Appendix to the Order of the Managing Director for Information Security of Kazakhtelecom JSC No. _____dated "__" _____ 2026

Information Security Risk Assessment Methodology Kazakhtelecom JSC

Almaty, 2026

CONTENT

Chapter 1. General provisions

1. This Information Security Risk Assessment Methodology of Kazakhtelecom JSC (hereinafter – the Methodology) defines the composition and procedure for performing procedures for identifying, analyzing, evaluating, controlling information security risks, as well as monitoring the effectiveness of applied risk management methods.

2. The Methodology has been developed in accordance with the legislation of the Republic of Kazakhstan, the Risk Management and Information Security Policy of Kazakhtelecom JSC (hereinafter – the Company), other internal documents of the Company, as well as on the basis of international practices in the field of risk management and internal control.

3. This Methodology has been developed in order to provide practical assistance to the Company's employees who identify, analyze, evaluate (reassess), control information security risks and monitor the effectiveness of information security risk management methods.

4. This Methodology is mandatory for employees holding senior positions, as well as employees involved in the information security risk management process. The heads of the structural divisions are responsible for bringing this Methodology to the attention of the employees of the supervised divisions.

Chapter 2. Terms, definitions and abbreviations

5. The following terms, definitions and abbreviations are used in this Methodology:

accessibility – a property of the system (environment, processing tools and technologies) in which information circulates, characterized by the ability to ensure timely and unhindered access of users to the information they are interested in and the readiness of appropriate automated services to service requests from users whenever they are contacted. there is a need;

DRMIC – Department of Risk Management and Internal Controls;

IS – information security;

Risk identification – the process of finding, compiling, and describing risk elements.;

An information asset (hereinafter referred to as IA) – a tangible or intangible object that is information or contains information, or serves to process, store, transmit information and is of value to Company in the interests of achieving goals and continuity of its activities.;

An information security incident (hereinafter referred to as ISI) – a single or serial malfunction of the information and communication infrastructure or its individual facilities that endanger their proper functioning and/or create conditions for the illegal receipt, copying, distribution, modification, destruction or blocking of electronic information resources;

confidentiality – a property of information that indicates the need to impose restrictions on the number of users who have access to this information, and is ensured by the system's ability to keep this information secret from users who do not have the authority to access it;

risk management – the process of selecting and implementing protective measures to change risks;

risk assessment – the process of comparing the results of a risk analysis with established risk criteria to determine whether the risk and/or its magnitude are acceptable or acceptable;

information security risk – the potential for a vulnerability to be exploited to endanger an asset or group of assets, leading to a threat to Company. It is defined as a combination of the probability of an event and its consequences.;

risk manager – a responsible employee of the Risk Management and Internal Controls Department.;

ISD – Information Security Department of Kazakhtelecom JSC;

risk reduction – actions taken to reduce the likelihood of information security events and their consequences;

SD – a structural division of the Central Office or a branch of the Company.;

threat – a potential or real possibility of unlawful intentional or accidental impact on an information asset, leading to loss, disclosure, or unauthorized changes to information properties (confidentiality, accessibility, integrity);

risk management – coordinated actions aimed at managing and managing an organization, taking into account existing risks.;

vulnerability – a flaw in an informatization object, the use of which may lead to a violation of the integrity and (or) confidentiality, and (or) accessibility of the informatization object.;

integrity – a property of information that consists in its existence in an undistorted form (unchanged in relation to some fixed state).

Chapter 3. Information security risk management methodology

§1. Information security risk management process

8. Information security risk management is a continuous cyclical process for identifying, assessing, monitoring information security risks, making and implementing management decisions aimed at reducing the likelihood of an adverse outcome and minimizing possible losses in the field of information security, integrated into the Company's overall risk management system.

9. The main objectives of information security risk management are:

1) identification of information security risks, their causes and ways of implementation;

2) analysis of the probability of realization of information security risks and the degree of consequences of information security violations;

3) decision-making regarding information security risks, planning and implementation of measures for their treatment;

4) conducting regular and effective monitoring of information security risks and improving the information security risk management process;

5) professional development of employees in the field of information security risk management.

