Appendix
to the Order of Kazakhtelecom JSC
dated __ _____ 2023
No. _____

Policy of Anti-virus Protection of Kazakhtelecom JSC's Information Systems

Almaty, 2023

Contents

1 Terms, abbreviations and definitions

IS - information security. The state of protection of information resources and systems, which ensures their confidentiality, integrity, authenticity and availability, which is achieved by a whole set 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.);
RD means the Company's regulatory documents (policies, standards, orders, regulations, guidelines, instructions, etc.);
Company - Kazakhtelecom Joint Stock Company;
Software - software;
Policy - this Policy of antivirus protection of Kazakhtelecom JSC's information systems approved by the Company;
User - an employee of the Company or a representative of a third party using information received from its owner, proprietor or intermediary in accordance with the established rights and rules of access to information;
APM - anti-virus protection means;
Computer equipment(CE) means computer equipment (stationary computers or workstations, portable computers or laptops, etc.);
SS - structural subdivision of the Company;
SS TS - a structural subdivision of the Company or a third party that provides technical support for users and UAS in the Company;
TS - technical support;
Third party, third party - 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;
HTTP, HTTPS - Hyper Text Transfer Protocol, Hyper Text Transfer Protocol Secure ;
FTP - File Transfer Protocol;
IMAP - Internet Message Access Protocol - protocol for accessing e-mail;
OSI - The Open Systems Interconnection model;
POP3 - Post Office Protocol Version 3 - protocol used for receiving mail from a mail server by a client;
SMTP - Simple Mail Transfer Protocol - a protocol used to transfer e-mail between servers;
TCP/IP - Transmission Control Protocol/Internet Protocol - a network model of data transmission describing the method of data transmission from source to destination.

2 Purpose and scope of the Policy

1. This Policy defines a system of measures aimed at protecting the Company's IS and users' IT systems, including workstations, laptops, servers, etc., from IS threats, destructive impact of computer viruses and other malicious software (“Trojan” programs, logic bombs, etc.), as well as establishes uniform requirements for the organization of the anti-virus protection system for the Company's IS and all types of IT systems, requirements for the configuration of applied software tools and procedures for their operation.

2. Negative consequences may include the probability of virus infection of individual network nodes and/or virus epidemics, disclosure or loss of sensitive and confidential information, intellectual property theft, reputational consequences, as well as impact on important internal systems and business processes of the Company.

3. This Policy shall apply to all Company employees and others who are granted access to the Company's IS.

4. This Policy shall apply to all the Company's IS resources (server equipment, IT systems, other technological services and systems) connected to the Company's networks.

5. The Policy establishes the responsibility of all employees of the Company and other persons connecting to the Company's networks, using, operating and maintaining the Company's IS.

6. 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

7. In cases when it is impossible to install APM on the CE, server equipment (etc.), the use of such CE, server equipment (etc.) is possible only upon agreement with the IS SS.

3 General provisions and requirements of the Policy

8. The Policy is developed in accordance with the legislation of the Republic of Kazakhstan in the field of IS, RD of the regulator (regulatory and supervisory authorities), IS Policy of the Company, IS Concept of the Company, a series of international standards on IS ISO/IEC 27000, COBIT, ITIL, the 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.

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

10. 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), internal documents of the Company defining IS requirements;

2) detection of a decrease in the general and/or specific level of the Company's IS (based on the results of an internal or external audit);

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

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

11. 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.

12. Antivirus protection shall be achieved by:

1) operating the APM;

2) keeping virus signature databases (anti-virus databases) of the APM up to date on servers, workstations, IT systems and other technological services and systems;

3) regular updating of the APM software on servers, workstations, APM and other technological services and systems.

13. Malware control methods shall include three components:

1) prevention - actions to prevent malware infection;

2) detection - a methodology for determining the presence of malware;

3) removal - the physical removal of malware codes from infected files or an infected system.

14. APM are installed on servers, CE (workstations) and other technological services and systems or function as part of integrated defense systems (security gateways, etc.) and provide:

1) periodic verification of all information stored on any hard disks, data storage systems of technical means;

2) “real-time” verification of running programs, opened files, processes, etc..;

3) real-time inspection and control of network traffic.

15. The procedure for using the APM is determined by the provisions of the Policy, the operating documentation of a particular APM, anti-virus protection instructions and other RD.

16. Only authorized employees (administrators, technicians, etc.) of the relevant TS SS shall install the Company-authorized APM on users' CE.

