«Қазақстан темір жолы»
ұлттық компаниясы» акционерлік қоғамы

Акционерное общество
«Национальная компания «Қазақстан темір жолы»

Joint-Stock company «National Company
«Kazakhstan Temir Zholy»

Approved
by the decision of the Management
Board of the joint-stock company
"National Company
"Kazakhstan Temir Zholy"
dated July 18, 2019 No. 02/22
question No. 5

Information Security Policy of the Joint-Stock company "National Company "Kazakhstan Temir Zholy"

Version 4.0

Group of documents:	Basic documentation
Developer:	Department of corporate security
Responsible for the analysis and updating of the document:	Department of corporate security

Nur-Sultan
2019

Table of contents

1 General provisions

1. This Information Security Policy of the Joint Stock Company "National Company "Kazakhstan Temir Zholy" (hereinafter the Policy) has been developed in accordance with the requirements of the international standard ISO 27001:2013 "Information technologies - Security methods – Information security management Systems - Requirements".

2. The Policy is an internal document of the joint stock company "National Company "Kazakhstan Temir Zholy" (hereinafter JSC "NC "KTZ").

3. This Policy applies to the group of companies of JSC "NC "KTZ" (Joint Stock Company "National Company "Kazakhstan Temir Zholy") and its subsidiaries, one hundred percent of the voting shares (participation interests) of which are directly owned by JSC "NC "KTZ" on the right of ownership or trust management.

4. The management of JSC "NC "KTZ" is aware of the importance and manages information security, providing the necessary conditions for the development, improvement of measures and means of protecting information assets in the context of threats to information security, the development of legislation and regulations governing the activities of JSC "NC "KTZ".

5. JSC "NC "KTZ" is the largest transport and logistics holding of state significance, which is part of the assets of the Joint Stock Company "Samruk-Kazyna" Welfare Fund". The implementation of these activities is related to the management of information, including information transmitted by the state, which is an important asset of JSC "NC "KTZ", and depends on ensuring information security, which means ensuring confidentiality, integrity, and availability of assets.

6. JSC "NC "KTZ" pays special attention to information security issues, constantly improves the information security management system (hereinafter – the ISMS), the means and methods used to protect against threats to information security, and provides continuous training of the Company's employees to maintain competence in the field of information security at a high level.

7. The ISMS is part of the management system of JSC "NC "KTZ". The Policy provisions consider the expectations of all interested parties and are mandatory for all employees of JSC "NC "KTZ" and its subsidiaries in the process of forming a portfolio of investment projects, as well as are brought to the attention of customers and other third parties with access to information systems and documents of JSC "NC "KTZ", in the part that is directly interrelated with JSC "NC "KTZ" and its activities.

8. The Policy provides for the main objectives, principles, and requirements for the protection of information.

9. The Policy has been developed in accordance with the legislation of the Republic of Kazakhstan on the use of information systems and information security, as well as the requirements of international information security management standards.

10. The Policy covers all information systems and documents owned and used by JSC "NC "KTZ" its subsidiaries. Ensuring information security is a prerequisite for the implementation of the activities of JSC "NC "KTZ".

2 Goals, requirements, and basic principles

11. The main purpose of the Policy is to minimize damage from events that pose a threat to information security by preventing them or minimizing their consequences.

12. The ISMS is based on a risk-based approach aimed at reducing the likelihood of information security events.

13. Ensuring information security is necessary to reduce the risks and economic losses associated with various threats to the existing information resources of JSC "NC "KTZ" and its subsidiaries. To this end, it is necessary to maintain the main properties of information, namely:

1) availability is a property characterized by the ability of timely unhindered access to information of subjects who have the appropriate authority to do so;

2) confidentiality is a property indicating that only a limited circle of persons determined by its owners can have access to information.

3) integrity is a property of information that consists in its preservation in an undistorted form (unchanged in relation to some fixed state of it).

14. To ensure a sufficiently reliable information security system, it is necessary to constantly reassess its parameters, adapt to reflect new dangers emanating from the external and internal environment. There should be no obstacles to making changes to standards, procedures or Policies as the need arises. In this regard, the following stages of the information security management cycle are determined:

1) planning (development) – analysis of risks, goals, tasks, processes, procedures, software, and hardware related to risk management and information security improvement to obtain results in accordance with the Development Strategy of JSC "NC "KTZ".

2) implementation (implementation and operation) – introduction of control mechanisms, processes, procedures, software and hardware;

3) verification (monitoring and analysis) – assessment and, where necessary, measurement of the performance characteristics of processes in accordance with Policies, goals and practical experience, analysis of changes in external and internal factors affecting the security of information resources, reporting to management for analysis;

4) correction (maintenance and improvement) is the adoption of corrective and preventive measures based on the results of internal and external checks of the state of information security, requirements from the management of other factors, to ensure continuous improvement of the information security system.

