APPROVED
Director of the State Enterprise
"Kostanay Polytechnic Higher College"
of the Education Department
of the Akimat of Kostanay Region
_____________ Katkenov K.A.
"_1_"_november_____ 2024

Information Security Policy MSOE "Kostanay Polytechnic Higher College" of the Education Department of the Akimat of Kostanay Region

on 12 sheets

DEVELOPED BY
Deputy Director for IT
Khramey I.S.
MSOE "Kostanay Polytechnic
Higher College" of the Education
Department of the Akimat of Kostanay Region
"_1_"_november_____ 2024

Kostanay, 2024

1. Rules for the Use of the Internet and E-mail

Terms and Definitions

The following basic concepts and terms are used in these Rules:

1) Electronic information resources - information stored in electronic form (information databases) contained in information systems;

2) Information system (hereinafter referred to as IS) - a system designed to store, process, search, distribute, transmit and provide information using a hardware and software complex.

3) Internet resource - an electronic information resource, the technology for its maintenance and (or) use, functioning in an open information and communication network, as well as an organizational structure that ensures information interaction;

4) Internet provider - an organization providing Internet access services and other services related to the Internet service;

5) Workstation - a set of hardware and software designed to solve a certain range of problems;

6) Confidential information - information that does not contain state secrets, access to which is restricted in accordance with the laws of the Republic of Kazakhstan or their owner, or the owner in cases stipulated by the legislation of the Republic of Kazakhstan;

7) Email monitoring - tracking electronic messages (where, where from, message size) in order to prevent spam, the presence of malicious code that can be transmitted using electronic means of communication and protection against it;

8) Monitoring of Internet resources - identifying the topics of sites visited by users, identifying the location of access to the Internet, while only viewing the name of the Internet resource (website address) is carried out in order to block malicious sites;

9) Monitoring of the information system - used to check the effectiveness of the adopted control tools and check compliance with the access policy model;

10) Email distribution - a means of mass communication, group communication and advertising;

11) IT specialists - responsible for ensuring the development and troubleshooting of complex malfunctions in the college's information systems, as well as technical support of information resources and systems.

Purpose of the document

1. These Rules for the Use of Email and Internet Services on College Workstations regulate the rules for working with email and the Internet service.

2. The effectiveness of Internet access management, compliance with the requirements for organizing information security in the use of Internet resources is controlled by the structural unit for ensuring information security.
3. The hardware and software for organizing access to the Internet and the email system belongs to the college. All messages, materials created, transmitted or received using the email system and the Internet, as well as other information resources of the college, are and remain the property of the college and cannot be the personal property of any employee.
4. All persons are prohibited from unauthorized viewing of messages and user information.
5. The use of information resources by an employee means his consent to the terms of provision of these resources.
6. The content of the information may be brought to the attention of authorized persons by decision of the college management.
7. IT specialists responsible for the information security of the college have the right to block malicious Internet resources.
8. Access to external Internet mail resources is prohibited.

Ensuring information security

1. When using e-mail and Internet services, it is prohibited to:
1) use resources for campaigning or advertising commercial enterprises, propaganda of religious or political ideas, or other purposes not related to the performance of official duties;
2) create offensive or provocative messages. These are messages containing sexual harassment, racial insults, gender discrimination, or other comments that touch on issues of age or sexual orientation, religious or political preferences, nationality, or health status in an offensive manner, as well as other information prohibited by the legislation of the Republic of Kazakhstan;
3) use attachments of graphic, video, executable, etc. files that are not related to official activities, as well as files whose size exceeds the established one;
4) request to send messages containing information constituting official and/or confidential information with limited access and/or distribution in open (unencrypted using state encryption tools - cryptographic information protection tools (CIPF) form, as well as using foreign mail servers;
5) use group mailing for personal purposes;
6) use resources for sending pyramid letters, chain letters, advertising messages and other similar information not related to official activities;
7) distribute malicious files and programs, as well as software and materials protected by copyright;
8) use accounts of other mail systems and users; gain access to electronic messages of other users (except in cases authorized by the college management;

When using the Internet, it is prohibited to:

1) use the Internet for the purpose of transmitting and distributing materials containing confidential information with limited access and/or distribution in the open (unencrypted using state encryption tools - cryptographic information protection tools (CIPF);
2) visit websites containing materials of a terrorist, extremist, unconstitutional and other destructive nature;
3) visit questionable and malicious sites, as well as sites whose information is not related to the performance of functional duties;
4) download (transmit) malicious files and programs, software and materials protected by copyright, as well as multimedia files of all types;
5) use Internet chat services;
6) install programs for work via remote access with Internet access on workstations;
7) connect college computers to the Internet through third-party Internet providers, as well as use an unauthorized modem connection.

