**Annex**
**to the Order of Kazakhtelecom JSC dated**
**June 19, 2023 No. 153**

# Information Security Policy of Kazakhtelecom JSC

Almaty, 2023

**Table of contents**

## 1 General regulations

1. The Information Security Policy (hereinafter - the Policy) is a set of preventive measures to protect information, including information with limited dissemination (official information), information processes and includes requirements for users of information systems of Kazakhtelecom JSC (hereinafter - the Company), its branches and structural divisions in their activities.

2. The Policy was developed in order to define strategic purposes, objectives and basic requirements for a set of measures in the field of information security (hereinafter - information security), as one of the critical factors of successful and stable operation of Kazakhtelecom JSC (hereinafter - the Company), ensuring the stability of information systems (hereinafter - IS) and information security, ensuring comprehensive protecting the interests of the Company, its employees, as well as third parties, contractors from threats in the field of information technology.

3. The Policy is a fundamental document reflecting the vision and intentions of the Company's management in the field of information security, sets purposes, objectives and principles in the field of information security, which guide the Company in its activities. Serves as a guide in the development of relevant documents of the information security management system (hereinafter – ISMS);

4. The regulatory and legal basis of the Policy is the requirements of the provisions of the legislation of the Republic of Kazakhstan (hereinafter – RK) on the use of IP and IS, as well as the requirements of international information security management standards (ISO/IEC 27000, ITIL).

5. By IS within the framework of this document, the Company understands the state of protection of its interests (purposes) from threats in the field of information technology (hereinafter - IT). Security is achieved by providing a set of properties of information assets: confidentiality, integrity and accessibility.

6. The Company's IS is provided within the framework of the cyclic IS model: "planning — implementation — verification — improvement", which corresponds to the principles and model of corporate management in the Company.

7. The Policy is a publicly available document that can be provided without restrictions to all interested parties.

## 2 Main purposes and objectives

8. The policy is aimed at achieving the main objectives:

1) ensuring the availability of the Company's information assets to support its business processes;

2) protection of the integrity of the Company's information assets in order to support the high quality of business processes;

3) maintaining the confidentiality of information of the Company and other parties;

4) ensuring the continuity of the main business processes operating in the Company;

5) compliance of the information security measures applied in the Company with the requirements of legislation, as well as the requirements of regulatory and supervisory authorities.

9. The main tasks for the implementation of the Policy are planning, implementing and monitoring the implementation of a set of organizational and technical measures to ensure IS based on an assessment of the Company's risks in the IT field, aimed at:

1) protection of information from real and potential modern cyber threats;

2) prevention, detection and deactivation of various modern cyber threats;

3) establishing the causes and conditions of cyber threats;

4) rapid response to the impact of modern threats and their precise localization;

5) minimizing damage from events that pose a threat to the security of information by preventing them or minimizing their consequences;

6) application of modern international methodologies and practices to improve the mechanisms of rapid response and investigation of cyber threats;

7) effective IS risk management;

8) ensuring employees' awareness of the Policy, measures taken, requirements for ensuring IS, duties and rules of conduct imposed on employees, as well as ensuring control over their proper implementation;

9) increasing the level of knowledge and development of corporate culture in the field of IS;

10) improvement of the ISMS;

11) ensuring compliance with the requirements of the legislation of the Republic of Kazakhstan in the course of the Company's IS activities.

12) conducting the practice of disciplinary punishment in case of violation of the Information Security Policy.

10. In order to achieve these goals and solve the listed tasks, the Company is building an ISMS that meets the requirements:

1) legislation of the Republic of Kazakhstan and standards in the field of information security;

2) ISO/IEC international standards in the field of IS;

3) regulatory documents of the regulator;

4) corporate regulatory documents, contractual obligations and other regulatory documents in the field of IS.

The ISMS, being part of the general management system of the Company, is documented in this Policy, as well as other ISMS documents (IS concept, private policies, regulations, guidelines, standards, instructions, regulations, procedures, etc.), detailing, developing the provisions set out in this Policy at the level of their practical implementation and are mandatory for all employees of the Company, as well as representatives of third parties who have access to the Company's information resources.

## 3 Basic principles of information security

11. The Policy is based on the following basic principles:

1) legality of IS provision;

2) involvement of the Company's top management in the process of ensuring IS;

3) business orientation;

4) process approach;
5) comprehensive use of methods, methods and means of protection;
6) following best practices;
7) reasonable sufficiency;
8) awareness and personal responsibility.

## 4 Responsibility and intentions of management

12. Ensuring the Company's IS is achieved by implementing a set of necessary processes and measures supported by each SD and the Company's employee to the extent necessary and determined for him in accordance with the provisions of internal documents on ensuring the Company's IS.
13. The Company's management strives to ensure the efficient and stable operation of the Company, as well as to maintain the confidence of all interested parties in the reliability and stability of the Company's work, in the protection of their interests from the impact of various adverse factors.
14. The Company's management includes:
1) Chairman and members of the Board of Directors;
2) Members of the Management Board;
3) Chief and Managing Directors;
4) General Directors of Divisions - branches and structural divisions (hereinafter – SD);
5) Managers of the SD.

15. The management of the Company assumes responsibility for the implementation of this Policy.

16. Management strives to organize IS activities in accordance with the legislation of the Republic of Kazakhstan, standards such as ST RK ISO/IEC 27001, NSD of the Company and best practices.

17. The Company's management strives to achieve this goal by creating, supporting, controlling and developing an effective ISMS based on a balanced set of organizational and technical measures to ensure IS.

18. Heads of functional units, SD, employees of the Company are responsible for fulfilling their duties to ensure the maintenance of activities and compliance with the requirements of the IS in accordance with the documents of the ISMS.

19. The responsibility of Representatives of third parties who have access to the information resources of the Company shall be provided for in the contractual obligations of the parties.

## 5 Final regulations

20. The provisions of this Policy are subject to revision based on the results of an external audit, internal analysis and assessment of IS risks for the Company's information system, as a result of any changes in the Company's activities, changes in the legislation of the Republic of Kazakhstan and as necessary.

21. If, as a result of changes in the legislation of the Republic of Kazakhstan, the norms of this Policy come into conflict with the current legislation, these norms of the Policy become invalid and until changes, additions to this Policy are made, it is necessary to be guided by the current legislation of the Republic of Kazakhstan.

22. Issues not provided for in the provisions of the Policy are resolved in accordance with the legislation of the Republic of Kazakhstan, internal documents and decisions of the Management Board of the Company (at the same time, the legislation of the Republic of Kazakhstan has prevailing force).

23. Non-compliance with the procedure and rules for the use of information resources and IS measures taken in the Company entails liability in accordance with the current legislation of the Republic of Kazakhstan and internal regulatory documents of the Company.

24. The content of this Policy shall be brought to the attention of the Company's employees in accordance with the procedure established by the Company's regulatory documents and procedures.

25. This IS Policy comes into force from the moment of its approval by the Chairman of the Management Board of the Company and is valid until the adoption of a new IS Policy.

26. The head of the SD IS is responsible for making changes to the Policy.

27. Control over bringing the requirements of the points of this Policy to the heads of the SD of the Company is assigned to the head of the SD IS. Control over the familiarization of the Company's employees with these documents lies with the heads of branches and the heads of the SD of the Company.

28. This Policy is posted on the official website of the Company.