

**Annex**  
**to the Decision of the Board of Directors**  
**Kazakhtelecom JSC**  
**Dated 04 November 2022, Minutes # 12\_\_\_\_\_**

**REGULATION**  
**on Commercial Secret of Kazakhtelecom JSC**

**1. General provision**

1. The purpose of this Regulation on Commercial Secret for Kazakhtelecom JSC (hereinafter referred to as the "Regulation") is to develop and establish a unified system within Kazakhtelecom JSC (hereinafter referred to as the "Company") to protect Commercial Secrets. This system aims to safeguard economic interests and prevent potential economic damage caused by the unlawful or negligent actions of legal entities or individuals, such as unauthorized disclosure or misuse of confidential information.

2. This Regulation are developed in accordance with the Civil Code of the Republic of Kazakhstan, the Entrepreneurial Code of the Republic of Kazakhstan, the Law of the Republic of Kazakhstan "On Joint Stock Companies," other applicable regulatory acts of the Republic of Kazakhstan, the Charter of Kazakhtelecom JSC, and other internal Company documents. They are intended to protect the Company's interests concerning the classification, Commercial Secret, and handling of information deemed Commercial Secrets and to identify information that cannot be classified as a Commercial Secret.

3. This Regulation apply to information constituting a Commercial Secret, regardless of the medium on which it is recorded (e.g., paper, electronic, photographic, film, audio, or videotape).

4. The process for protecting confidential information within the Company's corporate information system, including electronic document flow, as well as the list of "Categories of Information Resources Subject to Protection" in electronic document flow, is governed by a separate document.

5. This Regulation do not apply to matters related to the protection of state secrets of the Republic of Kazakhstan.

**2. Key Terms Used in the Regulation**

6. **\*\*Access Restriction Label\*\*** – A document label or combination of identifiers applied in compliance with established requirements, indicating that the document contains confidential or official information and has restricted access to a limited group of users. In the Company, the label "Confidential" is used.

7. **\*\*Document\*\*** – Information recorded on a tangible medium with identifying details, created, received, and retained by the Company or an employee of the Company

for evidentiary or reference purposes in fulfilling legal obligations or performing Company activities.

8. **\*\*Access to Information (Documents) Constituting a Commercial Secret\*\*** – The ability to obtain and use information (documents) with the consent of its owner or on another lawful basis, while maintaining its Commercial Secret.

9. **\*\*Key Management Personnel\*\*** – Employees directly overseeing the Company's strategic activities, excluding executives, the Head and employees of the Internal Audit Service, and the Corporate Secretary. The list of key management personnel is defined by the Company's Board.

10. **\*\*Company Commercial Secret (Commercial Secret)\*\*** – Information not classified as a state secret, which is determined and protected by the Company. This includes scientific, technical, technological, production, financial-economic, or other data that has actual or potential commercial value due to its unknown status to third parties, with access restricted by law to certain individuals. Disclosure, unauthorized acquisition, or use could harm the Company's interests.

11. **\*\*Counterparty\*\*** – The party in a civil contract with whom the owner of Commercial Secret information has shared such information.

12. **\*\*Confidential Information\*\*** – Any type of information (including commercial, banking, tax, notarial, medical, personal, and legal secrets) to which access is restricted by the Company's internal documents, thereby imposing a binding obligation on those with access not to disclose this information to third parties without the owner's written consent.

13. **\*\*Owner of Information Constituting a Commercial Secret\*\*** – A person who legally possesses information and, under the laws of the Republic of Kazakhstan or contractual terms, has the right to permit or restrict access to the information designated as a Commercial Secret and legally establishes a Commercial Secret regime.

14. **\*\*Transfer of Information Constituting a Commercial Secret\*\*** – The transfer of information classified as a Commercial Secret by its owner, recorded on a tangible medium, in strictly defined cases and following established procedures:

1) to a counterparty under a civil contract within the scope and terms set by the contract, including measures for maintaining its commercial secret;

2) to state authorities or other bodies for performing their functions, with the owner's written consent. the company may decline to provide state bodies and officials performing registration, control, or oversight functions with access to commercial secret information unless it is essential for fulfilling their duties;

3) to legal and natural persons in cases of production or commercial necessity, with the owner's written consent and a commercial secret agreement;

4) to the media for publication purposes, with the owner's written consent;

5) to company employees as part of employment relations, requiring them to sign a non-disclosure commitment. the company, or an authorized representative, may require employees to sign a non-disclosure agreement for commercial secrets and notify inspectors of liability under the laws of the republic of kazakhstan.

