Appendix
to the Order of Kazakhtelecom JSC
dated 29 __July_____ 2021
No. 207___

Appendix
to the Order of Kazakhtelecom JSC
dated __ _____ 2022
No. _____

Security Policy for acquisition, development, operation of software and hardware-software of Kazakhtelecom JSC

Almaty, 2022

Contents

1 Terms, Abbreviations, and Definition

IS administrator - a privileged user who has extended powers (privileges) to configure and operate the IS, as well as to manage access to the IS;
AED - archive of electronic documents;
IS - information security. The state of security of information resources and systems, which ensures their confidentiality, integrity, authenticity and availability, which is achieved by a whole complex of organizational and technical measures aimed at data protection;
IR - information resource (asset). For the purposes of this Policy, it means an ordered set of information presented in electronic form (files, databases, algorithms, computer programs, applications, etc.) and contained, stored, processed, transmitted and used in the Company's information systems (data transmission networks, systems for storage, processing, transmission, visualization of information, etc.);
IS - information system. A system designed to store, process, search, disseminate, transfer and provide information using appropriate organizational resources (human, technical, financial, etc.);
IT - information technology. Processes, methods of searching, collecting, storing, processing, providing, distributing information and ways of implementing such processes and methods;
RD - regulatory documentation of the Company (policies, standards, orders, regulations, guidelines, instructions, etc.);
Company - Kazakhtelecom Joint Stock Company;
ES - experimental service;
Computer equipment passport - a document containing a complete list of computer equipment and software;
List of software - a document “List of software authorized for use”. It contains a list of commercial and freely distributed software authorized for use in the Company for a specified period. It shall be approved by an order or any other regulatory document with appropriate force.
Software - software;
Policy - this Security Policy approved by the Company when acquiring, developing, operating software and hardware and software means of Kazakhtelecom JSC;
User - the Company's employee or third party's representative working with the Company's IS and using its IR in accordance with the established rights and rules of access to information;
Industrial (production) operation;
Computer equipment means computer equipment (stationary computers or workstations, portable computers or laptops, etc.);
SS - structural subdivision of the Company;
SS IT - a structural subdivision of the Company responsible for IT, technical maintenance and operation of the Company's IR and IS;
SS TS - a structural subdivision of the Company or a subdivision (or organization) engaged to perform these functions, which performs technical support of users and IT systems in the Company;
RS - requirement specification;

TS - technical support;
Third party, third person - an individual or legal entity, contractor, supplier, partner, counterparty, contractor, etc., interacting with the Company on the basis of contractual agreements and not being a full-time employee of the Company;
PTA-Private Technical Assignment;
EDS - the Company's electronic document management system;
PoC - Proof-of-concept ("pilot" project, concept testing, etc.). Demonstration of practical feasibility of a method, idea, technology, realizability in order to prove the fact that the method, idea or technology works.

2 Purpose of the Policy and its scope

1. This Policy shall regulate the processes of software acquisition, development, testing, implementation and operation in the Company's IS.

2. The Policy is a guiding document and is intended for mandatory use in the Company.

3. The requirements of the Policy minimize the probability of negative consequences and security threats to the Company's IS due to violations of the requirements to the processes of software acquisition, development, testing and operation.

4. Negative consequences may include the probability of damage to the Software and IS, emergence of Software and IS vulnerabilities, introduction of malware into the IS, disclosure or loss of sensitive and confidential information, theft of intellectual property, reputational consequences, as well as impact on important internal systems and business processes of the Company.

5. This Policy shall apply to any Software running on the Company's IS resources.

6. The Policy establishes the responsibility of all Company employees and third parties using the Company's IR and IS, developing, acquiring, testing, using, operating and maintaining the Software for the benefit of the Company, and is binding.

7. The Policy is intended to be distributed within the Company and provided to all Managers, Employees of the Company and other interested parties - participants of the Company's business processes.

8. All exceptions to the rules and requirements of this Policy shall be agreed with the SS IS.

3 General provisions and requirements of the Policy

9. The Policy is developed in accordance with the legislation of the Republic of Kazakhstan in the field of IS, the regulatory and supervisory authorities (regulatory and supervisory bodies), IS Policy of the Company, IS Concept of the Company, series of international standards on IS ISO/IEC 27000, COBIT, ITIL, current state and near-term prospects of development of the Company's information structure and the possibility of modern organizational and technical methods of information protection.

