Approved by the resolution
of the Board of Directors
of PCLL “KMG Kashagan B.V.
dated October “18” 2024.

Information Security Policy of PCLL “KMG Kashagan B.V.”

Ensuring information security (IS) is one of the priority areas in the framework of the Mission implementation, the achievement of the Vision and strategic goals of PCLL "KMG Kashagan B.V.". For these purposes, PCLL “KMG Kashagan B.V.” implements and maintains an information security management system (ISMS).

1. The PURPOSE of this Policy is to comprehensively protect the interests of PCLL “KMG Kashagan B.V.”, its branch in the RoK, its employees, as well as counterparties from threats in the field of information and communication technologies, including by ensuring and constantly maintaining the following state of the corporate computer network:

- availability of processed information for authorized users;
- stable operation of the local area network;
- ensuring the confidentiality of information stored, processed on computer equipment and transmitted through communication channels;
- integrity and authenticity of information stored and processed in the local area network and transmitted through communication channels.

2. The OBJECTIVES of this Policy are:

- protection against interference by unauthorized persons in the operation of the local area network;
- differentiation of access of authorized users to information, hardware, software and, if necessary, cryptographic means of protection used in the local area network;
- log user actions when using local area network resources in system logs;
- periodic monitoring of the correctness of the actions of users of the system by analyzing the contents of logs;
- control of the integrity (ensuring immutability) of the program execution environment and its restoration in case of violation;
- protection of information from unauthorized modification, distortion, deletion;
- control of the integrity of the software used, as well as protection of the system from the introduction of malicious codes, including computer viruses;
- protection of trade secrets and personal data from leakage, unauthorized disclosure or distortion during its processing, storage and transmission, including through communication channels;
- ensuring authentication of users participating in the information exchange;
- timely identification of IS threats, causes and conditions that contribute to damage;
- creation of a mechanism of rapid response to threats to IS and negative trends;
- creating conditions for minimizing and localizing the damage caused by illegal actions of individuals and legal entities, reducing the negative impact and eliminating the consequences of information security violations;
- as well as other tasks defined by the applicable norms of the Kingdom of the Netherlands, the legislation of the Republic of Kazakhstan , including the Law of the Republic of Kazakhstan dated November 24, 2015, No. 418-V "On Informatization"; the Decree of the Government of the Republic of Kazakhstan dated December 20, 2016, No. 832 "On the approval of unified requirements in the field of information and communication technologies and information security"; the ISMS standards ISO/IEC 27001, ST RK ISO/IEC 27001, and ST RK ISO/IEC 27002, as well as the Corporate Information Security Standard of JSC "Samruk-Kazyna" (Protocol No. 40/24 dated 25.07.2024).

The PRINCIPLES of this Policy are:

❖ supporting the achievement of the business goals of the Company;
❖ prevention of risks and threats in the field of IS of the Company;
❖ ensuring confidentiality, availability and integrity of Company information assets;
❖ compliance with international standards in the field of IS;
❖ ensuring the continuity of operation of the Company's ISMS.

This Policy provides the basis for the regime and guidance in the development of IS rules, methodologies, regulations and instructions.

The management of the Company assumes responsibility for the organization of IS provision in the Company, declares its commitment to the above goals, objectives and principles.

All Employees of the Company shall comply with the requirements of this Policy and ensure IS within the scope of their activities. Employees of the Company shall inform their direct supervisors and representatives of the IS division about violations and deviations from the requirements of this Policy and other regulatory documents in the field of IS approved in the Company.