15. **\*\*Commercial Secret Regime\*\*** – Legal, organizational, and technical measures to prevent unauthorized disclosure, access, destruction, alteration, copying, and other illegal actions regarding information containing Commercial Secrets, along with legal, organizational, and technical actions to safeguard the Commercial Secret of this information, conducted by its owner.

16. **\*\*Disclosure of Information Constituting a Commercial Secret\*\*** – Any act or omission resulting in the Commercial Secret information becoming known to third parties in any form (oral, written, electronic) without the owner’s consent or in violation of a civil contract. Information constituting a Commercial Secret may not be disclosed without the Company’s consent, except as mandated by a court ruling or other cases established by the laws of the Republic of Kazakhstan.

### **3. Right to Classify Information as Commercial Secrets and Methods of Obtaining Such Information**

6. The classification of information as a Commercial Secret, as well as the determination of the scope and content of such information, is conducted by the Company in accordance with the Company's Charter and the legislation of the Republic of Kazakhstan.

7. Information classified as a Commercial Secret, obtained from its holder based on a civil contract in compliance with this Regulation, is considered legally obtained. The relevant contract must include a clause informing the counterparty that specific information is protected as the Company’s Commercial Secret by law and obligates them to maintain Commercial Secret.

8. Information classified as a Commercial Secret and held by the Company may be disclosed or shared with legal entities and individuals for business or operational necessity, upon written approval by the Company’s Board Chairman. This approval is also signed by the relevant Managing Director or General Director of a branch, whose duties include oversight, control, and management of the disclosed information, and the corresponding Commercial Secret Agreement is executed.

9. Information classified as a Commercial Secret and held by the Company may be provided upon request by authorized state bodies or other interested parties in cases explicitly provided for by the laws of the Republic of Kazakhstan. The receiving party must be notified that the provided materials or documents are classified as the Company’s Commercial Secrets and are not to be disclosed. Receipt of this information on a physical medium must be confirmed with a signature on the original document or its copy, while the movement of electronic media containing confidential information (CD, DVD, flash drive, etc.) is tracked in accordance with this Regulation.

10. Information classified as a Commercial Secret and held by the Company is considered illegally obtained if:

1) company measures to protect the commercial secret of this information were intentionally violated in obtaining it;

2) the recipient was aware or had sufficient reason to believe that the information constituted a commercial secret of the company and that the provider had no legal basis for sharing it.

#### **4. Information Not Eligible for Commercial Secret Classification**

11. Commercial Secret status cannot be applied by the Company to information that:

1) is contained in the company's foundational documents, authorizing statutory activities;

2) pertains to environmental pollution, fire safety, sanitary-epidemiological or radiation conditions, food safety, or other factors negatively impacting the safe operation of production facilities;

3) concerns the number and identity of the company's employees, working conditions (excluding remuneration conditions), production injury rates, and occupational illness indicators, as well as the availability of job openings;

4) relates to the company's outstanding salary and social payment obligations;

5) involves violations of the laws of the republic of kazakhstan and any instances of employee accountability for such violations;

6) is required to be disclosed or must be freely accessible by the laws of the republic of kazakhstan.

#### **5. Company Rights Concerning Commercial Secret Information**

12. The Company's rights take effect once a Commercial Secret regime (Commercial Secret designation) is applied to the information.

13. The Company has the right to:

1) establish, modify, or cancel the commercial secret regime in writing as per this regulation;

2) use commercial secret information for appropriate purposes in a manner consistent with the law;

3) permit or deny access to commercial secret information and set access terms and conditions;

4) require legal entities, individuals, and state bodies with access to commercial secret information to respect its Commercial Secret;

5) legally defend its rights in cases of disclosure, unlawful acquisition, or illegal use of commercial secret information, including claims for damages caused by such actions.

## **6. Holder of Commercial Secret Information Obtained Within Employment Relationships**

14. The Company is the holder of Commercial Secret information acquired by its employees in the course of their employment. The Company's foundational documents define who has free access to this information in accordance with the laws of the Republic of Kazakhstan.

15. If an employee produces a legally protectable result, such as an invention, utility model, industrial design, computer program, or database, while performing their work duties or a specific assignment, the relationship between the employee and the Company will be governed by intellectual property laws.