10. The provisions of the Policy shall be revised on a permanent basis, but at least once every two years.

11. Unscheduled revision of the Policy shall be carried out in case of:

1) changes in regulatory legal documents of the Republic of Kazakhstan, RD of the regulator (regulatory and supervisory authorities) defining IS requirements;

2) detection of reduction of general and/or private level of IS of the Company (according to the results of internal or external audit);

3) significant changes in organizational and/or infrastructure, resources and business processes of the Company;

4) identification of significant deficiencies or contradictions of the Policy provisions with other internal documents of the Company.

12. The provisions of the Policy may be supplemented, but not canceled (replaced), by the provisions of other private IS policies of the Company and documents developed on their basis.

13. Additional information on safe operation and information protection in the Company's IS can be obtained from other private IS policies of the Company.

14. Any Software used to carry out the Company's activities shall comply with its licensing terms (regardless of whether it is commercial or freely distributed), be used strictly in accordance with the license agreement, be approved in the Software List and be purchased directly from the developers or official representatives and suppliers. Cases of storage and/or use of Software that is not licensed shall be excluded.

15. All processes and procedures related to the acquisition, implementation, testing, commissioning, operation, support, maintenance, administration, troubleshooting, etc. of the Software shall be performed in accordance with the established procedures. software shall be performed in the prescribed manner, in strict compliance with the requirements of the provisions of this Policy and other internal RD of the Company.

16. To fulfill the requirements of this Policy, the Company shall develop and implement the Software List (see Appendix 1 to this Policy) containing the list of software categories and requirements for them. For the categories, the following shall be defined:

1) descriptions;

2) requirements (criteria) for permissibility of installation and use.

17. The following conditions apply to the list of categories:

1) Software of certain categories may be prohibited completely;

2) only individual software of a category is allowed to be used;

3) individual software of a category is prohibited, everything else is allowed;

4) the requirements may be supplemented and combined.

18. The objectives of the Software List development are as follows:

1) protection of the Company's CE, IR and IS from malware, virus attacks and other security threats;

2) to reduce the probability (risk) of the Company's information leakage;

3) reducing the probability (risk) of transfer of the Company's internal information (including categorized information) via publicly available, external and/or prohibited servers (services);

4) increasing manageability and controllability of the used software by the applied and prospective information protection and monitoring means.

19. The following principles shall be applied in the development of the Software List:

1) the prohibition to use the software should not interfere with the performance of official, functional duties of persons working with it (if there are no real alternatives to the software);

2) for distributed software, the maximum advantage should be given to the one whose servers are located in the Company's networks on the territory of the Republic of Kazakhstan;

3) in all other cases, if it is necessary to use external resources for the Company's software functioning and there is no other (alternative) acceptable solution, such use shall be justified and appropriate IS risks shall be taken, as well as the application of increased requirements to IS provision at all stages of implementation, use and monitoring of such software shall be ensured.

20. The list of software shall be developed, maintained and updated by the authorized SS IT in coordination with the SS IS.

21. Any SS initiating the acquisition, development, implementation, etc. of new software shall be required to formally notify the authorized SS IT of these facts in order to update the Software List.

22. Information on newly acquired Software shall be entered into the Software List in the form of an addendum and/or amendment.

23. In order to keep the Software List up-to-date, in the event of decommissioning (decommissioning) of a particular Software, it is necessary to make timely amendments (changes) to the Software List.

24. In case the regulatory legal acts of the Republic of Kazakhstan impose special requirements to the Software (for example, the requirement for certification of such Software by authorized bodies, etc.), it is necessary to ensure compliance with such requirements.

25. Only authorized software from the Software List, necessary and sufficient to perform the assigned tasks, shall be installed on the CE and IS.

26. The description of the CE configuration and the list of software installed on it shall be recorded in the CE Passport (see Appendix 2 to this Policy), which shall be signed by an authorized employee of SS TS, the head of SS TS, the CE user and his/her direct supervisor. This confirms the agreement of the parties:

1) with the configuration of the CE equipment and the list of installed software specified in the CE passport;

2) with the fact of transfer of responsibility for the use of any unlicensed software, unauthorized change of the CE configuration and unauthorized installation of any software on the CE entrusted to this user from the Company to the employee (CE user).

27. All operations on installation, maintenance and support, uninstallation of the CE software must be performed directly (with the participation of) authorized employees of SS TS.

28. Permission to use this or that software (especially such software as Google Drive, Yadex.Disk, etc.) does not indicate the permission to transfer information through it, which is the property of the Company, access to which is categorized, limited by the requirements of the legislation of the Republic of Kazakhstan, the requirements of the regulator, as well as the requirements of the provisions of the Company's Regulations.