Rules for organizing the authentication procedure

General Provisions

These Rules for organizing the authentication procedure (hereinafter referred to as the Rules) define the requirements for registering user accounts and password protection of information systems and are intended to minimize damage from the implementation of information security threats, as well as to increase the overall level of confidentiality, integrity and availability of information in the college IS.

1. The terms used in this document have the following definitions:

1) information security (hereinafter referred to as IS) is a set of legal, technical and organizational measures aimed at ensuring the protection of information resources from unauthorized access, intentional or accidental distortion and destruction, physical destruction, including as a result of man-made and natural impacts, as well as the state of security of state information resources and systems, ensuring the confidentiality, integrity and availability of information;

2) information system (hereinafter referred to as IS) is an organizationally ordered set of information and communication technologies, service personnel and technical documentation that implements certain technological actions through information interaction and is designed to solve specific functional problems.

3) System administrator - a specialist responsible for the administration, maintenance and smooth functioning of the entire college information system;

4) College information system users - employees working with the college information system;

5) Information confidentiality - ensuring that information is provided only to authorized persons;

6) Information integrity - a state of information (resources of an automated information system) in which it (their) change is carried out only intentionally by entities entitled to it;

7) Authentication - confirmation of the authenticity of the subject or object of access by determining whether the presented access details correspond to those implemented in the system;

8) Primary password - a combination of characters (letters, numbers, special characters) set by the OS, DBMS, software administrator when creating a new account;

9) Main password - a combination of characters (letters, numbers, special characters) known only to the system administrator, used to confirm the authenticity of the account owner;

10) Account information about the user: user name, password, access rights to resources and privileges when working in the college information system.

Requirements for administrators and users of the college IS

Administrators and users of the college IS are required to:

1) Remember their password and not save it or transfer it to other people in any form;

2) Be registered in the college domain service.

3) In case of loss or compromise of the password, immediately notify the immediate management of this fact and change the password;

4) It is necessary to change the password at least once a month;

5) When changing the password, comply with the requirements according to Appendix 1;

6) When entering the password, exclude the possibility of it being spied on by third parties (a person behind your back, a person observing the movement of fingers in direct visibility or in reflected light, etc.) and technical means (stationary and built-in video cameras in mobile phones, etc.);

7) Ensure the confidentiality and security of the login and password.

Administrators and users of the college IS do not have the right to:

1) Work under someone else's account. If the head of the college IS user suggests that the college IS user work under such conditions, the college IS user has the right to demand a written instruction (order) from the head and not to start work until receiving such an instruction (order);

2) Connect computing equipment to the college corporate network without registering it with the college domain service.

3) Share a personal password with anyone;

4) Write passwords on paper, in a file, electronic notebook or other information carriers, including on objects;

5) Include passwords in automatic login scripts, for example, in macros or function keys.

Requirements for registration elements and passwords

1. To work in the college IS, you must have a user account for the college IS (login and password).

2. When creating a new account, the system administrator creates it with a primary password and notifies the user of the temporary password by e-mail. When logging into the system for the first time, the user must change the temporary password. When choosing a password, you must be guided by the "Password Requirements" (Appendix 1).

3. The owner is personally responsible for maintaining the secrecy of the main password. It is prohibited to disclose the password to other people, including college employees, write it down, or send it in plain text in e-mail messages.

4. The password should never be stored in the computer system in an unprotected form. The owner should avoid making notes (e.g. on paper, in files, software, or a portable device) of passwords without a guarantee of their secure storage and approval of the storage method.

5. Control over blocking of accounts is carried out by the person responsible for the administration of the college's IS, in accordance with the records of the account registration log.

6. The employee responsible for the system and technical maintenance of computers, as well as other office equipment on the college's neutral device, must ensure mandatory registration of all college users in the college's domain service in accordance with the established rules of the college's domain.

7. The policy of the college's domain service is regulated by the employee responsible for ensuring the information security of the college.

Password change procedure

1. The user/system administrator must change the main password at least once a month in accordance with the Appendix.

2. The main password can only be created by the user/IS administrator

3. The college prohibits the generation of passwords by computer programs and third parties.

4. An unscheduled change of the main password by the user/system administrator can be made at any time at the request of the responsible persons at the IS.

Password Management in the College IS

1. Passwords are the primary means of confirming user access authority to the College IS. The College IS must provide an effective interactive means of ensuring secure passwords (Appendix 1).

2. The following functionality must be implemented in the Password Management in the IS:

1) Requirement to change the primary password upon first login to the system;

2) Selection and change of passwords with a procedure for confirming them to eliminate typing errors (if necessary);

3) Password strength checks in accordance with Appendix 1;

4) Mandatory change of passwords at specified intervals,

5) Exclusion of the use of the last three passwords;

6) Exclusion of the possibility of using a password that differs from the previous three last passwords in less than 4 positions;
7) Store passwords in encrypted form;
8) Do not display passwords on the screen when they are typed on the keyboard;

Responsibility

1. In case of violation of the requirements of this provision of the Rules, the system administrator is subject to administrative or other liability in accordance with the current legislation of the Republic of Kazakhstan.
2. For disclosure of password information that constitutes an official secret, the employee is subject to disciplinary liability in accordance with the current legislation of the Republic of Kazakhstan and internal regulations.