10. The information security risk management process consists of the following main stages:

1) identification of information security risks;

2) information security risk assessment;

3) information security risk management;

4) Information security risk monitoring

11. The flowchart of the risk management methodology is shown in Figure 1.

§2. Identification of information security risks

12. The purpose of identifying information security risks is to identify possible information security threats that may harm the Company's activities, the causes of their occurrence and the possible consequences of their impact.

13. The following procedures are carried out to identify information security risks:

1) identification and evaluation of IA;

2) identification of information security threats;

3) identification of vulnerabilities;

4) identification of existing security features.

14. Identification and evaluation of IA, as well as determination of the degree of their confidentiality, integrity and accessibility are carried out by the joint venture companies of the Company, which are the owners of IA, together with the ISD.

15. Identification of the IA consists in identifying the IA at the disposal of the joint venture, as well as in identifying their users, means of processing, transmitting and storing data.

16. The assessment of IA is considered from the point of view of a qualitative assessment of possible damage due to violation of their properties. The damage caused by an information security violation is assessed according to the criteria set out in Table 1 of Appendix 1 to this Methodology.

17. An IA is considered valuable when the degree of the consequences of an information security violation inflicted on any of the three properties of the IA (confidentiality, integrity, accessibility) is assessed at a high and critical level.

18. In case of creation of new business processes or when changing existing ones, as well as when introducing new information systems, additional identification and evaluation of IA is carried out.

19. The results of the identification and assessment of IA are drawn up in accordance with Annex 2 to this Methodology.

20. At the request of the ISD, the Joint Venture provides information on the means of processing, transmitting and storing IA in accordance with Annex 2 to this Methodology.

21. The identification of threats, vulnerabilities and existing means of protecting information assets is carried out by the ISD.

22. Identification of possible threats is carried out using available information about ISI, previously conducted audits and information from other sources. Information about possible information security threats can also be obtained from the users of the Information agency, the management of the Company and other sources. Examples of the types of

information security threats and their sources are given in Appendix 3 to this Methodology.

23. Using the results of previous information security threat identifications, it is necessary to take into account that significant threats are constantly changing, especially if the business process or information security is changing.

24. An important element of the information security threat identification process is the identification of threat sources and threat implementation mechanisms on which further risk identification and assessment will be based, as well as ways to process them.

25. The identification of vulnerabilities is carried out in order to identify shortcomings and weaknesses in existing information security tools that can be used to implement information security threats. To identify vulnerabilities, reports on previous risk assessments, comments from internal and external auditors, security requirements, and security test results are used.

26. Vulnerabilities can be identified in the following areas: organization of work, processes and procedures, personnel, physical environment, configuration of information systems, hardware, software and data network equipment, dependence on external parties, and others.

27. The following methods can be used as vulnerability detection methods:

1) checking the system configuration manually;

2) network scanning;

3) penetration testing of the software and hardware of the data transmission network;

4) program code analysis and others.

28. Examples of vulnerabilities in various areas of information security, as well as examples of threats that can exploit these vulnerabilities, are given in Appendix 4 to this Methodology.

29. The identification of existing means of protection is carried out in order to determine the degree of protection of an information asset from threats, including their compliance with the requirements of information security imposed on IT.

30. The following measures may be used to identify protective equipment:

1) study of documents containing information on the applied means of protection (documents regulating business processes and work with the IA in question, a plan for the implementation of protection measures, etc.);

2) inspection of protective equipment, checking their actual functionality with a documented list of functions;

3) checking the implemented security measures for their correct and effective operation;

4) analysis of the results of internal and/or external audits of the information security of the Company and the measures taken to eliminate the identified violations and comments

31. Based on the results of identification, existing methods and means of protection can be identified as ineffective, insufficient or unjustified. For such methods and means of protection, it is important to determine the need to remove them and replace them with other, more effective ones.

32. The results of the identification of information security threats, vulnerabilities and information asset protection tools are recorded in accordance with Annex 5 to this Methodology.