29. Software purchase and development contracts shall include suppliers' obligations to maintain, update versions, eliminate and/or replace the Software in case of errors and/or incorrect operation of the Software.

30. If possible, and for specialized software - obligatory, the Software shall be supplied together with source code (codes).

31. When using the Software it is necessary to:

1) comply with the requirements of this Policy;

2) use the Software at your disposal exclusively for fulfillment of your official, job, functional, etc. duties;

3) ensure safety of the media with key information, certificates of authenticity of commercial software, etc., glued to the case of the system unit of the CE;

4) assist the authorized employees of the SS TS (if necessary, the SS IT and the SS IS) in performing works on installation, configuration, troubleshooting and audit (accounting), etc. of the installed software;

5) to notify the authorized employees of the TS (if necessary, the IT and SS IS) of any facts of violation of the requirements of this Policy.

32. When operating the Software, users are prohibited from:

1) illegal (unlicensed) use and storage of copyrighted information (software, photos, music files, games, etc.) on hard disks of the Company's CE and IS;

2) independently install software on the CE and other information processing tools;

3) independently make changes to the design, configuration, placement of the CE and other equipment of the Company's IS;

4) change the composition of the software installed on the CE (install new software, change the composition of software package components and remove software);

5) use the CE with installed software for purposes other than intended;

6) use the installed software not intended for the performance of their functional duties, including system utilities and programs;

7) to bring any system or application programs not specified in the CE passport on external media and unauthorizedly run them on their own or other CE.

33. Protection of operating systems and application software against known technical vulnerabilities shall be maintained by timely installation of critical security updates.

34. To ensure correct operation of the software, it is recommended to apply automatic software update systems. Critical software security updates shall be subject to mandatory distribution to all Company IS.

35. When changes are made to operating systems, including after installation of updates, the SS TS shall verify correct operation of critical applications.

36. SS IS shall regularly check the software installed in the Company for compliance with copyright and related intellectual property rights in accordance with the established requirements.

37. Requirements for third party representatives using the Company's software in their activities shall comply with the requirements of the provisions of this Policy and shall be included in the relevant provisions of contracts and agreements.

38. Software installed or used in the Company in violation of this Policy shall be blocked and/or removed by authorized and responsible persons of the relevant SS.

39. Any initiatives and actions regarding the Software (acquisition, implementation, accounting, storage, use, etc.) shall be performed in accordance with the procedures and forms established and adopted by the Company, in compliance with the requirements of the provisions of this Policy and the documents developed on its basis.

40. The decision on the need, necessity to acquire and implement Software as part of various initiatives (design, modernization, expansion, etc.) required for the Company's operations and functioning of its business processes shall be made by the initiating interested SS (Customer SS).

41. Procedures for expert review, peer review and approval of a particular software within the framework of an initiative decision on the expediency of its application, compliance with the norms and requirements of the RD, compliance with the rules of implementation, integration and use in the Company's IS, verification of technical and technological aspects, etc., shall be

performed by an authorized collegial body (working group, council, committee, etc.) that shall review such initiatives.

42. Such authorized collegial body shall consist of competent employees of the IT and IS SS(employees from other SS may also be involved, if necessary), who shall have a high level of expertise in the issues and areas under consideration.

43. General Director of ITD (substitute person) should approve decisions made by the authorized collegial body.

44. The initiator of acquisition and implementation of new software can be:

1) Heads of SS performing maintenance, operation, support of CE, IR and IS of the Company;

2) managers of joint ventures engaged in project and other activities in the Company aimed at implementation, development, improvement, optimization, etc. of the Company's CE, IR and IS;

3) managers of joint ventures that develop and implement new business lines, business systems, etc.;

4) managers of joint ventures who are business owners of IR (IS) or persons acting in their interests.

45. The initiator shall prepare a memo addressed to the Company's Chief IT Director (substitute) containing:

1) justification of the necessity to use the new software;

2) functional requirements to the software;

3) list of tasks to be solved by the software;

4) the degree of criticality of input and output information.

46. The memo shall be prepared electronically in the EDS system.

47. The memo shall be coordinated with the IT and SS IS management.

48. The memo shall be submitted for review and approval to the Company's Chief IT Director (substitute person) who, based on the provided data and analysis, shall make a decision on the feasibility of using the new software and approve the initiation of the project for the software implementation.

49. All activities related to project preparation, execution of necessary documents and review of the project by the Project Committee shall be carried out in accordance with the Company's internal documents regulating the project management procedure.