15. The construction of the information security system of JSC "NC "KTZ" and its subsidiaries, as well as its functioning, should be carried out in accordance with the following principles:

1) legality – any actions taken to ensure information security are carried out within the framework of the legislation of the Republic of Kazakhstan, using all methods of detection, prevention, localization and suppression of negative impacts on the objects of information protection of JSC "NC "KTZ" and its subsidiaries;

2) focus on business information security is considered as a process of supporting the main activity. Any measures to ensure information security should not entail serious obstacles to the activities of JSC "NC "KTZ" and its subsidiaries;

3) continuity – the use of information security management systems, the implementation of any measures to ensure the information security of JSC "NC "KTZ" and its subsidiaries should be carried out without interrupting or stopping the current business processes of JSC "NC "KTZ" and its subsidiaries;

4) complexity – ensuring the security of information resources throughout their life cycle, at all technological stages of their use and in all modes of operation;

5) validity and economic feasibility – the capabilities and means of protection used must be implemented at the appropriate level of development of science and technology, justified from the point of view of a given level of safety and must comply with the requirements and standards. In all cases, the cost of information security measures and systems should be less than the amount of possible damage from any type of risk.

6) priority – categorization (ranking) of all information resources of JSC "NC "KTZ" and its subsidiaries to the degree of importance in assessing real as well as potential threats to information security;

7) the necessary knowledge and the lowest level of privileges – the user receives the minimum level of privileges and access only to those data that are necessary for him to perform activities within his authority;

8) specialization – the operation of technical means and the implementation of information security measures should be carried out by professionally trained specialists;

9) awareness and personal responsibility – managers at all levels and employees should be aware of all information security requirements and are responsible for meeting these requirements and compliance with established information security measures;

10) interaction and coordination – information security measures are carried out on the basis of the interconnection of the relevant structural divisions of JSC "NC "KTZ" and its subsidiaries, coordination of their efforts to achieve their goals, as well as establishing the necessary links with external organizations, professional associations and communities, government agencies, legal entities and individuals;

11) confirmability – documents confirming the fulfillment of information security requirements and the effectiveness of its organization's system should be created and stored with the possibility of prompt access and recovery.

3 Objects of protection

16. The main objects of information security protection in JSC "NC "KTZ" and and its subsidiaries are the following elements:

1) information resources containing information classified in accordance with the current legislation and local acts of JSC "NC "KTZ" and its subsidiaries as a commercial, official or other legally protected secret, including information resources included in the projects of the Digital Railway program and the transformation program in JSC "NC "KTZ" (hereinafter – protected information);

2) means and systems of informatization (computer equipment, information and computing complexes, networks, systems), on which the protected information is processed, transmitted and stored;

3) software tools (operating systems, database management systems, other system-wide and application software) of automated systems of JSC "NC "KTZ" and its subsidiaries, with the help of which the protected information is processed;

4) processes of JSC "NC "KTZ" and its subsidiaries related to the management and use of information resources;

5) premises where the protected information processing facilities are located;

6) working rooms and offices of employees of JSC "NC "KTZ" and its subsidiaries, premises of JSC "NC "KTZ" and its subsidiaries, intended for conducting closed negotiations and meetings;

7) employees of JSC "NC "KTZ" and its subsidiaries who have access to protected information;

8) technical means and systems that process open information, but are located in the premises in which the protected information is processed;

9) virtual environments (computing resources or their logical integration, abstraction from hardware implementation, providing logical isolation from each other of computing processes running on the same physical resource) when using the server infrastructure.

17. Protected information can:

1) be placed on paper;

2) exist in electronic form (processed, transmitted and stored by computer technology, recorded and reproduced using technical means);

3) transmitted by telephone, fax, telex, etc. in the form of electrical signals;

4) be present in the form of acoustic and vibration signals in the air and enclosing structures during meetings and negotiations.

4 Threats to information security

18. Threats to information security are understood as potentially possible events, processes, or phenomena that, by affecting information or components of an information system or resource, can directly or indirectly lead to damage to the interests of owners and users.

