

POLICY ON INFORMATION CONFIDENTIALITY AND SECURITY



1. Objective and Scope of the Policy

This Policy has been drawn up for the purpose of regulating the principles and measures to be complied with and taken into account by the Limak employees to ensure and maintain the confidentiality, security, integrity and continuity of all sorts of confidential information. Limak employees are aware of the fact that use and disclosure of any sorts of information in breach of this policy shall adversely affect the competitiveness of Limak and inflict damages and losses on Limak. In this manner, Limak employees are aware that they are responsible for the use and disclosure of confidential information in accordance with the principles and procedures contemplated in this policy, and for ensuring and protecting the confidentiality and security of the information and security and accordingly emphasizes on to aspect.

2. Information Confidentiality

In accordance with the Turkish Code of Obligations No. 6098 and Labor Law No. 4857, the employees are liable and responsible to protect and retain all sorts of confidential information thoughtfully particularly the business and/or trade secrets within the framework of loyalty obligation towards Limak. This obligation of the employees survives throughout the employment relationship and upon the termination of the employment relationship for any reason whatsoever. Limak employees, in accordance with the employment agreement concluded with Limak, are liable and responsible of the confidentiality of the information and documentation acquired during their jobs, duties and positions related to their works performed. Confidential information shall not be used and disclosed to the third parties in breach of this policy.

2.1. Definition of Confidential Information

Confidential information includes all sorts of information in any format including, but not limited to, commercial, financial, operational, contractual, technical information, trade secrets, information subject to intellectual property, inventions, ideas, personal data, all kinds of documents, reports, information notes, analyzes, compilations, summaries, project descriptions, licenses, permits, business plans, processes, strategies and methods, explanations about current potential projects and products, know-how, software, customer lists, information about pricing and information that is obliged to ensure its confidentiality within the scope of "confidentiality agreements" concluded with third parties, and information obtained through these ("**Confidential Information**").

The confidential information can belong to Limak as well as the parties in relation with Limak within the scope of its activities and operations (employees, business associates, suppliers, customers and stakeholders, etc.) or even the competitors.

2.2. Disclosure and Use of Confidential Information

Limak employees are only entitled to disclose the confidential information and share with the third parties under the circumstances hereinbelow:

- In case disclosure of the confidential information to the relevant third parties is required within the scope of the ordinary activities and operations of Limak and only to the limited extent to

these activities and operations, the non-disclosure agreement shall be concluded between the parties or an affirmative covenant shall be issued in written for the third parties for the purpose of determination of the use and security of the confidential information disclosed,

- Provided that the previously affiliated director is notified, the instructions of the competent authorities and courts or provisions of the relevant legislation shall be applied,
- In case of disclosure of the confidential information of the third parties, the written consent of the relevant third parties shall be obtained,
- In case of any requirement for the disclosure of the confidential information without the non-disclosure agreement/affirmative covenant, prior written authorization of Limak and/or affiliated director shall be obtained accordingly.

Limak employees are responsible to comply with and abide by as well as practice due diligence for the principles stated hereinbelow within the scope of the disclosure and use of the confidential information:

- Even in circumstances where the relevant information is not stated to be and flagged as confidential information in written or verbally, all sorts information that can be classified as confidential information are required to be protected and treated as confidential information.
- Confidential information can only be disclosed solely for the purpose of designated purposes and to the employees required to know due to their duties and tasks and accordingly used by these individuals for this purpose.
- Except the circumstances stated hereinabove, confidential information cannot be disclosed to the third parties. This rule shall also apply to the family members of the employees and the employees not required to know the confidential information as well as the former employees.
- Confidential information cannot be reproduced, amended and destructed without the prior authorization.
- No disclosure, intercourse and endeavors can be performed regarding the confidential information at location where it can be exposed to the third parties or public domain, and through the social media accounts and mobile applications.
- Confidential information of the third parties, including the competitors of Limak, cannot be provided in violation of the law and code of ethics and such confidential information is required to be safeguarded and shared by exercising the same due diligence and care as if such information belongs to the employees and/or Limak. In case of acquisition or use of confidential information in breach of these rules, the relevant Limak employees are obliged to notify this situation promptly to the affiliated director.
- No employee is entitled to exert pressure on and compel another employee for the disclosure of confidential information in possession or been aware of.
- Law on Protection of Personal Data No. 6698 and secondary legislation shall apply during the performance the processes related to the confidential information.
- Limak employees are required to protect confidential information against unauthorized access, use or destruction within the framework of this policy and other policies and practices of the Department of (Limak Technology) Information Technologies and take the required measures and precautions.
- The employees, when leaving the duty in Limak, are obliged to return the entire confidential information (including originals and copies) accessed during the works.
- Limak employees are advised and encouraged to consult with the Legal Department regarding the practices and applications with the confidential information.