50. In the course of project preparation, authorized employees of the IT SS shall study software market offers and conduct other necessary research to make a decision on the expediency of software acquisition or development.

51. Research on software protection mechanisms and IS compliance shall be carried out by authorized employees of the IT Service Provider.

52. The decision to develop or acquire software shall meet the functional requirements and general IS requirements of the Company's IS to the maximum extent possible.

53. Once the decision to acquire or develop software has been conceptualized, the detailed requirements for the new software shall be defined.

54. Functional requirements shall be presented by the employees of the initiator of software implementation (SS-customer).

55. The software to be acquired and implemented shall have the necessary and sufficient requirements for its operation and compliance with RD requirements.

56. The requirements in terms of technical implementation of the software shall be made by the SS IT .

57. Requirements in terms of IS mechanisms and software protection shall be imposed by the SS IS.

58. Requirements for new software within the IS framework shall be determined taking into account:

1) requirements of national and international IS standards;

2) requirements of the legislation of the Republic of Kazakhstan;

3) requirements of the regulator;

4) internal documents on IS provision;

5) the degree of criticality of the processed information, including the level of confidentiality;

6) additional requirements in the field of IS.

59. As part of IS requirements, the need to include the following functionalities in the software shall be determined:

1) identification and authentication;

2) management of access to and actions on data;

3) registration, storage and processing of security events;

4) file and program environment integrity control;

5) cryptographic protection of information during its storage in the Company's IS and transmission via networks and communication channels;

6) use of data confidentiality labels, screen and printed forms in accordance with the requirements of the provisions of the Company's RD;

7) other.

60. Once the detailed requirements have been determined, the software acquisition or development process shall be initiated.

61. Software shall be acquired in accordance with the Company's current procurement forms and rules.

62. The SS IS and SS IT shall participate in the work of the tender commission as technical experts.

4 Procedure for Acquiring Software

63.The following recommended course of action should be followed as part of the software acquisition:

1) If a decision is made to purchase software, a Technical Specification shall be drawn up, defining the composition, quantity and cost of the tools to be purchased;

2) The Technical Specification shall be prepared by an authorized person in the Company, which may be an IT SS or an authorized collegial body (working group, council, committee, etc.) with the possibility to attract the necessary competence from among the employees of the Company's SS to obtain the necessary consultations and assistance in work or it may be an external organization (company) providing the necessary services.

3) Technical specification shall be coordinated by the management of SS IT, SS IS and approved by the General Director of ITD;

4) After approval of the Technical Specification for software acquisition, it shall be fully analyzed by PoC. For this purpose the software vendor shall provide a demo version of the software (including software licenses, etc.) and qualified technical support for the PoC period;

5) the procedure for analyzing the new Software is described in the relevant clauses of this Policy. Upon completion of the analysis of the new Software within the framework of PoC, the Software Acceptance Certificate shall be drawn up in accordance with the results and recommendations (see Appendix 3 to this Policy);

6) if the Software analysis revealed partial and/or complete non-compliance of the Software with the requirements, a decision shall be made to purchase additional software to implement the requirements or to refuse to use the Software in the Company's IS;

7) on the basis of the agreed Software Acceptance Act, further procurement of a full-fledged software package may be carried out on behalf of the Chief Director for IT;

8) after acquisition (purchase and receipt) and before industrial use, the Software shall be introduced into the ES. The procedure of the ES is defined by the relevant clauses of this Policy.

5 Procedure for Developing Software

64.The following recommended procedure shall be followed in the course of software development:

1) based on certain requirements to the new software, the RS for software development or a document replacing it should be drawn up;

2) The RS should be prepared by an authorized person in the Company, which may be an SS IT or an authorized collegial body (working group, council, committee, etc.) with a possibility to attract necessary competencies from among the employees of the Company's SS to obtain necessary consultations and assistance in work or it may be an external organization (company) providing necessary services.

3) When drafting the RS, the following shall be determined:

the list of the Company's joint ventures where the software is to be implemented;

necessary information on information processing technology;

information on the information received as a result of solving tasks (information recipients, frequency of information issuance, samples of output and screen forms);

the degree of criticality of the processed information.