§3. Information security risk assessment

33. Information security risk assessment is aimed at analyzing identified information security risks and determining their level.

When assessing the risk of information security, it is necessary to analyze the degree of its impact and the probability of its occurrence for each of the properties of information security.

To analyze the risks of information security, a preliminary study is conducted of the causes of information security risks, their sources and possible losses in the event of their implementation, taking into account the results of identification, threats, vulnerabilities, and information security tools.

Information security risk assessment activities are carried out by experts, employees of the Information Security Service and the owner of the Information Security Agency (hereinafter referred to as experts). If necessary, employees of the joint venture using the IA in question may be involved as an expert. The information security risk assessment is updated at least once a year, and is additionally carried out in case of changes in the technologies used, business processes, internal documents of the Company, as well as when identifying new threats, vulnerabilities identified by the results of audits, investigations of information security violations, and others.

34. To determine the level of information security risk, it is necessary to assess the likelihood of information security threats and the degree of consequences of information security violations.

35. To assess the likelihood of the identified information security threats, the following factors are analyzed:

1) information about the location of the information security threat source;

2) information about the motivation and qualifications of the source of the information security threat and the reasons for its occurrence;

3) statistical data on the frequency of previously implemented information security threats;

4) information on ways and mechanisms of implementing information security threats;

5) information about the vulnerability of existing information asset protection tools.

The probability of an information security threat is assessed according to the criteria defined in Table 2 of Appendix 1 to this Methodology.

36. When receiving different expert estimates, the average estimate of the indicators under consideration is taken. In quantification, the average estimate is the arithmetic mean of the experts' estimates rounded to an integer ("the sum of the experts' estimates/the number of experts", here [] – rounded to an integer), and the average qualitative estimate is equal to the calculated average quantitative estimate according to Tables 1 and 2 of Appendix 1 to this Methodology.

37. The level of each information security risk is determined by experts based on an assessment of the likelihood of information security threats and an assessment of the degree of consequences of information security violations, given in accordance with Table 3 of

Appendix 1 to this Methodology.

The results of the conducted information security risk assessment are recorded by the ISD in the form KT/F-31-05, according to Appendix 5 to this Methodology.

Based on the results of the conducted IS risk assessment, an IS risk map is compiled, which is a schematic representation of the classification of IS risks according to the degree of their impact and the likelihood of their occurrence.

§4. Information security risk management

38. Risk management consists in deciding on further actions regarding information security risks with high and critical levels identified as a result of the risk assessment.

39. The selection of information security risk management measures is carried out by the ISD experts together with the IA owner.

40. There are the following risk management options or combinations thereof:

1) risk minimization;

2) risk elimination;

3) Risk taking;

4) transfer of risk.

41. Risk minimization can be achieved by introducing new or updating existing security features. The choice of protective equipment should be justified and take into account various limitations in their choice, such as:

1) temporary;

2) financial;

3) technical;

4) operational;

5) legal;

6) labor and others.

42. Risk mitigation may be the most beneficial solution and may be applied in cases where the risks are considered too high or the cost of implementing other risk management options exceeds the benefit. In such cases, business processes may be adjusted or revised in such a way as to eliminate the risk in question.

43. Accepting a risk means refusing to take any actions aimed at reducing the likelihood or impact of risk. Such risks are subject to mandatory review at least once a year.

44. Risk transfer consists in delegating risk to another party that can manage this type of risk most effectively. Risk transfer can be carried out by insuring losses from its damage, or by concluding a contract with a service provider who will control the risk.

45. Risk transfer may create new risks or change existing ones, therefore, after taking this measure, additional risk reassessment is necessary.

46. In order to implement the decisions taken on information security risk management, the Company's Information Security Risk Management Plan (hereinafter referred to as the Processing Plan) is being developed in accordance with Appendix 6 to this Methodology.