## **7. Protection of Commercial Secrets and Measures to Safeguard Confidential Information**

16. Commercial Secret protection includes prohibiting the unlawful acquisition, distribution, or use of Commercial Secret information in accordance with the laws of the Republic of Kazakhstan.

17. The Company's Commercial Secret protection measures include:

- 1) Defining documents, materials, and information of Kazakhtelecom JSC containing Commercial Secrets;
- 2) Restricting access to Commercial Secret information through procedures for its management and monitoring compliance;
- 3) Recording the identities of individuals granted access to Commercial Secrets and to whom it was disclosed or transferred;
- 4) Managing the use of Commercial Secret information by employees based on employment agreements;
- 5) Labeling physical media (documents) containing Commercial Secret information with the "Confidential" ("C") mark, indicating the copy number.

18. The employee who created a document, the head of the central office division, and branch heads who sign the document are responsible for correctly assigning Commercial Secret marks.

19. Documents containing Commercial Secret information are labeled with the "Confidential" ("C") mark when disclosure could harm the Company's interests. Access to these documents is restricted to employees with job duties involving the document's execution, as authorized by their department head.

20. Commercial Secret status is considered established after implementing the measures outlined in subpoints 1–5 of point 28 of this Regulation.

21. Alongside the measures specified in subpoints 1) – 5) of point 28 of this Regulation, the Company has the right, if necessary, to apply technical means and methods for protecting confidential information, as well as other measures consistent with the law.

22. Commercial Secret protection measures are considered reasonably sufficient if:

- 1) Access to information classified as a Commercial Secret is restricted to any individuals only with the Company's consent;
- 2) The use of information classified as a Commercial Secret by employees and its transfer to counterparties is ensured without violating the Commercial Secret regime.

## **8. Reception, Transmission, Registration of Documents Containing Confidential Information**

23. The reception and registration of incoming/outgoing documents marked "C" in paper form are conducted in a special log by the office of the organizational control unit of the Central Office (hereinafter referred to as the CO Office) and by the structural unit of the Company's branch responsible for managing office records (Documentation Expertise Center).

24. In the structural unit of the CO/branch, the tracking of reproduction, destruction, and movement of internal documents marked "C" in paper form is conducted in a special tracking log. The tracking of electronic confidential information carriers (e.g., CDs, DVDs, flash drives) is recorded in a separate log for electronic carriers. Storage of logs for tracking both paper and electronic confidential information carriers, files with confidential documents, and electronic carriers is carried out in a locked safe/cabinet with the responsible structural unit/branch manager or designated staff member.

25. If it is necessary to reproduce or replicate documents marked "C" in paper form, a note is made in the tracking log about the number of reproduced copies, and each recipient is specified.

26. Internal documents marked "C" in paper form are stored in a separate file in the CO/branch, where a list of attached documents is maintained. The file is stored in a safe or locked cabinet with the relevant structural unit manager or designated staff member.

27. Files and logs for tracking confidential information carriers are included in the CO/branch's classification list and subsequently added to the general file classification.

28. The dispatch of paper documents marked "C" to recipients outside the Company is carried out through the Republican Special Communication Service.

29. In cases of transferring documents with the aforementioned markings from one structural unit of the CO to another, an entry is made in the unit's tracking log, and the document is transferred under a receipt indicating the name of the unit, position, and full names of the persons handing over and receiving the document.

30. At least once a year (end of the year), a check is conducted on the availability and storage conditions of documents marked "C" in paper form. For this purpose, a relevant commission is established by order of the Chairman of the Company's Management Board, specifying the commission's powers, composition, and member count. Based on the results of the inspection, an Inspection Report is drawn up, noting any remarks about storage conditions. The report is signed by all members of the commission and sent to the Chairman of the Company's Management Board for review and necessary actions.

31. If necessary, no more than once a year, outdated or irrelevant documents marked "C" are destroyed by order of the Chairman of the Management Board/General Director of the branch, based on the relevant order. A commission is established, specifying its

powers, composition, and number of members. The CO/branch structural unit manager, who oversees the staff responsible for storing "C"-marked documents, sends a corresponding memo to the Chairman of the Management Board/General Director of the branch indicating the need for document destruction. The commission comprises at least three people, including the employee responsible for "C"-marked document storage, a Security and Civil Defense Service employee, and the unit manager or a designated substitute. The commission is led by the Security and Civil Defense Service employee. An Act of Destruction is drawn up, listing the date, registration number, title of the document to be destroyed, and the reason for destruction. The Act is signed by all commission members.

