Appendix to the Order of
Kazakhtelecom JSC
No.___
dated "__" _____ 2025

Information Security Policy of Kazakhtelecom JSC

Almaty, 2025

Content

Chapter 1. General provisions

1. Information Security Policy (hereinafter – the Policy) is a complex of preventive measures for the protection of information, including information with restricted distribution (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 has been developed with the aim of defining strategic goals, objectives and basic requirements for a set of measures in the field of information security (hereinafter – the IS) as one of the critical factors for the successful and stable operation of the Company, ensuring the sustainability of information systems (hereinafter – the ISys) and the preservation of information, ensuring comprehensive protection of the interests of the Company, its employees, as well as third parties and contractors from threats in the field of information technology.

3. The Policy is a fundamental document that reflects the vision and intentions of the Company's management in the field of IS, establishes goals, objectives and principles in the field of IS, which guide the Company in its activities. It serves as a guide for the development of relevant documents of the information security management system (hereinafter – the ISMS).

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

5. IS in this document, the Company understands information security to mean the state of protection of its interests (goals) from threats in the field of information technology (hereinafter – IT). Security is achieved by ensuring a set of properties of information assets: confidentiality, integrity and availability.

6. The Company's information security is ensured within the framework of a cyclical IS management model: “planning — implementation — verification — improvement”, which complies with the principles and model of corporate management in the Company.

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

Chapter 2. Main goals and objectives

8. The policy aims to achieve the following main objectives:

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

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

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

4) ensuring the continuity of the Company's core business processes;

5) ensuring that the information security measures implemented by the Company comply with the requirements of legislation and the requirements of regulatory and supervisory authorities.

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

1) protecting information from real and potential modern cyber threats;

2) preventing, detecting and deactivating various modern cyber threats;

3) establishing the causes and conditions of cyber threats;

4) responding quickly to the impact of modern threats and accurately localising them;

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

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

7) effective management of IS risks;

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

9) raising the level of knowledge and developing a corporate culture in the field of information security;

10) improving the ISMS;

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

12) maintaining a practice of disciplinary action in case of violation of the Policy.

10. To achieve these goals and solve these tasks, the Company is building an ISMS that meets the requirements of:

1) Kazakhstan legislation and standards in the field of IS;

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

3) regulatory documents of the regulator;

4) the Company's regulatory and regulatory documents, contractual obligations and other regulatory documents in the field of IS.

The ISMS, being part of the Company's overall management system, is documented in this Policy, as well as in other ISMS documents (specific rules, requirements, regulations, guidelines, standards, instructions, provisions, procedures, etc.), which detail and develop the provisions set forth in this Policy at the level of their practical implementation and are binding on all Company employees, as well as third-party representatives who have access to the Company's information resources.

Chapter 3. Basic principles of information security

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

1) legality of IS;

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

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

Chapter 4. Responsibility and intentions of management

12. The Company's IS is achieved through the implementation of a set of necessary processes and measures supported by each SD and employee of the Company to the extent necessary and specified for them in accordance with the rules and requirements of internal documents on ensuring the Company's IS.

13. The Company's management strives to ensure the effective 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 operations and in the protection of their interests from various adverse factors.

14. The Company's management includes:

1) The Chairman of the Management Board and members of the Board of Directors;

2) The First Deputy Chairman of the Management Board, members of the Management Board;

3) Chief and Managing Directors;

4) General Directors of Divisions – branches and structural units (hereinafter – the SU);

5) SU managers.

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

16. The management strives to organise activities to ensure IS in accordance with the legislation of the Republic of Kazakhstan, standards such as ST RK ISO/IEC 27001, the Company's NRD 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 information security.

18. The heads of functional units, SU, and Company employees are responsible for fulfilling their duties to maintain operations and comply with information security requirements in accordance with ISMS documents.

19. The responsibility of third-party representatives who have access to the Company's information resources must be stipulated in the contractual obligations of the parties.

Chapter 5. Final provisions

20. The provisions of this Policy are subject to review as necessary, based on the results of external audits, internal analysis and assessment of information security risks for the

Company's IS, as a result of any changes in the Company's activities, changes in the legislation of the Republic of Kazakhstan, but at least once every two years.

21. If, as a result of changes in the legislation of the Republic of Kazakhstan, the provisions of this Policy come into conflict with the current legislation, these provisions of the Policy shall cease to be valid and, until amendments or additions are made to this Policy, the current legislation of the Republic of Kazakhstan shall be followed.

22. Issues not covered by the provisions of the Policy shall be resolved in accordance with the legislation of the Republic of Kazakhstan, internal documents and decisions of the Company's Management Board (with the legislation of the Republic of Kazakhstan taking precedence).

23. Failure to comply with the procedure and rules for using information resources and the IS measures adopted by the Company shall entail liability in accordance with the current legislation of the Republic of Kazakhstan and the internal regulatory documents of the Company.

24. The content of this Policy shall be brought to the attention of the Company's employees in the manner specified by the Company's regulatory documents and procedures.

25. This IS Policy shall come into force upon its approval by the Chairman of the Company's Management Board and shall remain in force until a new IS Policy is adopted.

26. The Managing Director for Information Security shall be responsible for making changes to the Policy.

27. The Managing Director for Information Security is responsible for ensuring that the requirements of this Policy are communicated to the managers of the Company's SU. The managers of the Company's branches and SU are responsible for ensuring that the Company's employees are familiar with this document.

28. This Policy is posted on the Company's official website.