§5. Information security risk monitoring

47. Information security risks are monitored by the owner of the information agency and the employees of the Information Security Service, and are aimed at analyzing the following factors:

1) the emergence of new IS threats and the definition of mechanisms for their implementation;

2) the emergence of new or strengthening existing vulnerabilities;

3) changing the probability of information security risks;

4) changing the degree of consequences of implementing information security violations;

5) deterioration of the effectiveness of existing methods and means of protection;

6) changing the sources of realized information security risks;

7) other.

Based on the monitoring results, if the above factors are identified, the ISD initiates a reassessment of the IS risks.

§6. Procedure and deadlines for organizing information security risk management

48. Annually, no later than February 20 of the reporting year, the joint venture of the Company sends to the ISD for approval the results of the identification and assessment of IA in the form KT/F-31-04, in accordance with Appendix 2 to this Methodology.

49. The ISD reviews the results of the IA assessment for compliance with Appendix 2 to this Methodology and, no later than March 10 of the reporting year, sends the list of valuable IA for review and approval to the Managing Director for Security.

50. ISD:

1) identifies information security risks for the Company's securities by April 1 of the reporting year;

2) conducts an assessment and processing of identified information security risks by May 1 of the reporting year, together with the owner of the information agency;

3) develops a Processing Plan in the KT/F-31-06 form and sends it to the IA owner for review and approval no later than May 20 of the reporting year.

51. Within 10 (ten) business days, the IA owner reviews the Processing Plan, and if there are comments and suggestions, sends them to the ISD or informs them of their absence.

52. The agreed Processing Plan is sent to the Managing Director for Security for approval within 10 (ten) business days. No later than 3 (three) business days after the approval of the Processing Plan, the ISD sends it to the relevant joint ventures for the implementation of the measures provided for in the Processing Plan.

53. On a quarterly basis, no later than the 10th business day following the reporting period, the ISD sends the information on the execution of the Processing Plan, or changes to the measures and their deadlines in the form KT/F-31-07, according to Appendix 7 to this Methodology.