32. It is strictly prohibited to receive or transmit documents containing Commercial Secrets via email, Internet messengers, or social networks.

33. When it is necessary to create documents containing Commercial Secrets in SED 2.0 (Electronic Document Management System), the following options should be considered:

1) option 1: the "lock" option (shown by a "lock" icon) can be used by any lotus notes application user when creating a document in the subdivision's brd. the "document actions - additional - readers" option allows employees to select, add, or delete readers at their discretion. the document is visible to the document's author and to employees included in the "readers" section;

2) option 2: if a draft document is placed in the "familiarization" db, the document is visible to the author, the direct supervisor of the unit, employees included in the approval list, and a limited group of people authorized to view the db content.

## **9. List of the Company's Documents Constituting Commercial Secrets**

34. Commercial Secrets of the Company are defined as information specified in the attached List to this Regulation (Appendix 1).

35. The procedure for handling information specified in the List and the responsibility for following this procedure is established by this Regulation.

## **10. Rights and Obligations of the Company and Employees for Maintaining Commercial Secret Commercial Secret**

36. To safeguard Commercial Secrets, the Company is obligated to:

1) provide the employee whose access to commercial secret information is necessary for performing job duties with a signed acknowledgment of the list of information that constitutes commercial secrets owned by the company and its counterparties;

2) provide the employee with a signed acknowledgment of the company's commercial secret regime and the liability measures for its violation;

3) create necessary conditions for the employee to comply with the established commercial secret regime;

4) grant the employee access to commercial secret information with the employee's consent, unless specified as part of the employee's job duties.

37. To ensure the protection of Commercial Secret information, the employee is obligated to:

1) comply with the company's commercial secret regime, not disclose commercial secret information owned by the company and its counterparties, and not use such information for personal purposes without their consent;

2) avoid disclosing confidential information owned by the company after the termination of the employment contract, for the period established in the commercial secret obligation;

3) return any material carriers containing commercial secrets to the company upon termination of the employment contract.

38. The Company reserves the right, in accordance with the laws of the Republic of Kazakhstan, to claim damages from the employee for losses caused by disclosing Commercial Secret information accessed during job duties. This right extends to former employees if the disclosure occurred within the period established by this Regulation. Additionally, anyone who illegally obtains, discloses, or uses Commercial Secret information is required to compensate the Company for any damages in accordance with the civil legislation of the Republic of Kazakhstan.

39. Damages or losses are not compensated by the employee or former employee if the disclosure of Commercial Secret information was due to force majeure, extreme necessity, or the Company's failure to enforce the Commercial Secret regime.

40. Employees who, by virtue of their official duties, gain access to Commercial Secret information are required to sign a non-disclosure agreement upon hiring and when transferring between Company units, as per Appendix 2 to this Regulation.

41. To restrict access to Commercial Secret information, unit managers are required to coordinate with the network administrator (ASU) on the procedure for accessing the unit's network resources.

## **11. Liability for Violation of the Regulation**

42. Responsibility for maintaining the Commercial Secret regime lies with the heads of structural units/branches, as well as employees who are granted access to any Commercial Secret information.

43. Responsibility for maintaining Commercial Secret for information stored on the Company's server, and for protecting against unauthorized or remote access to restricted information resources, including those held by Company employees, lies with the Head of the Information Technology Division.

44. Control over compliance with and enforcement of the requirements of this Regulation within the Company is assigned to the Head of the Security Service.

45. Disclosure by an employee of information constituting a Commercial Secret, which became known to them in connection with their job duties, may serve as grounds for termination of the employment contract.

46. A person who used Commercial Secret information without sufficient grounds to believe that such use was illegal, including access resulting from an accidental error, cannot be held liable under the laws of the Republic of Kazakhstan. The Security Service must analyze each case individually, taking into account the corporate responsibility of



the person involved and their immediate supervisor, to determine whether a violation occurred intentionally or unintentionally.

**Appendix 1  
to the Commercial  
Commercial Secret  
Regulation  
of JSC "Kazakhtelecom"**

**LIST  
of Documents, Materials, and Information Containing Commercial Secrets of  
JSC "Kazakhtelecom"**

1. This List has been developed in accordance with the Commercial Secret Regulation of JSC "Kazakhtelecom" and represents a collection of categories of documents, data, and information constituting Commercial Secrets, for which an appropriate security regime is established.

