Privacy Policy

NC KTZ JSC is a transport and logistics company of national importance, part of the assets of Samruk-Kazyna Joint Stock Company. The implementation of this activity is related to the management of information, including that transmitted by the state, which is an important asset of NC KTZ JSC and depends on ensuring information security, which means the confidentiality, integrity and availability of assets in accordance with the Rules for the identification, classification and labeling of assets related to information processing tools approved by a separate local act.

The scale of the Company's activities has a significant impact on all aspects of the country's socio-economic development, and the multiplicity of stakeholders imposes enormous responsibility on NC KTZ JSC.

The Company sees one of the foundations for a stable economic position and further development in the maximum satisfaction of customer requirements and expectations in the field of information security.

The information security management system (hereinafter referred to as the ISMS) is part of the management system of NC KTZ JSC. In order to determine the procedure for organizing work to ensure the safety of trade secrets of NC KTZ JSC, the Rules for ensuring the safety of trade secrets of NC KTZ JSC have been adopted (approved by the decision of the Board of NC KTZ JSC dated November 6, 2020 No. 02/36). The rules for ensuring the safety of trade secrets of NC KTZ JSC apply to all activities, including suppliers, taking into account the expectations of all stakeholders and is mandatory for fulfillment by all employees of NC KTZ JSC and its subsidiaries in the process of forming a portfolio of investment projects, and is also brought to the attention of clients and other third parties who have access to information systems and documents of NC KTZ JSC , in the part that is directly related to NC KTZ JSC and its activities.

The ISMS is based on a risk-oriented approach aimed at reducing the likelihood of information security events occurring. Ensuring information security is necessary to reduce risks and economic losses associated with various threats to the existing information resources of NC KTZ JSC and its subsidiaries.

The main objects of information security protection in JSC "NC "KTZ" and UP are the following elements:

1) information resources containing information classified in accordance with current legislation and local acts of JSC NC KTZ and its subsidiaries as a commercial, official or other secret protected by law, including information resources included in the projects of the Digital Railway programs and Transformation programs at NC KTZ JSC (hereinafter referred to as protected information);

2) information technology tools and systems (computer equipment, information and computing complexes, networks, systems) on which the processing, transmission and storage of protected information is carried out;
3) software (operating systems, database management systems, other general system and application software) of automated systems of JSC NC KTZ and its subsidiaries, with the help of which protected information is processed;
4) processes of NC KTZ JSC and subsidiaries related to the management and use of information resources;
5) premises in which the means of processing protected information are located;
6) work premises and offices of employees of NC KTZ JSC and subsidiaries, premises of NC KTZ JSC and subsidiaries intended for conducting closed negotiations and meetings;
7) employees of NC KTZ JSC and subsidiaries who have access to protected information;
8) technical means and systems that process open information, but are located in premises in which protected information is processed;
9) virtual environments (computing resources or their logical combination, abstracted from hardware implementation, providing logical isolation from each other of computing processes running on the same physical resource) when using server infrastructure

When developing and applying information security tools and methods, the requirements of contractual obligations and contracts concluded by NC KTZ JSC and subsidiaries with third parties are taken into account. Third party access to the information resources of NC KTZ JSC and its subsidiaries is carried out only after analyzing the risks that may arise when providing such access and taking adequate protective measures. In particular, it is envisaged that a third party will provide confirmation of the compliance of the connected/integrated systems, as well as an audit by NC KTZ JSC of their infrastructure for compliance with information security requirements.

Responsibility for managing the processes of development, implementation, and monitoring of the ISMS is assigned to the Information Security Service.

The Information Security Service, in accordance with the tasks assigned to it, organizes and takes measures to ensure information security, including the following functions:

1) formation and implementation of a unified information security policy of the Company and its subsidiaries through the development and implementation of a comprehensive security system, concepts, standards, methods, regulations and other internal documents in the field of information security and risk management in the supervised area of activity, as well as updating and coordinating them execution by group of companies;
2) conducting internal audits and internal investigations into information security incidents, incl. facts of violations of property and non-property rights and interests of the Company, if necessary, taking measures to eliminate identified violations;

3) implementation of measures to improve the level of information security, organization and coordination of processes related to the training of Company employees and their involvement in the field of information security, conducting briefings, exercises and training, including with management personnel;
4) development, documentation, implementation, monitoring, execution and improvement of control procedures, maintaining the effective functioning of the internal control system within the framework of its powers, enshrined in the Company's local regulations;
5) study and assessment of the state of information security, identification of information and technical resources to be protected, formation of requirements for information protection during the creation and development of informatization objects;
6) identification and analysis of threats to information security in relation to the Company and its subsidiaries, vulnerabilities of information systems, software, software and hardware and taking measures to eliminate them;
7) risk management within the functions and powers of the Service, as well as making management decisions on the activities of the Service taking into account risks;
8) other functions, the implementation of which will contribute to the implementation of the goals and objectives of the Service.

The Company provides the necessary organizational and technical conditions for maintaining the confidentiality of customer information, including by:
1) control over compliance with the Company's trade secret regime;
2) investigation of facts of leakage of information constituting a commercial secret of the Company;
3) checking user workstations and communication channels for leakage of information constituting a trade secret;
4) approval of the transfer of information constituting a trade secret. When the Company enters into civil law contracts, the execution of which is related to the provision (transfer) of information to counterparties, the nature of the information collected, the use of the collected information that constitutes a trade secret, a Confidentiality Agreement is concluded in the form approved by a separate local act, or the conditions for maintaining confidentiality are taken into account in the concluded with the counterparty document (the conditions for the possibility for customers to decide how personal data is collected, used, stored and processed are also taken into account).
5) development of documents on the protection of information constituting a commercial secret of the Company;
6) development of the List and its updating taking into account the proposals of the Company's joint venture, while updating should be carried out when the List, the subject of work, the direction of activity, market conditions and external environment, as well as when the legislation of the Republic of Kazakhstan changes;
7) identification of types and potential sources of threats to information,

requiring protection, analysis of vulnerabilities and risks;
8) use of appropriate information security tools.

Since 2012, NC KTZ JSC has been certified in accordance with the requirements of the international standard ISO/IEC 27001:2013 in the field of information security management. NC KTZ JSC also entered into a contract with QazCloud LLP for the provision of services to identify technical channels of information leakage and special means, including carrying out measures to ensure information security in the information and communication infrastructure.

The Company has organized the activities of the Information Security Operations Center (SOC) of QazCloud LLP, the activities of which are licensed in accordance with the requirements of the legislation of the Republic of Kazakhstan.
Monitoring of information security events is implemented using a SIEM system, to which all main sources are connected (servers, equipment, information security and monitoring tools, user computers, etc.).

If an employee fails to comply with information security requirements, disciplinary liability is applied to him. For example, in the event of intentional or careless disclosure of information constituting a trade secret of the employer and its counterparties, the employee bears disciplinary liability in the manner established by the Labor Code of the Republic of Kazakhstan.