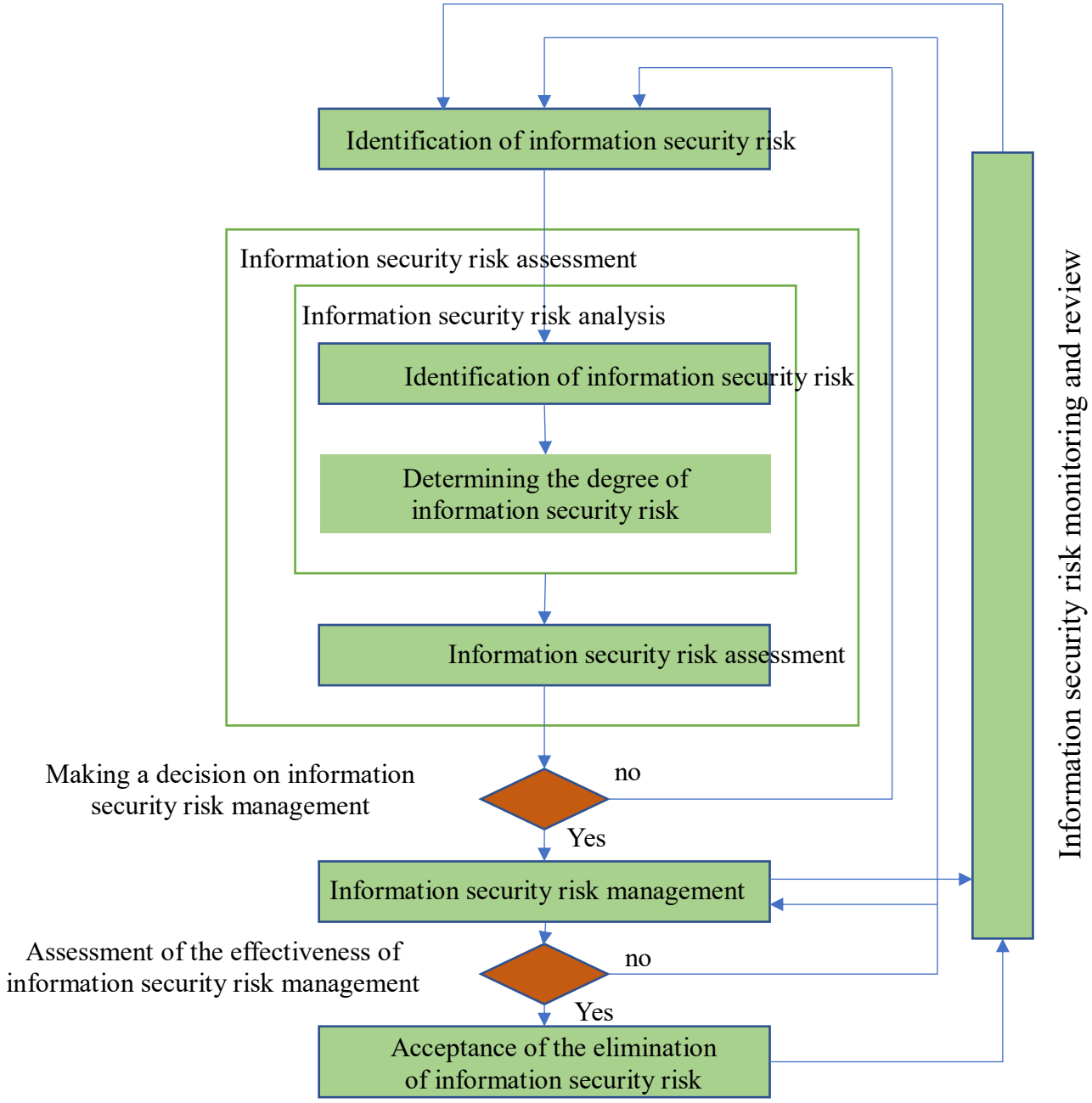

Figure 1 – Flowchart of information security risk management methodology

Chapter 4. Responsibilities and powers

54. Managing Director of Security:
1) reviews and approves the Processing Plan;
2) controls the implementation of the Company's Processing Plan;
3) reviews and approves the List of valuable IA.
55. SD:
1) identifies and evaluate IA in a timely manner;
2) provides and monitors internal control in the joint venture;
3) provides timely information to the ISD on identified and/or realized risks of

information security of ongoing business processes in accordance with Appendix 8 to this Methodology;

4) executes the Processing Plan within the established time frame;

5) prepares and provides timely information to the ISD on the execution of the Processing Plan.

56. ISD:

1) provides operational information security risk management of the Company;

2) timely identifies information security risks;

3) develops a Processing Plan, implements and monitors its execution;

4) promptly registers and takes operational measures on realized information security risks;

5) ensures an appropriate level of information security in Company;

6) develops and improves the methodological framework for information security risk management in the Company;

57. DRMIC:

1) participates in the development and improvement of the methodological framework for information security risk management in the Company.

2) monitors the execution of the Joint Venture Processing Plan;

provides consulting assistance to the ISD on the requirements of this Methodology.

Chapter 5. Documentation

KT/F-31-04 – List of information assets
KT/F-31-05 – Information Security Risk Register
KT/F-31-06 – Information Security Risk Management Plan
KT/F-31-07 – Information Security Risk Assessment Report

Chapter 6. Link

ISO 27005-2010 Information Security Risk Management.
ST RK ISO/IEC 31010-2010 Risk Assessment Methods
ISO 9001:2015 Quality Management System. Requirements.
ST RK 9001-2016 Quality Management System. Requirements.

Appendix 1
to the Methodology for assessing Information
Security risks of Kazakhtelecom JSC

Table 1. Assessment of the degree of consequences of information security violations