4) RS should be coordinated with the management of SS IT, with the management of SS IS in terms of availability of necessary requirements to functional capabilities for information protection and approved by the General Director of ITD;

5) after approval of the RS, if necessary, authorized employees of the IT SS shall develop a statement of work for implementation of a certain part of the requirements included in the RS. The RS shall be coordinated with the management of the SS IS;

6) software development shall be performed by an external (third-party) development organization, which shall have a license to develop the relevant software, on the basis of a contract. The contract shall specify:

requirements to the materials provided by the software development organization;

the developer's responsibility for the quality of work performed, for compliance of the software product with technical and functional requirements of the RS;

developer's responsibility for the absence of undocumented features in the developed software;

7) upon completion of the work, the developer organization shall provide the Company with:

finished software product;

software source codes

complete operational and technical documentation for the software.

8) upon receipt of the developed software product (Software), the authorized employees of the SS IT shall conduct PoC for Software analysis, the procedure of which is defined by the relevant clauses of this Policy;

9) errors detected in the course of testing shall be eliminated by the Software development organization within the established terms;

10) in case of impossibility of prompt elimination of faults in the Software, the software development organization together with the representatives of the IT Service Provider shall prepare proposals for their elimination in the course of ES. In this case the Software Acceptance Act shall be drawn up, to which a list of remarks (faults) to be eliminated in the course of ES shall be attached;

11) in case of impossibility to eliminate the faults in the course of ES, the development organization prepares proposals on additional software revision with a corresponding postponement of the completion date. Proposals shall be submitted to the SS IT management and the Chief Director for IT for final decision making.

6 Procedure for Analyzing Software

65. In the course of PoC to analyze the new Software, the following parameters of the Software shall be assessed:

1) compliance of the software with the functional requirements of the Company's IS;

2) compliance with the requirements for protection of information stored and processed in the Company's IS;

3) compliance of the software functional capabilities with the norms and standards of information processing in the Company's IS;

4) the ability to work effectively on software and hardware platforms and telecommunication infrastructure of the Company's IS;

5) reliability of operation;

6) flexibility of technological solutions, database, information exchange technology, integration capabilities, etc.;

7) quality of maintenance, possibility to receive and install new modifications and changes to the product as they appear;

8) quality of developed technical and user documentation, complexity of technical support, modernization of application software systems, modification and administration of the software;

9) ability to adapt to changing conditions of the Company's IS functioning, including the ability to maintain the required level of protection of the Company's IS resources;

10) absence of undocumented capabilities.

66. Software analysis shall be performed in accordance with the flowchart (see Appendix 4 to this Policy).

67. To conduct PoC and test (analysis, testing) of the Software, authorized employees of the IT SS shall develop a Program and methodology for testing (testing) of the Software, which shall regulate the procedure for conducting and types of tests, and shall contain:

1) description of the object of tests (name, scope and designation of the tested program);

2) purpose of the tests;

3) requirements to the program (requirements to be checked during tests and specified in the RS for the program);
4) requirements to program documentation (the composition of program documentation to be submitted for testing is specified);
5) means and procedure of tests (program and technical means used during the tests are specified, as well as the procedure of conducting the tests);
6) set of test tasks (descriptions of tests with indication of expected results of tests shall be given).
68.The software test program and methodology shall be coordinated with:
1) IS SP management regarding IS compliance;
2) IT governance.
69.Software testing program and methodology shall be approved by Director General of ITD.
70.A set of test tasks shall contain a list of tasks that allow to check fulfillment of all requirements of the RS or PDT. The minimum set of tests shall include verification of:
1) fulfillment of functional requirements when using the Company IS test data;
2) interaction (integration) of the new software with existing components of the Company's IS;
3) compatibility with various platforms and peripheral devices used in the Company's IS;
4) Software operability under critical operating conditions under heavy load and insufficient RAM, disk space, insufficient exchange rate in communication lines and channels, disconnection of part of power supply lines, communication lines and channels, etc.;
5) the level of software stability when exposed to various cyber threats, including denial-of-service attacks, exploitation of vulnerabilities in the code, etc.;
6) correctness of internal algorithms of variable calculation and protection against incorrect input/output;
7) documentation and help files;
8) correctness of operation of standard information protection mechanisms in the software;
9) the degree of compliance with the requirements of information protection standards, legislation of the Republic of Kazakhstan, regulator's requirements, as well as internal IS documents of the Company.
71.Testing of new software functionality within the PoC shall be carried out on a specially equipped stand (test zone, pilot zone, etc.). The stand shall be physically and logically isolated from the Company's networks and IS.
72.Verification of the software functionality shall be conducted jointly with:
1) IS administrators who will maintain this software;
2) authorized employees of the SS IS;
3) authorized employees of the SS IT;
4) authorized employees of the SS that initiated the implementation of the software;
5) if necessary, involving competent specialists from software developers and/or suppliers.
73.Data for testing shall be provided to the SS that will operate the new software (will be the user of the software). The data shall correspond to the information to be processed in the new subsystem of the Company's IS, but shall not contain confidential information.
74.The criterion of correct test execution is compliance of the test results with the requirements described in the RS.
75.All test results should be recorded in the Test Protocol, which should be signed by all test participants and approved by the General Director of ITD.

