"APPROVED"

By the Resolution of the 14th meeting of "Almalik KMK" JSC Supervisory Board on August 30, 2023

"Almalik KMK" JSC Breach Notification Policy

1. General rules

1. "Almalik KMK" JSC (hereinafter - the Company) strives to ensure that the employees of the company adhere to the high standards of ethics and principles defined in the Code of Conduct of the company. The Code of Conduct requires all employees to report in good faith any actual or potential violation of the Code and any other illegal, unlawful, unethical or dangerous activity.

2. The Company regulates the purpose, application, authority to which to report violations, as well as protection of the whistleblower after bona fide appeals, with this Policy on Notification of Violations (hereinafter referred to as the "Policy").

2. Purpose and Scope of Policy Application

3. The purpose of the policy is to reinforce the obligation of Company employees to report their concerns and suspected wrongdoing and to assist the Compliance Department and/or Internal Audit Department in their work.

4. The Company undertakes to protect from harassment those employees who fulfill these obligations in good faith. The policy also explains to employees what constitutes protected activity, what notification channels to use, and in what exceptional circumstances an employee may disclose relevant information to an authorized outside party.

5. The policy aims to clarify the issues of anonymity and confidentiality, and describes the measures that the Company takes to protect applicants and combat any harassment related to illegal behavior.

6. This policy applies to all employees of the company, including members of the Executive Body.

3. Basic concepts and rules

7. **Behavior that violates the established norms** means that the employee of the Company does not comply with the Code of Conduct of the Company.

8. ***Protected activity*** includes sending a message containing information about potential misconduct through the channel specified in this Policy. Protected activities also include assisting the Compliance Officer and/or the Internal Audit Officer in their legal activities.

9. ***Chasing*** means any direct or indirect harm or harmful act suggested, threatened or committed against the applicant as a result of participation in protected activity. Harassment may include, but is not limited to, discriminatory treatment, changes in pay, demotion or transfer to another job position, or dismissal.

10. ***Applican***- an employee of the Company engaged in protected activity.

11. Company employees must report suspected cases of unethical behavior that has occurred or may occur, or any actions that may or may harm the company's mission and reputation.

12. To be protected by this Policy, the applicant must have reasonable grounds to believe that the information is accurate. Employees who knowingly report false or misleading information are not considered applicants and therefore are not provided with the protections provided in this Policy. Submitting false information constitutes a violation of the Code and may be subject to investigation by the Compliance Department and, if found, to disciplinary action.

13. The Company encourages employees to report their suspicions or concerns, knowing they will be protected from harassment. Identifying the whistleblower can help the Company determine the credibility of the complaint. Also, under certain circumstances, the applicant employee may request that his identity remain anonymous or not disclosed.

14. No employee may use his position to prevent other employees from exercising their rights or performing their duties.

4. Policy implementation

15. The applicant must notify the Compliance Service about the violations, the authorized person in the Compliance Service must receive the messages, provide relevant information and provide assistance if necessary, and also ensure that appropriate measures are taken after receiving such a message.

16. The authorized person is appointed by the head of the Compliance Service and works in close cooperation with him. The authorized person is responsible for ensuring adequate knowledge of the organization's notification processes, receiving any notifications and ensuring that such notifications are reviewed by the appropriate authorities, as well as maintaining contact with the

party submitting the notification and keeping them informed of updates in this regard.

17. The applicant may send a message using one of the following methods:

by e-mail;

by mail;

by hotline;

by contacting the authorized person directly.

18. To facilitate proper verification and evaluation of submitted messages, the following information should be included in the message whenever possible:

a detailed description of an event that has occurred or may occur;

the place, time and date of the incident or when and where it is likely to occur;

the name and position or other identifying information of the person(s) involved in the incident;

the name and position of the person submitting the message, if the message is not submitted anonymously;

the reasons that led to the submission of the notice or complaint;

references to available documents confirming the reliability of the reported facts.

19. If the applicant does not want to report it to the Compliance Service through one of the methods described above, he can report it to the head of the Human Resources Department, the head of the Internal Audit Service, or the director of the company. Upon receipt of a notice, the applicable recipient must immediately submit the notice to the Compliance Service. Messages sent to any other head of the Company should be immediately forwarded to the Compliance Service or one of the constituent units of the Company mentioned above.

20. The Company encourages non-anonymous messages with as much detail as possible. This will assist in any further action to determine whether the complaint is valid. The applicant can also submit a message anonymously using any communication channels or request that his identity not be disclosed. If the

whistleblower identity is unknown, the authorized officer will do all efforts to protect the whistleblower's identity Otherwise, the Company will not be able to offer the protection provided in this Policy.

21. The identity of the applicant will be considered as anonymous as possible, except when the applicant has agreed to disclose his identity and otherwise required by law. In this case, the Company must notify the applicant before disclosing his identity.

22. The Company encourages applicants to use the internal channels outlined in this Policy to report issues. Internal reporting provides the Company with the ability to prevent dishonest acts or conduct that violates established norms, as well as protection from harassment.

23. The Company shall, in exceptional circumstances, ensure that applicants report any suspected acts of non-compliance with the Company’s external norms. In order for such external disclosure to be afforded the protections provided in this Policy, this notice is necessary to prevent:

that there is a serious threat to public safety or health;

serious damage to Company or violation of national and international law.

24. A person who decides to submit an external report must strictly comply with the above conditions in order to be protected under this Policy, unless that person has made the report anonymously.

25. The Company prohibits harassment of applicants who engage in protected activities. Harassment by employees, if discovered, is considered misconduct that may result in disciplinary action.

26. Any applicant who believes that he/she has been subject to persecution, using the notification channels indicated above must submit all information and documents supporting the claim of harassment to the Compliance Service. The Compliance Service will prevent harassment within the jurisdiction, as well as maintain contact with the applicant and provide updates on the reporting process.

5. Rights of employees involved

27. Employees who are or may be the subject of a report must be notified immediately of the allegations against them, unless such notification would prevent the investigation of the situation.

28. Since the notification of violations and subsequent procedures are related to the processing of personal data, these data will be considered in accordance with the rules established by the applicable regulatory legal documents and the company's internal documents on the protection of personal data.

29. The department responsible for this Policy is the Compliance Service. The Compliance Service is responsible for ensuring that the Policy is up-to-date and demonstrating best practices. The authorized officer is responsible for ensuring the effective application of the Policy.

30. Each manager must follow this Policy within the scope of his/her functional responsibility, lead by example and provide guidance to subordinates.

6. Monitoring compliance with the Breach Notification Policy

31. The Compliance Service reviews the Policy at least once every two years or periodically as necessary to determine the necessary changes and additions to the goals of the Policy, as well as to ensure compliance with applicable laws and internal policies and procedures of the company.

32. Any changes to the policy will be approved by the Supervisory Board on the recommendation of the Anti-Corruption and Ethics Committee of the Supervisory Board.