Degree of consequences of information security violations qualitative/quantitative scales	Description of the damage caused by an information security violation		
	Disruption of business continuity	*Loss of reputation Financial losses*	*Financial losses (affected by the size of risk appetite)*
Minor/1	The consequences of realizing the risk are insignificant. 1.The continuity of the production process/service provision may stop, it is possible to eliminate the causes of the shutdown within 1 hour 2. The quality of management will be reduced, without the threat of loss of control 3. The qualitative and quantitative results of the production process/service provision will deteriorate, but the result will remain acceptable The actual time frame for achieving the goals may increase.	Short-term negative articles by a limited number of media outlets, as well as limited dissemination of negative information on social networks; no impact on the rating; a slight decrease in support from stakeholders, a decrease in the trust of some parties interacting with Company (counterparties), a decrease in trust from some individuals among the population of the Republic of Kazakhstan	Up to 15%
Notable/2	The consequences of realizing the risk are significant, but can be completely corrected. 1.The continuity of the production process/ service provision will stop, it is possible to eliminate the causes of the shutdown within 12 hours 2 . Partial loss of control, while maintaining the basic control functions. 3 . It will worsen the qualitative and quantitative results of the production process/service provision, the result may be unacceptable. The actual time frame for achieving the goals will	Periodic negative media reports, dissemination of negative information about Company on social networks and blogs; not a significant effect on the rating; decrease in the support of stakeholders. loss of trust of the parties interacting with the Company (counterparties) and the population of the Republic of Kazakhstan	From 15% to 25%

	increase		
High/3	The consequences of realizing the risk are very significant, but they can be corrected to a certain extent. 1. The continuity of the production process/service provision will stop, eliminating the causes of the shutdown will take more than 12 hours 2. Partial loss of control, with the threat of loss of basic control functions. 3.Unacceptable result of the production process that does not meet the requirements 4. The actual time frame for achieving the goals will increase significantly.	Constant negative reports by local media, replication of information on social networks, blogs; negative effect on the rating; significant decrease in the support of stakeholders. The dissemination of negative information about the Company through the media, forums and blogs, the Internet, and the refusal of some interacting parties (counterparties) to cooperate with the Company.	From 25% to 35%%
Critical/4	Critical consequences from the realization of risk, which can only be partially eliminated. Will cause a complete shutdown of the production process/service provision	Constant negative reports from the international media, the strongest negative effect on the rating. Serious deterioration of the Company's image, loss of trust on the part of a significant part of the parties interacting with the Company (counterparties) and the population of the Republic of Kazakhstan.	Over 35%

Table 2. Assessment of the probability of the implementation of information security threats

The level of probability of the implementation of information security threats qualitative/quantitative scales	*Description*
Rare/1	It is unlikely that the implementation of information security threats will occur. There are no statistics, motives, etc. that would indicate that this will happen.
From time to time/2	There is a possibility that the implementation of information security threats will occur. There have been incidents in the past, or there are statistics or other information indicating that such or similar incidents have occurred before, or there are indications that certain reasons for such actions may be sources of threat.
Often/3	It is characterized by the presence of a high probability of the implementation of information security threats. There are statistics or other information indicating that the implementation of information security threats will occur. There are serious reasons or motives for the sources of the threat to take action.
Very often/4	It is expected with great confidence that the implementation of information security threats will take place. There have been incidents in the past, or there are statistics or other information indicating that such or similar incidents have occurred all the time.

Table 3. Determination of the information security risk level

Information security risk level		**The degree of consequences of information security violations**			
		Minor	*Notable*	*High*	*Critical*
Level of probability of the implementation of information security threats	Rarely	Low	Low	Average	Average
	From time to time	Low	Average	High	High
	Often	Average	High	High	Critical
	Very often	Average	High	Critical	Critical

Appendix 2 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

KT/F-31-04 – List of information assets

1	2	3	4	5	6	7	8	9		
№	Name of the information asset (IA)	Name of the business processes in which IA is used	Division that forms the IA	Divisions-users of IA	Processing and storage facilities	Transmission medium	IA properties that may be violated	Assessment of the degree of consequences of an information security violation		
								Disruption of business continuity	Loss of reputation	Financial losses
1 (example)	Personal data of the client (individual)	Provision of ID Net service	Business-to-Customer Division	Business-to-Customer Division	CRM 2.0	Corporate data network	Confidentiality	Critical	Critical	Notable
							Integrity	Critical	High	High
							Availability	*Notable*	Notable	Notable
2										

Appendix 3 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

An example of threat types and their sources
Threats may be intentional (D), accidental (A), or related to the external environment (E).