76.In case of full compliance of the software with the requirements of the RS, the decision to put the software into the DE is made.

77.Based on the result of the analysis the General Director of DIT makes a decision on the possibility of using the Software in the Company's IS and its introduction into the SE.

7 Procedure for Conducting ES

78.The following recommended procedure shall be followed during the:

1) on the basis of the Software Acceptance Act, the new software shall be evaluated jointly with:

IS administrators (if necessary, involving SS IS);

authorized employees of the SS that will operate the new software (will be the software user);

2) the duration of the software evaluation shall be not less than one month;

3) upon completion of the software ES, an Act of putting the software into operation (see Annex 5 to this Policy) shall be drawn up and signed by the heads of all SS involved in the ES. The IS auditor shall verify the correctness and accuracy of the Act. On the basis of the Statement, the new software shall be introduced into Industrial (production) operation.

8 Procedure for Storing Distributions, Licenses, and Software Documentation

79.The following recommended procedures shall be followed for the storage of software distributions, licenses and documentation:

1) IT and/or IS SS management should keep paper and/or electronic documentation for the software maintained by the respective unit;

2) if necessary, paper and/or electronic documentation may be kept at the SS that operates (is the user of the software) and/or is the business owner of the software. In this case, the head of such a SS shall appoint an employee responsible for storing the documentation. Access to the documentation may be granted only with the authorization of the head of the SS;

3) a single AED must be created for storing software distributions and documentation. Management of the AED shall be assigned to an authorized employee of the IT SS;

4) after the acquisition and/or development of new software, a Software Passport in paper and/or electronic form (see Annex 6 to this Policy) shall be prepared by the employees of the IT Service Provider;

5) software distributions, program codes, documentation and the Software Passport in electronic form shall be transferred to the AED;

6) access to the AED shall be restricted and provided in accordance with the procedure defined by the Policy on Access Management to the IR;

7) documents confirming the purchase of the Software shall be kept in the SS responsible for financial reporting (accounting department, etc.) throughout the entire period of use of the Software and licenses in the Company's activities, copies of the said documents shall be kept in the SS IT;

8) software license agreements, software protection keys, software distributions, etc. shall be kept in the IT department.

9 Procedure for Operating Software

80.The following recommended procedure shall be observed within the framework of the Software operation:

1) installation and configuration of new software shall be performed in accordance with the established requirements of the provisions of internal regulations (e.g., Rules for making changes to the configuration of the Company's IS hardware and software, etc.);

2) installation of software distributions not from the AED and not included in the Software List is prohibited;

3) permanent operation of the Software shall be carried out in accordance with the requirements of the license agreement;

4) he Software shall not include program debugging tools by the time of its commercial operation in the Company's IS.

10 Procedure for Monitoring Installed Software

81.The following recommended course of action shall be followed to control the installed software:

1) an authorized representative of the IT Service Provider shall control the installed software:
selectively on 5% of IT systems of the Company's IS users - twice a year;
on all servers and network equipment of the Company's IS - once a year;

2) after the control activities, the authorized representative of the IT SS shall prepare and send a report with the control results to the IS IS;

3) the SS IS shall analyze the reporting information and, in case of non-compliance of the installed software with IT system passports, server forms and software installation requests, the responsible employee of the SS IS shall act in accordance with the established rules for investigation of IS incidents;

4) the IS SS shall verify compliance with the requirements of the IS Policies during software implementation and verify the correctness of software implementation.

11 Roles and Responsibilities

82. Control over fulfillment of the requirements and rules of the Policy shall be vested in the IS SS, Heads of SS, Heads of the Company's branches.

83. Responsibility for control over the Policy's implementation and relevance, as well as its amendments, shall be vested in the SS IS.

84. Responsibility for ensuring proper fulfillment of the requirements and rules of the Policy shall be assigned to all interested SSs within the scope of their authority and in accordance with the provisions established by the Policy and the documents developed on its basis.

