to information systems.

Information is classified into four levels: "Public", "Internal Use", "Confidential" and "Strictly Confidential". Access, storage, transmission, reproduction and destruction rules are defined separately for each class and documents are labelled accordingly.

8.5 Basic Confidentiality Obligations

- Confidential information is used only to the extent required by the work and within the framework of the "need-to-know" principle.
- Confidential information may not be shared with unauthorised persons — including other employees within the Company.
- Sharing information with third parties must be based on a written non-disclosure agreement (NDA) signed in advance.
- Confidential information may not be copied to personal devices, personal e-mail accounts, unapproved cloud services or removable storage media.
- Confidential information may not be shared on social media, at conferences, in press statements or in publicly available artificial intelligence tools.
- Upon termination of the business relationship, all confidential information and all media containing it are returned to the Company; no copies may be retained.
- The confidentiality obligation continues indefinitely after the termination of the employment contract.
- Obtaining and using competitor information from third parties by unlawful means is prohibited.

8.6 Protection of Personal Data

In its capacity as data controller, the Company complies with the general principles set out in Art. 4 of the KVKK with regard to the personal data it processes: lawfulness and fairness; accuracy and being up to date where necessary; processing for specific, explicit and legitimate purposes; being relevant, limited and proportionate to the purpose; and retention only for the period stipulated by the legislation or required for the purpose of processing.

- Personal data is processed only where one of the processing conditions listed in Arts. 5 and 6 of the KVKK exists.
- Data subjects are informed in accordance with KVKK Art. 10 before the data processing activity; explicit consent is obtained where necessary and data subjects are informed that consent may be withdrawn.
- A Personal Data Processing Inventory is prepared and kept up to date; the VERBİS registration obligation is fulfilled to the extent the Company falls within its scope.
- Retention periods are determined in accordance with the Personal Data Retention and Destruction Policy; at the end of the period, data is deleted, destroyed or anonymised.
- Data processing agreements compliant with the KVKK are concluded with parties from which services are received in the capacity of data processor.

- Transfers abroad are carried out under Art. 9 of the KVKK on the basis of an adequacy decision, appropriate safeguards (standard contracts, binding corporate rules) or exemption provisions, and notification obligations to the Authority are observed.
- Data subject requests are resolved within thirty days at the latest in accordance with the Communiqué on the Procedures and Principles of Application to the Data Controller.
- Employee monitoring activities (cameras, log records, vehicle tracking, e-mail monitoring) are carried out only for legitimate purposes, proportionately and with prior notification of employees.
- The use of cookies on the corporate website is managed transparently through a separate Cookie Policy and a cookie management tool; explicit consent is obtained for non-essential cookies.

8.7 Protection of Intellectual and Industrial Property Rights

The rights in inventions, designs, software and works produced by employees in the course of their employment belong to the Company within the framework of the legislation and contractual provisions. Notification and remuneration processes for employee inventions are conducted in accordance with the provisions of the Industrial Property Law. Technical solutions for which a patent application is planned are under no circumstances disclosed before the filing date; access restrictions are applied to information that is preferred to be protected as a trade secret. The intellectual property rights of third parties are respected; the use of unlicensed software is prohibited.

8.8 Information Security Measures

- **Technical measures:** firewall and network segmentation, endpoint protection and malware detection, disk and transmission encryption, multi-factor authentication, authorisation and role-based access management, logging and monitoring, patch and vulnerability management, regular backups and backup restoration tests.
- **Administrative measures:** information security awareness training, phishing simulations, clean desk and clear screen practice, confidentiality undertakings, onboarding and offboarding authorisation processes, supplier security assessment.
- **Physical measures:** card-access control to production areas, server rooms and R&D laboratories, visitor registration and escort arrangements, camera surveillance in critical areas, use of locked cabinets and document shredders for paper documents.
- Unauthorised photography and video recording in production and laboratory areas are prohibited.
- Business continuity and disaster recovery plans are prepared and tested regularly.

8.9 Incident Management

Any actual or suspected information security or data breach is reported without delay to the Information Technology Department and the Legal/Compliance Department. Breach incidents are managed according to a response procedure comprising the stages of detection, containment, root cause analysis, remediation and reporting. In the event of a personal data breach, the Personal Data Protection Board is notified as soon as possible and in any case within seventy-two hours; the data subjects concerned are informed within the shortest reasonable time. Breach records are kept and measures are taken to prevent the recurrence of similar incidents.

8.10 Sanctions, Monitoring and Entry into Force

A breach of this Policy may give rise to disciplinary sanctions up to termination of the employment contract for just cause, liability for damages and criminal liability in respect of acts constituting an offence. Contractual sanctions are applied in the event of breaches by third parties and the relationship may be terminated.

The effectiveness of the Policy is monitored through the number of breach incidents and response time, the awareness training completion rate, the phishing simulation success rate, the number of data subject requests and response time, and audit findings. The Policy is reviewed at least once a year or immediately in the event of a change in legislation and enters into force upon approval by the Board of Directors.

PREPARED BY

Legal and Compliance Department

Name – Surname / Signature / Date

APPROVED BY

Board of Directors

Name – Surname / Signature / Date