Sources	Threats	Designation
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Destruction or damage of equipment or media	A, D, E
	Dust, corrosion and icing	A, D, E
Natural events	Climatic phenomena	E
	Seismic phenomena	E
	Meteorological phenomena	E
	Flood	E
Loss of necessary services	Failure of the air conditioning or water supply system	A, D
	Power outage	A, D, E
	Telecommunication equipment failure	A, D
Malfunctions due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulse	A, D, E
Asset compromise	Interception and sending of a compromised signal	D
	Eavesdropping	D
	Theft of media or documents	D
	Restoring information on media sent for recycling	D
	Information discovery (disclosure)	A, D
	Data from unreliable sources	A, D
	Hardware tampering	D
	Interference with software tools	D
	Threat of privacy violation	A,D
	Threat of accessibility violations	A,D
	Threat of integrity violation	D
	Location detection	D
Technical failures	Hardware malfunction	A
	IP saturation	A, D
	Software failure	A
	IP maintainability violation	A, D
Unauthorized actions	Unauthorized use of equipment	D
	Fraudulent copying of software	D
	Data distortion	D
	Illegal data processing	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Falsification of rights	D
	Denial of actions	D
	Violation of the working capacity of the staff	A, D, E

Appendix 4 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

Examples of vulnerabilities in various areas of information security and their threats

Тип	Examples of vulnerabilities	Угрозы
Hardware facilities	Poor-quality maintenance, installation from damaged storage media	Violation of the maintainability of the information system
	Susceptibility to humidity, dust, pollution	Dust, corrosion, icing
	Ineffective control over making configuration changes	Error in use
	Susceptibility to voltage changes	Loss of power supply
	Unsecured storage	
	Lack of caution when destroying	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	Absence or insufficient software testing	Theft of media or documents
	There is no 'logout' when leaving the workstation	User abuse of authority
	Transfer or reuse of media or data without proper erasure	Abuse of rights
	Insufficient number of checks	Abuse of rights
	Incorrect allocation of access rights	Abuse of rights
	Widespread software	Unauthorized modification of existing systems
	Complex user interface	Data distortion
	Disadvantages of documentation	Error in use
	Setting incorrect software settings	Error in use
	Lack of backup procedures	Error in use
	Unauthorized copying	Loss of information
	Unsecured connections to public networks	Theft
	Incorrect dates	Unauthorized access
Network	Disadvantages of identifying and identifying mechanisms for user authentication	Error in use
	Unsecured password tables	Forging rights
	Improper password management	
	Launching redundant services	Unauthorized access
	Incomplete or new software	Forging rights
	Vague or incomplete specifications for developers	Illegal data processing
	Ineffective control over making changes	Software failure
	Uncontrolled downloading and use of software	Software failure
	Disadvantages of the backup procedure	Software failure
	Disadvantages of the physical protection system (buildings, doors and windows)	Use of malicious and unlicensed software
	Lack of evidence of sending or receiving messages	Distortion and loss of recovery data
	Unsecured communication lines	Theft of media or documents
	Unsecured sensitive traffic	Denial of actions
	Poor joint wiring	Eavesdropping
	Incorrect network architecture	Data interception, unauthorized access

