KOLUMAN
INFORMATION AND DATA SECURITY POLICY

KOLUMAN

Compliance Program

1. Purpose and Scope

Information is one of Koluman Holding's most valuable assets. Our information security policy aims to ensure the confidentiality, integrity, and availability of information obtained by all our employees, business partners, and stakeholders within the scope of the company's business processes. Our policy adopts best practices in information security, ensuring the company's compliance with legal regulations, the Personal Data Protection Law (KVKK), and international standards.

This policy covers the employees, managers, suppliers, contractors, customers, and business partners of Koluman Holding and its affiliated companies.

2. Information Security Principles

Our information security policy is implemented within the framework of the following fundamental principles:

Confidentiality: All critical information and personal data are protected against unauthorized access.
Integrity: The accuracy and immutability of information is ensured, preventing unauthorized changes.
Availability: Authorized users are provided with secure and uninterrupted access to the information they need, within the framework of established rules.
Compliance with Legislation: Full compliance is ensured with all relevant legislation, such as the Personal Data Protection Law, Competition Law, and Occupational Health and Safety Law.
Continuous Improvement: Information security systems are regularly reviewed, risks are analyzed, and continuous improvement is ensured.

3. Protection and Processing of Personal Data

Koluman Holding processes and protects the personal data of its employees, customers, and business partners in accordance with the following principles under the Personal Data Protection Law No. 6698 (KVKK):

Processing in accordance with the law and principles of good faith
Processing for specific, clear, and legitimate purposes
Processing that is relevant, limited, and proportionate to the purpose for which the data is processed
Maintaining data accuracy and currency
Retention for the period specified in the relevant legislation, followed by destruction
All personal data processed within the company is protected against unauthorized access, made accessible only to the extent required for the task, and the rights of data subjects are protected.

4. Cybersecurity and Technological Measures

Koluman Holding implements advanced cybersecurity measures to ensure the security of its information systems:Firewalls and Network Security: Network security measures are implemented to prevent unauthorized access.
Encryption and Data Protection: Sensitive information is protected using cryptographic methods.
Access Authorization: Access to information is granted only to authorized individuals and is regularly monitored.
Malware Prevention: Company systems are protected using anti-virus and threat detection systems.
Social Engineering and Fraud Prevention: Employees are regularly informed about cyber attacks and fraud attempts.

5. Physical and Electronic Information Security

The protection of information is not limited to digital environments. Koluman Holding takes the following measures to ensure information security in both physical and electronic environments:

Office and data center security is ensured, and unauthorized access is prevented.
Documents and files are stored in secure storage areas.
Security measures are taken against external threats with CCTV and access control systems.
Physical documents are destroyed in accordance with established procedures.

6. Risk Management and Emergency Planning

Koluman Holding implements a proactive Risk Management Program to identify, assess, and minimize information security risks:

Potential threats are identified and risk analyses are conducted regularly.
Additional security measures are taken for high-risk processes.
Crisis management and emergency plans are prepared to respond to information security breaches.
Relevant authorities and affected parties are notified in a timely manner in the event of a potential data breach.

7. Education and Awareness Activities

Information security can be ensured not only through technological measures but also through the awareness level of employees. Therefore;
All employees receive regular information security training.
Awareness campaigns are conducted regarding cyber attacks, data leaks, and fraud.
Content that raises awareness about compliance and ethical principles is shared.

8. Information Sharing and Relations with External Organizations

Koluman Holding regulates the sharing of critical information, including trade secrets and personal data, with external organizations within a specific framework of rules:

All business partners and suppliers are obligated to comply with information security standards.Information sharing with external stakeholders is conducted only in accordance with business requirements and with written approval. Sanctions are imposed on those responsible for information security breaches.

9. Compliance and Audit Mechanism

To ensure the effective implementation of information security policies, internal audit and corporate risk management processes are conducted as follows:
Regular information security audits are performed.
Compliance violations and data security vulnerabilities are investigated in detail.
Annual risk assessments are conducted, and policy updates are implemented.
Regular feedback is provided to company employees and stakeholders regarding compliance processes.

10. Effectiveness and Updates

First Publication Date	Revision Date/No.	Explanation
08.04.2025	-	-

Compliance Programme

KOLUMAN