19. Threats to information security are divided into:

1) random, which may be caused by the following factors:

natural disasters;

mistakes due to inattention;

hardware and software errors;

low awareness of employees in the field of information security;

insufficient physical provision of the information security perimeter;

2) intentional, which may be caused by the following factors:

falsification or destruction of data;

misuse of data;

unauthorized access to information;

computer attacks (a purposeful attempt to implement the threat of unauthorized influence on information, electronic resource, information system or gaining access to them using software or hardware and software, or protocols of inter-network interaction);

20. Threats to the information security of JSC "NC "KTZ" and its subsidiaries include (but are not limited to):

1) loss of protected information;

2) distortion (unauthorized modification, forgery) of protected information;

3) leakage, unauthorized familiarization with the protected information of unauthorized persons (unauthorized access, copying, theft, etc.);

4) unauthorized use of information resources (abuse, fraud, etc.);

5) unavailability of information because of its blocking, failure of equipment, database management systems, distributed computing networks, exposure to viruses, natural disasters and other force majeure circumstances, and malicious actions.

21. As a result of the impact of these threats, the following negative consequences may arise, affecting the state of information security of JSC "NC "KTZ" and its normal functioning:

1) traffic safety emergencies;

2) financial losses related to leakage or disclosure of protected information;

3) financial losses associated with the destruction and subsequent recovery of lost information;

4) damage from the disorganization of the activities of JSC "NC "KTZ" and its subsidiaries losses associated with the inability to fulfill its obligations;

5) damage from making managerial decisions based on biased information;

6) damage caused by the absence of the management of JSC "NC "KTZ" and its subsidiaries objective information;

7) damage caused to the reputation of JSC "NC "KTZ" and its subsidiaries;

8) other type of damage.

5 Information security measures

22. The main measures to ensure the information security of JSC "NC "KTZ" and its subsidiaries:

1) administrative, legal and organizational measures;

2) physical security measures;

3) software and technical measures.

23. Administrative, legal, and organizational measures include (but are not limited to):

1) control of compliance with the requirements of the legislation of the Republic of Kazakhstan and internal documents of JSC "NC "KTZ" and its subsidiaries;

2) development, implementation and control of the implementation of rules, methods and instructions supporting the Policy;

3) control of compliance of business processes of JSC "NC "KTZ" and its subsidiaries the requirements of the Policy;

4) informing and training employees of JSC "NC "KTZ" and its subsidiaries work with information systems and information security requirements;

5) responding to channels of unauthorized information leakage, incidents related to it, localization and minimization of consequences;

6) analysis of new information security risks;

7) monitoring and improving the moral and business climate in the team;

8) definition of actions in case of emergency situations;

9) carrying out preventive measures when hiring and firing employees of JSC "NC "KTZ";

10) measures to control the legality of the use of software.

24. Physical security measures include (but are not limited to):

1) organization of access and intra-facility modes;

2) building a security perimeter of protected objects;

3) organization of round-the-clock security of protected objects, including with the use of technical security means;

4) organization of fire safety of protected objects;

5) control of access of employees of JSC "NC "KTZ" and its subsidiaries the security rooms and restricted access rooms.

25. Software and technical measures include (but are not limited to):

1) use of licensed software and certified information security tools;

2) the use of perimeter protection (firewall, IPS, etc.);

3) application of comprehensive anti-virus protection;

4) the use of information security tools embedded in information systems;

5) ensuring regular backup of information;

6) control over the rights and actions of users, primarily privileged;

7) the use of cryptographic protection of information in accordance with the procedure established by regulatory legal acts;

8) ensuring trouble-free operation of hardware;

9) monitoring the status of critical elements of the information system.

6 Responsibility and compliance with legal requirements

26. Appropriate processes have been implemented in JSC "NC "KTZ" and its subsidiaries to ensure compliance with the requirements of regulatory legal acts, compliance with intellectual property rights, protection of legally protected personal information, compliance with restrictions on the use of cryptographic means.

27. All requirements and provisions of the international standard ISO/IEC 27001 are mandatory in the field of their application, determined by the relevant documents.

28. When developing and applying information security tools and methods, the requirements of contractual obligations and contracts concluded by JSC "NC "KTZ" and its subsidiaries with third parties are considered.

29. Access by a third party to the information resources of JSC "NC "KTZ" and its subsidiaries is carried out only after analyzing the risks that may arise when providing such access and taking adequate protective measures. If necessary (in particular, if there are requirements of regulatory legal acts or international standards), JSC "NC "KTZ" and its subsidiaries checks contractors (suppliers of goods and services) for compliance with certain requirements.

30. Based on the Policy, local acts are developed regulating the procedure and methods for ensuring information security, standards, etc.

31. Responsibility for compliance with this Policy is assigned to employees of JSC "NC "KTZ" and its subsidiaries.

7 Policy review

32. The Policy is reviewed as necessary, but at least once every 24 months.