	Transmitting passwords in clear text	Telecommunication equipment failure
	Insufficient network management (the system's ability to withstand routing errors)	Remote espionage
	Unsecured connections to a public network	Remote espionage
	Lack of procedures to ensure the return of resources upon dismissal	Saturation of the information system
	Insufficient competence of staff in information security issues	Unauthorized use of equipment
	Improper use of software and hardware	Unauthorized access
	Possible difficulty in defining security requirements	Error in use
	Lack of monitoring mechanisms	Error in use
	Insufficient supervision of freelance and off-duty workers	Error in use
	The lack of specific instructions for the proper use of data transfer media and messaging	Illegal data processing
Location of the organization	Insufficient physical control over access to the building and its premises	Theft of media or documents
	Flood	Unauthorized use of equipment
	Lack of physical protection of the building, doors and windows	Destruction of equipment or media
	Shortcomings in the access rights review procedure	Loss of power supply
	Omission of terms (regarding security) in contracts with clients and/or third parties	Theft of equipment
	Shortcomings in the information processing control procedure	Abuse of the right
	Lack of procedures for risk identification and assessment	Abuse of the right
	Complete or partial absence of information in fault reports, administrator and user logs	Abuse of the right
	Inappropriate response from the service provider	Abuse of the right
	Omission of terms (regarding information security) in service agreements	Abuse of the right
	Disadvantages of the change control procedure	Violation of the maintainability of the information system
	Disadvantages of a formal management procedure with information security management system documentation	Violation of the maintainability of the information system
	Shortcomings in the procedure for providing public access to information	Violation of maintainability
	Improper allocation of information security responsibilities	Data distortion
Other	Disadvantages in the implementation of continuity plans	Data from unreliable sources
	Lack of procedures for ensuring software input into operational systems	Denial of actions
	Lack of reports in the administrator and operator registration files	Hardware failure
	Lack of procedures for processing classified data	Error in use
	Omission of conditions (regarding information security) in contracts with employees	Error in use
	Lack of a specific disciplinary process in case of an information security violation	Error in use
	Insufficiency of certain rules on the use of mobile	Illegal data processing

	computer equipment	
	Non-compliance with the norms of "clean desk and clean screen"	Theft of equipment
	Lack of restrictions on information processing facilities	Theft of equipment
	Lack of established control mechanisms in case of safety violations	Theft of media or documents
	Lack of regular reviews of control results	Theft of media or documents
	Lack of procedures for reporting security vulnerabilities	Theft of media or documents
	Lack of procedures for agreeing terms with intellectual property	Unauthorized use of equipment

Appendix 5 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

KT/F-31-05 – Information Security Risk Register

№	Information asset	Риск	Probability of occurrence		Probability estimation	Possible consequences					Assessment of the consequences	Risk assessment (probability * consequences)	A risk management plan (for risk level >4) may refer to an external plan	The risk factor after the implementation of the plan
			Probability	Previous manifestations		Probability of loss of the Company's Client	Potential harm to Company's IP	Inability to meet the requirements of the regulator	Potential non-compliance with the legislation of the Republic of Kazakhstan	Impact on the reputation of the Company				

Appendix 6 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

KT/F-31-06 – Information Security Risk Management Plan

General description of the risk

Date of filling in	
Name of the risk	
Risk code	
Risk Owner/Position	
Full name	
Structural division	

Risk management measures

№	Risk factor/consequence	Name of the event	Implementation plan (stages of the event)	Implementation period	Responsible department for the event	Budget (thousand tenge)	Expected result/Goal	Indicator/calculation of the effect

Appendix 7 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

KT/F-31-07 – Report on completed information security risk management activities

General description of the risk

Date of filling in	
Name of the risk	
Risk code	
Risk Owner/Position	
Full name	
Structural division	

Risk management measures

№	Risk factor/consequence	Name of the event	Implementation plan (stages of the event)	Implementation period	Responsible department for the event	Execution Status (Yes/ No)	Budget (thousand tenge)	Expected result/ Goal	Indicator /calculation of the effect	Result, taking into account the measures taken (effect)

Appendix 8 to the
Methodology for assessing
Information Security risks of
Kazakhtelecom JSC

The form of registration of risky events on information security risks on ___ _____ 20___

Structural division of Kazakhtelecom JSC_____

Date of occurrence (detection) of the event	The structural division of the Company that resulted in the event	Event description/violation	Reason for the occurrence of the event	Estimated/actual size of the consequences of a risky event (damage/loss) *	Measures to minimize/eliminate a risk event or its consequences
1	2	3	4	5	6

* In the column "Estimated/actual size of the consequences of a risky event (damage/ loss)", indicate the possible (actual) amount of loss and/or other possible or actual consequences.

Executor: _____ signature: _____ date:_____
Agreed: _____