**1. Production**

2. Traffic data (billing system - volume and duration data) from Kazakhstan's switching stations.

3. Technical, organizational, and financial data on commercial network deployments.

4. Full database of JSC "Kazakhtelecom" subscribers.

5. Information on the bitmap of payphones with smart card technology.

6. Details on primary network load and switching stations.

7. List of transmission lines and network paths on primary and intra-zone networks (without geographic linkage or specifying power information).

8. The list of transmission lines and network paths of JSC "Kazakhtelecom" for primary trunk networks (PTN) and intrazonal primary networks (IPN), (without geographic reference and without specifying their capacities, as well as without identifying the consumers of trunk communication lines leased by the Government, Ministry of Defense, National Security Committee, and Ministry of Internal Affairs of the Republic of Kazakhstan).

9. Information on the load of transmission systems (TS) for cable, fiber-optic, and microwave radio relay lines (MRL), (without geographic reference and without specifying their capacities, as well as without identifying the consumers of trunk communication lines leased by the Government, Ministry of Defense, National Security Committee, and Ministry of Internal Affairs of the Republic of Kazakhstan).

10. Scheme of the organization of paths and channels (without geographic reference and without specifying their capacities, as well as without identifying the consumers of trunk communication lines leased by the Government, Ministry of Defense, National Security Committee, and Ministry of Internal Affairs of the Republic of Kazakhstan).

**2. Management and Human Resources**

11. Certain decisions of the Board of Directors and Management Board containing Commercial Secrets.

12. Information on preparation, adoption and execution of certain decisions of the Company's management on production, scientific, technical, commercial, organizational, strategic and other issues discussed at meetings and negotiations with other legal entities.

13. Information on completed and ongoing M&A transactions, restructuring, reorganization of subsidiaries and affiliated organizations, their components, and all related documentation, excluding information subject to mandatory disclosure.

14. Information on the development prospects of the Company (including information on the Business Plan and budgets of the Company and its subsidiaries).

15. Issues related to the Company's strategy.

16. Salary structure and amounts for employees of the central office and branches, excluding members of the Board of Directors, Chief Directors, and key management personnel.

17. Contents of employee personnel files, including personal data.

18. Composition of the executive reserve of the Company's management, related to top-level managers.

19. Specific documents from the BRD containing Commercial Secrets.

20. Orders containing personal data of employees: on hiring, disciplinary actions, termination of employment.

21. Information about employees entered into the SAP R/3 HR module.

22. Information about the home phone numbers and addresses of executives at all levels of the Company.

### **3. Projects**

23. Information revealing prospective tasks for developing projects and special orders.

24. General schemes for the development of telecommunications in regions and cities under republican jurisdiction, without geographic references and without information on their capacities.

25. Project passports.

26. Technical assignments for project development.

27. Summary data contained in the database, GIS Small world PNI.

28. Summary data contained in the database NRI Cramer.

29. Summary information on special consumers contained in the NRI Cramer database.

### **4. Market**

30. Information on original market research methods used by the Company.

31. Information on marketing research directions, market study results, including assessments of market conditions and prospects.

32. Information on original sales methods used by the Company.

## **5. Partners**

33. Systematized information on internal and foreign customers, contractors, suppliers, clients, consumers, service buyers, intermediaries, and other business partners of the Company, as well as its competitors, whose information is not available in public sources.

34. Information on the goals, tasks, and tactics of negotiations with business partners.

## **6. Negotiations**

35. Information on the preparation and results of negotiations with the Company's business partners.

## **7. Contracts, Agreements**

36. Terms of commercial contracts, payments, and services.

37. Terms of labor contracts (in terms of wages).

38. Summary tables of confidential rate calculations.

39. Information on traffic, income, and expenses by country, excluding statistical data.

40. Information contained in the electronic database "Contract Monitoring".

## **8. Prices**

41. Information on methods of calculation and tariff structure (prices) for services, excluding services in the natural monopoly sector.

## **9. Competitions/Tenders, Auctions**

42. Summary information on the areas and terms of rental and lease of real estate, excluding documents confirming the Company's ownership rights to assets on its balance sheet.

43. Summary information on the terms of transactions for the disposal and acquisition of real estate.

## **10. Finance, Economics, Law**

44. Information (register) about the shareholders of the Company, excluding information contained in public sources.

45. Information on the remaining balance of funds in the Company's accounts.

46. Content of accounting registers and internal reporting, excluding documents required to be published in printed form according to the legislation of the Republic of Kazakhstan.