17. The procedure for purchasing and installing APM:

1) only licensed APM are allowed for use in the Company's IS. Acquisition of APM and verification of their functionality shall be carried out in accordance with the Security Policy for the development, operation and acquisition of hardware and software and the technical requirements being developed;

2) installation and configuration of APM on servers, workstations, CE and other technological services and systems shall be performed only by authorized employees (administrators, technicians, etc.) of the Company's relevant SS responsible for maintenance (operation, support, servicing, etc.) of APM, CE, IS of the Company in accordance with manuals (instructions) for installation of purchased APM.

18. All APM shall comply with the requirements of this Policy and provide the following capabilities:

1) scanning of server equipment, CE and other technological services and systems according to a predetermined schedule;

2) scanning network traffic for viruses and other malware (at different OSI levels and at the level of different protocols HTTP(S), SMTP, FTP, POP3, IMAP, etc.);

3) Determining the types of network traffic to be inspected;

4) real-time monitoring of all running programs and opened files for viruses and other malware;

5) detection of viruses, Trojan horses and other malware;

6) blocking, removal of malware, treatment of infected files;

7) registration and signaling of attempts of virus infection of the Company's IS, introduction of malware, etc.;

8) automatic download of antivirus database updates from local antivirus software update servers or from antivirus software update servers on the Internet, controlled by the administrator of the antivirus protection system.

19. APM used for servers and CE shall be based on client-server technology. The server part shall provide the possibility of centralized management of the client parts of the APM, namely:

1) centralized setting of anti-virus protection policies (launching anti-virus tools, scanning, etc.);

2) centralized updating of virus signatures (antivirus databases).

20. APM that are a part of complex protection systems (security gateways, etc.) shall be operated and managed within the structure of the respective protection system, subject to the requirements of the provisions of this Policy.

21. Software and working files uploaded to the CE, servers and other data carriers shall be pre-checked by the APM.

22. All users of the Company's IS (including administrators, etc.) shall be prohibited from independently installing and using specialized software not officially approved (not authorized) for use in the Company without prior approval by the Company's IS SS.

23. Procedure for the use of APM on the CE:

1) APM shall be installed on all CE interacting with the Company's network and IS resources. It is allowed not to apply APM on the CE that do not have network connections to the Company's network and IS resources, information processing processes, etc.;

2) all users of the Company's IS (including administrators, technical specialists, etc.) are prohibited to create, upload to the Company's IS and distribute in the Company's IS any data knowingly containing viruses, malicious program code, etc.);

3) antivirus control of all disks and files of stationary CE should be performed in automatic mode when loading (starting) the CE at the beginning of each working day or during the period of inactivity of the user (least use of the CE);

4) antivirus control of all disks and files of mobile (wearable) CE should be performed in automatic mode at every CE booting (launching);

5) if it takes unacceptably long time to check all files on the CE disks, it is allowed to perform selective scanning of only the boot areas of disks, CE and operating system files, running processes. In this case, the full check should be carried out during the period of user inactivity (the least use of the CE);

6) launching of antivirus protection systems installed on the CE should be performed automatically according to the task (schedule) created centrally by the administrator of the Company's antivirus protection system using the task scheduler (included in the operating system or antivirus software delivery);

7) full anti-virus scanning of all disks of mobile computers shall be performed immediately before their connection to the Company's IS networks and resources;

8) all files received from external sources (in particular, by e-mail) or downloaded from removable media (flash drives, magnetic disks, tapes, CD-ROMs, etc.) shall be subject to mandatory antivirus control. The control of information must be carried out immediately after its download, until the moment of its use (launch), installed on the user's CE APM;

9) files placed in the electronic archive must be subject to mandatory anti-virus control;

10) The software installed (modified) on the servers must be previously checked by an authorized employee (administrator, technician, etc.) of SP TP for the absence of malware.

24. Control over compliance with the order of application of the CAZ is carried out by the administrator of the APM.

25. APM shall be applied on the following components of the Company's IS:

1) on file servers;

2) application and database servers;

3) on mail servers;

4) on web-servers;

5) at connection points to public access networks (Internet gateways, firewalls) and wireless networks.

26. The use of APM on the Company's IS servers used as file servers, application servers, web servers, etc. shall ensure:

1) antivirus scanning and treatment of files in “real time” mode, i.e. at the moment of an attempt to write or read a file, perform input/output operations on the server;

2) scanning of all directories and files on a schedule at least once a day (taking into account the load on the server).

27. The use of APM on the Company's IS servers used as mail servers shall ensure verification of all electronic mail messages received on these servers.

28. If the check of a message received from networks external to the Company's IS on a mail server shows the presence of a virus or other malware in the message, transmission of the message to the addressee (IS user) shall be blocked.

29. If the check of a message received from an IS user on the mail server shows the presence of a virus or other malware, the transmission of the message to the addressee (another IS user or an external person) shall be blocked. The responsible IS and IS SS IS administrators shall be automatically notified of the detection of viruses.