85.Heads of SSs are responsible for timely communication of the Policy requirements to the employees of their subdivisions and/or representatives of third parties as they relate to them and for compliance by the employees of their subdivisions and/or representatives of third parties with the requirements of the Policy.

86. Responsibility for organizational and methodological support of the processes of using the Company's IS software tools shall be assigned to the SS IS.

87.Control over the actions of IS administrators in the use of hardware and software shall be vested in the management of the IS in accordance with the requirements of the provisions of this Policy.
88. In case of detection of violations of the requirements of this Policy by an IS user (IS administrator), which have caused or may have caused serious damage to the Company's business activities, the management of the SS shall obligatory notify the IS SS of the incident and an internal investigation shall be initiated and conducted with the involvement of interested SSs and in accordance with the approved IS Incident Investigation Procedure.
89. Violation of the provisions of the Policy or documents developed in support of the Policy, including any intentional action taken to breach, block or otherwise circumvent established IS controls, may result in administrative or criminal penalties in accordance with applicable laws, as well as the Company's Personnel Management RD.
90.The decision on application and selection of liability measures shall be made by the Company's management based on the results of an internal investigation, depending on the expediency of application of the measures in question, as well as information on the willfulness of the violation.

Appendix 1
to the Security Policy for the Acquisition, Development, and Operation of Software and Hardware

List of authorized software

No.	Date of inclusion in the List	Software category	Description			Number of licenses and licensing features	Requirements
			Software manufacturer	Software name	Application area		
1	2	3	4	5	6	7	8
1	01.01.2021	Anti-virus software	Kaspersky	KAV	CE, servers	1000	Usage permitted
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

Appendix 2
to the Security Policy for the Acquisition, Development, and Operation of Software and Hardware

CE Passport

Number_____

Computer:

Name:		Inv. number:	
Model:		Serial number:	
Domain:		IP address:	

User:

Full name:		Number:	
E-mail:		Account:	
Group:		SS:	
Phone::		Note:	

Operating system:

Name:	Serial number:

Software:

Publisher:	Product:	Serial number:

Note:

_____

Date:	
Administrator:	
Owner:	

Employee of the SS TS

_____

(signature) (full name of the employee)

Manager of the SS _____

(signature) (full name of the employee)

Employee of the SS

_____

(user of the CE) (signature) (full name of the employee)

Appendix 3
to the Security Policy for the Acquisition, Development, and Operation of Software and Hardware

ACT
of acceptance and delivery of the software for trial operation

«___» _____ 20__ year No _____

This act is drawn up in the fact that

_____
(name of the developer/provider organization)

has developed/supplied the software

_____,

consisting of a set of tasks (tasks _____

Basis for performing work _____

The work to be submitted is presented in the form of

_____
(documentation name)

As a result of testing, it was established

_____
(this section reflects specific comments on program operation, failures, errors detected in the course of testing, indicating the reasons for their occurrence, the observed violations are given, deviations from the TOR are noted. If there are no remarks, it is determined that the software has passed acceptance tests, meets the requirements of the customer unit and is accepted for pilot operation)