3. Information Security

Limak takes the required measures within the scope of information security in order to ensure that the privacy, integrity, continuity and access of sorts of information stored and retained in various means, both physically and electronically are safeguarded and meticulously protected and to prevent the factors threatening and compromising the security thereof. Limak employees are aware that such information constitutes a substantial and significant part of Limak's assets.

The employees shall comply with and abide by the principles stated hereinbelow and take the required measures and precautions to ensure the security of the information accessed by means of physical and/or information technology systems and used:

- Limak employees are not entitled to use the information they shall access to while performing their duties and tasks in breach of the relevant legislation, this policy and other applicable practices and policies within Limak.
- Limak employees, in case of disclosure of information to the third parties is required, take cognizance of the principles of this policy on the disclosure and use of the confidential information and act accordingly in this regard.
- Limak employees further take cognizance of the precautions and measures required to be applied in terms of confidential information in the nature of personal data and accordingly perform and follow-up required processes for the finalization and conclusion by the relevant units of the information requests communicated by the persons with the personal data processed in this regard.
- Access to information is solely authorized to the competent Limak employees defined and to the limited extent in order to perform the ordinary activities and operations of Limak.
- Limak employees are not entitled to disclose and share information such as user name, password, etc. of the ones accessing to such information to anyone including other employees of Limak and accordingly shall hold such information confidential. Limak employees, in case of becoming suspicious of the existence of circumstances posing a threat to the confidentiality and security of such information, are promptly required to take the required precautions and measures and consult with Department of (Limak Technology) Information Technologies.
- In case of performance of any alterations and changes on the information, alteration logs are maintained and retained within the servers hosting the information.
- The information and documentation are required to be stored and maintained within the premises of Limak and not to be removed and taken out of the premises. In the event that it is required to remove or take out this information out of the premises, Limak employee shall seek for the prior approval of his/her director and/or other persons in charge for the confidentiality and security of the information.
- Limak employees shall use the information to be accessed during the performance of their duties within the framework of the principles and rules notified by Limak by means of devices and means assigned.

In terms of ensuring the security of the information;

- Information stored on the physical environment and means is required to be maintained in a specific manner and securely at the areas notified by the persons responsible for the retention of the relevant information or at the closets assigned for the personal use of Limak employees and under no circumstances not to the left unattended and exposed for the access of other persons at the common areas of the Limak premises (meeting rooms, printer, fax machines, etc.).
- Policies on the information access, security, use, storage and destruction have been determined for the information stored within the information technology and training and awareness raising

endeavors for the employees on the information security are performed and conducted at certain intervals, authorization matrix and access logs are regularly maintained, user account management is monitored, situations including risks are reviewed, the required technological solutions are produced, precautions and measures are taken to ensure the security of all sorts of mediums hosting the information and data loss prevention software is used for the purpose of ensuring the continuity of storage of information and information and data are backed up, the relevant network and application security measures and cyber security security precautions are taken against the adverse conditions such as loss of data, unauthorized access, copying, unauthorized alteration and applications and practices related to those are regularly monitored and the audits and inspections are performed and conducted accordingly.

The top management explicitly commits to meeting all applicable requirements related to information security and, while taking all necessary measures to ensure the continual improvement of the Information Security Management System, will also provide the required leadership and commitment.

4. Implementation

Limak employees, in case of any hesitation related to the implementation of the principles and measures contemplated in this policy or in case they are convinced of an occurrence of a breach or violation or become aware of such breaches or violations, shall consult with the opinion of the Ethical Committee or notify this situation to the Ethical Committee.