30. APM used at connection points to public access networks or wireless networks shall provide virus and other malware scanning of network traffic, incoming and outgoing with respect to the Company's IS networks and resources.

31. The data archiving procedure (storage/backup system to magnetic tape or other media, system) shall include a preliminary anti-virus control procedure.

32. Any software to be installed (modified) on the CE shall be taken from the approved register of the Company's trusted software from the official repository of the developer's website. At the same time, an updated (current) version of the APM must already be installed on the CE (server). After that, the responsible IS administrator (system administrator, application administrator, etc.) shall install this software.

33. Server system administrators and IS resource administrators of the Company shall constantly maintain the highest possible level of information security of the software and hardware entrusted to them. For this purpose it is necessary to:

1) monitor information coming from system and software developers about detected errors and vulnerabilities;

2) timely install updates and patches officially recommended by system and application software developers;

3) disable all unused services and applications of the operating system (or application software);

4) keep the installed APM up to date;

5) keep logs of system events and analyze them regularly;

6) follow the recommendations of the IS SS.

34. Actions when malware is detected on IS servers:

1) in case of detection of files, processes, applications, etc. on servers infected with a virus, malicious code or other malicious software, system administrators of servers and/or administrators of the Company's IS resources (if necessary, together with authorized employees of SS TS) shall:

- if necessary and in order to reduce the risk of network spread of viruses, disconnect the server from the Company's networks for a period until the viruses or other malware are completely destroyed and the relevant server equipment is restored to serviceability;
- treat and/or destroy the infected files, malicious code, processes, etc.;
- report the fact of malware detection to the direct management of the SP (subdivision, organization) and to the IS SS, specifying the date and time of the alleged infection, the alleged source (sender, owner, etc.) of the infected file, the type of the infected file, the nature of the information contained in the file, the type of the virus, the measures taken to neutralize the virus, etc.

35. It is forbidden to use program codes, software or algorithms that lead to the destruction, destruction of the IR during normal (regular) operation and exploitation of the Company's IS.

36. Users are forbidden to disable the APM installed on the CE and/or make changes to their configurations that may lower the established level of protection, etc.

37. Updating of virus signatures (anti-virus databases) of antivirus protection systems on servers, workstations, CE and other technological services and systems shall be performed locally from certain servers of the Company's anti-virus protection system, exceptions may be only in cases when it is not technically possible to fulfill these requirements and such cases are agreed with the IS.

38. Updating of virus signatures (anti-virus databases) of the Company's anti-virus protection system shall be performed from sources determined by the company producing (vendor) APM.

4.Roles and Responsibilities

39. Control over compliance with the requirements and rules of the Policy shall be vested in the IS SS.

40. Responsibility for keeping the Policy up-to-date, as well as for making amendments thereto, shall be vested in the IS SS.

41. Responsibility for ensuring compliance with the requirements of the Policy shall be vested in all IS SS within the scope of their authority and in accordance with the provisions set forth in the Policy and the documents developed on its basis.

42. Heads of the SS shall be responsible for timely communication of the Policy requirements to the employees of their subdivisions and/or third party representatives as they relate to them and for compliance by the employees of their subdivisions and/or third party representatives with the requirements of the Policy.

43. Implementation of the provisions of this Policy related to the maintenance of anti-virus software, updating of anti-virus databases on servers (including servers of the anti-virus protection system) shall be assigned to authorized and responsible administrators of the APM IS.

44. Implementation of the provisions of this Policy related to the maintenance of anti-virus software, updating of anti-virus databases on the Company's IT systems shall be assigned to the users and authorized employees of the second support line (user technical support staff) of the SS TS.

45. Implementation of the provisions of this Policy related to responding to user reports on detection of viruses or other malware shall be assigned to the authorized employees of the first support line (Help Desk) of SS TS and, if necessary, to the authorized employees of the second support line (user technical support staff) of SS TS.

46. Organizational and methodological support of the anti-virus protection process shall be the responsibility of the IS.

47. Periodic control of compliance of the Company's IS users with the requirements of this Policy shall be the responsibility of the IS SS within the framework of IS audits.

48. Third parties interacting with and using the Company's network and IS resources as part of the fulfillment of their obligations under existing agreements and contracts shall be liable for the application, use or distribution of malware with respect to the Company's network and IS resources in accordance with the applicable laws of the Republic of Kazakhstan.

49. In case of detection of violations of the requirements of this Policy by an IS user, including any deliberate action taken to violate, block or otherwise circumvent the established IS controls, which have caused or may have caused serious damage to the Company's business activities, an internal investigation by the IS SS shall be initiated and conducted.

50. Failure to comply with the measures stipulated by this Policy shall entail liability in accordance with the applicable laws of the Republic of Kazakhstan and internal documents of the Company.