47. Cost estimates required to maintain the main production assets in working condition.

48. Information on the claim and lawsuit work conducted by the Company until the completion of legal proceedings.

49. Information on methods and results of cost calculation for services, as well as cost estimates detailing the cost structure of services, excluding services in the natural monopoly sector.

50. Information on the results of tax and other audits.

51. Systems for motivating and rewarding staff at the central office of JSC "Kazakhtelecom" and its branches, excluding members of the Board, Chief Directors, and key management personnel.

## **11. Science and Technology**

52. Information on the state of software and computer systems.

53. Original ideas for research and development (R&D) and specific design works (SDW) by the Company's employees.

54. Information on the "know-how" status.

## **12. Security**

55. Information on the procedures and status of organizing the protection of confidential information in the Corporate Information System (CIS) of JSC "Kazakhtelecom".

56. Information on the procedures and status of security, access control, and alarm systems at the Company's facilities.

## **13. Risk Management**

57. Risk management guidelines (Corporate Standard of the Risk Management System) of JSC "Kazakhtelecom".

58. Risk management strategy of JSC "Kazakhtelecom".

59. Risk register of JSC "Kazakhtelecom".

60. Work schedule for the further implementation, improvement, and effective functioning of the corporate risk management system at JSC "Kazakhtelecom".

61. Business continuity management concept of JSC "Kazakhtelecom".

62. Report on the results of the comparative analysis of business continuity management at JSC "Kazakhtelecom".
63. Standard Crisis Management Plan.
64. Standard Emergency Response Plan.
65. Standard Business Recovery Plan.
66. Risk management policy of JSC "Kazakhtelecom".

**Appendix 2  
to the Regulation on  
Commercial Secrets  
of JSC "Kazakhtelecom"**

**COMMERCIAL SECRET AGREEMENT  
on the non-disclosure of information constituting Commercial Secrets  
of JSC "Kazakhtelecom"**

I, \_\_\_\_\_  
\_\_\_\_\_,  
upon being employed in the position  
of \_\_\_\_\_,  
during my employment with JSC "Kazakhtelecom" and for 5 years after its termination,  
undertake:

1) not to disclose, transmit to third parties, publicly reveal, or use for myself or the benefit of others any information constituting commercial secrets entrusted to me or which becomes known to me in the course of my professional duties;

2) to carefully and conscientiously comply with the requirements of orders, instructions, and regulation regarding the protection of commercial secrets;

3) not to use the knowledge of commercial secrets to engage in any activities against the interests of jsc "kazakhtelecom";

4) in the event that third parties or organizations with which jsc "kazakhtelecom" has business relations attempt to obtain information constituting commercial secrets of jsc "kazakhtelecom" and/or other organizations with which jsc "kazakhtelecom" has business relations, i undertake to immediately inform:

the head of my department;

the Security Service of JSC "Kazakhtelecom";

5) Upon the termination of my employment with JSC "Kazakhtelecom":

I undertake to return all materials containing information constituting Commercial Secrets (manuscripts, drafts, drawings, magnetic tapes, punch cards, perforated tapes, discs, diskettes, memory drives, printouts, film negatives and positives, models, materials, products, etc.) that were in my possession during the course of my duties at JSC "Kazakhtelecom" to my immediate supervisor, or, in their absence, to the person acting in their place;

I undertake to immediately notify my direct supervisor of any loss or shortage of materials containing Commercial Secrets (identity cards, passes) as well as keys to restricted areas, storage rooms, safes (metal cabinets), personal seals, and any other incidents that may lead to the disclosure of Commercial Secrets, along with the reasons and circumstances that could lead to the leakage of such information.

I have been warned that failure to comply with any of the terms of this agreement may result in my dismissal from JSC "Kazakhtelecom".

I have also been informed of the relevant requirements for ensuring the protection of information constituting Commercial Secrets, and I am aware that violation of these

requirements may lead to criminal, administrative, civil-legal, disciplinary, or other liability in accordance with the applicable laws of the Republic of Kazakhstan.

Informed on \_\_\_\_\_ [date]

\_\_\_\_\_ / \_\_\_\_\_ /

(Full name)

(Signature)

**Security Service Worker** \_\_\_\_\_

/ \_\_\_\_\_ /

(Position, Full Name) (Signature)