_____

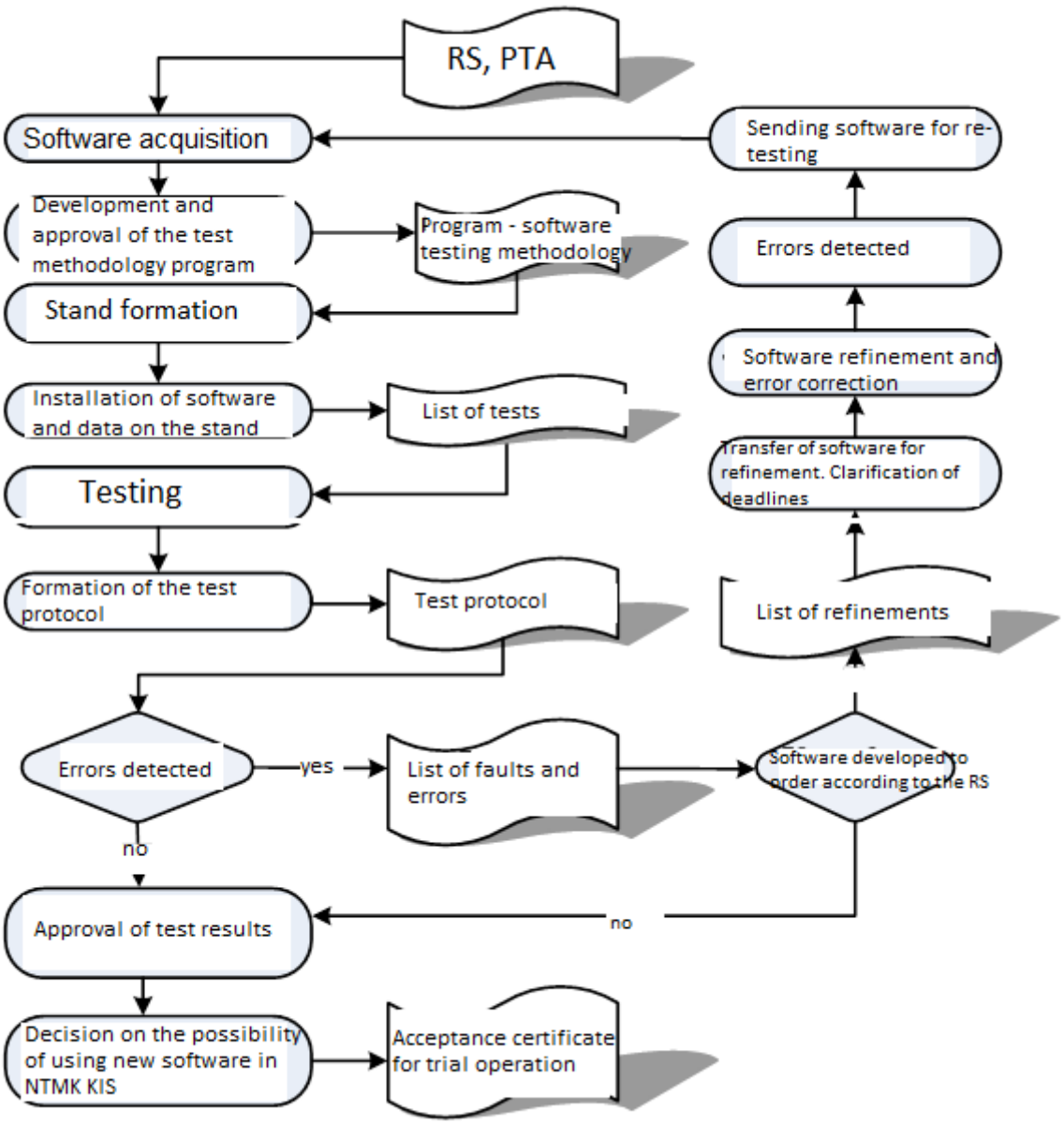
General Director of
ITD_____
«___» _____ 20__ year

Head of SS IS
_____
«___» _____ 20__ year

Head of SS IT
_____
«___» _____ 20__ year

Appendix 4
to the Security Policy for the Acquisition, Development, and Operation of Software and Hardware

Flowchart of new software analysis order



Appendix 5
to the Security Policy for the Acquisition, Development, and Operation of Software and Hardware

ACT
of putting the software into industrial operation

«___» _____ 20__ year No _____

This act is drawn up in the fact that the software_____
_____,

consisting of a set of tasks (task)_____
_____,

has passed acceptance tests and pilot operation, meets the requirements of the customer unit and is accepted for commercial operation.
Basis for performing work_____

The work to be submitted is presented in the form_____
(documentation name)

General Director of ITD
_____
«___» _____ 20__ year

Head of SS IB
_____
«___» _____ 20__ year

Head of SS IT
_____
«___» _____ 20__ year

Appendix 6
to the Security Policy for the Acquisition, Development, and Operation of Software and Hardware

Software Passport

Number_____

Name	Description
Software/module name	
Type	General/Special
Functional purpose	
Description of supplied software/module	
Developer/supplier	Name_____ Address_____ Contact information_____
Support form	None Hotline_____ Service Agreement No. Other _____
Number of licenses	_____
List of software documentation	Functional description User manual Description of technical architecture Installation instructions Description of databases Intermodule interaction diagram Administrator instructions Description of diagnostic messages Other documentation _____
Name of the department that purchased (ordered) the software	
Location of the storage location of the distribution and documentation	
Responsible for storage	
Date of software acceptance	
Responsible for maintenance	Full name_____ Contact information_____

back side of the Software Passport

Software and hardware requirements

Name	Description
Processor type	
RAM	
Disk space	

List of IS modules

with which the software interacts

Module name	Description of interaction

The head of the SS,
using the software _____
«___» _____ 20__ year

Employee responsible
for software maintenance _____
«___» _____ 20__ year

Employee responsible for storage of
distributions _____
«___» _____ 20__ year