1. Rules for organizing anti-virus control

General provisions

These rules are intended to organize the procedure for conducting anti-virus control and preventing the occurrence of cases of infection of software and information systems with computer viruses.

The rules regulate the actions of users when organizing anti-virus protection of the college's electronic technologies.

Installation and updating of anti-virus software
1. Only licensed anti-virus software is allowed for use in the college.
2. Installation and updating of anti-virus software is carried out by the department that carries out contractual maintenance of information systems.

Procedure for conducting anti-virus monitoring

1. Installation (change) of system and application software of computers and local area networks is carried out only in the presence of a specialist.
2. The software installed (changed) on the computer is checked for computer viruses. Immediately after installation (change) of the computer software, an anti-virus scan is performed by an employee of the Service Organization (hereinafter referred to as the SO) who installed the software.
3. Any information (test files of any format, data files, executable files) received and transmitted via telecommunication channels, as well as information from removable media (magnetic disks, tapes: CD-ROM, FlashUSB, etc.) received from third parties and organizations, is subject to mandatory anti-virus monitoring.
4. The User monitors the intended use of the automated workstation, as well as all its external devices.
5. All software installed on protected computers is pre-checked for malware. Information on removable media is checked immediately before its use.

6. A full scan of all files stored on the hard drives of the protected computer is performed at least once a month.

7. An extraordinary anti-virus scan of all disks and files of the protected computer is performed:

- immediately after installing or changing the software;
- after connecting a stand-alone computer to the local network;
- if there is a suspicion of the presence of malicious programs (atypical operation of programs, the appearance of graphic and sound effects, data corruption, loss of files, frequent messages about system errors, etc.).

8. In doubtful cases, to determine the presence or absence of malicious programs, it is necessary to involve technical support specialists in the check.

9. Users are prohibited from installing unlicensed software on workstations, independently making changes to configuration settings, as well as disabling or removing anti-virus programs.

Actions of employees upon detection of a computer virus

1. If there is a suspicion of the presence of a computer virus, a college employee conducts an extraordinary anti-virus check or, if necessary, involves an IT specialist to determine the presence or absence of a computer virus.

2. If a computer virus is detected, a college employee is obliged to suspend work and notify employees performing technical maintenance of the fact of detection of files infected with a virus;

Control during the organization of anti-virus protection

1. Control over the organization of anti-virus protection in the college and the establishment of the procedure for its behavior is assigned to employees ensuring information security (administration of the anti-virus protection system, adaptive security system, etc.).

2. Periodic monitoring of compliance with the provisions of this instruction is assigned to the Deputy Director for ICT.

Organization of anti-virus protection

1. The user is obliged to regularly check the anti-virus database.

2. In the absence of an anti-virus program, immediately inform the employees responsible for information security.

4 Instructions on the procedure for users to respond to information security incidents and in emergency (crisis) situations

General provisions and basic concepts

This Instruction on the procedure for users to respond to information security incidents and in emergency (crisis) situations defines the main measures, methods and means of preserving (maintaining) the operability of information systems (hereinafter ICS) in the event of various crisis situations, as well as the methods and means of restoring information and its processing processes in the event of a malfunction of the IS and its main components. In addition, it describes the actions of various categories of system personnel in crisis situations to eliminate their consequences and minimize the damage caused.

1. A situation arising as a result of an undesirable impact on the IS, leading to a threat to information security, is called a crisis. A crisis situation may arise as a result of intentional actions of an intruder or unintentional actions of users, accidents, natural disasters.

2. According to the severity and extent of damage caused, crisis situations are divided into the following categories:

1) threatening - leading to the complete failure of the information system and its inability to continue to perform its functions, as well as to the destruction, blocking, illegal modification or compromise of the most important information.

3. Threatening crisis situations include:

1) power outage in the building;

2) failure of the workstation responsible for file exchange (with loss of information);

3) failure of the workstation responsible for file exchange (without loss of information),

4) partial loss of information on the workstation responsible for file exchange, without loss of its operability;

5) failure of the local network (physical data transmission medium);

6) serious - leading to the failure of individual system components (partial loss of operability), loss of productivity, as well as to a violation of the integrity and confidentiality of programs and data as a result of unauthorized access.

4. Serious crisis situations include:

1) workstation failure (with loss of information);

2) workstation failure (without loss of information);

3) partial loss of information on the workstation without loss of its functionality;

4) natural disasters (fire, flood, hurricane, etc.).

5. A detailed description of the procedure for users in emergency (crisis) situations is in Appendix 1 to this Security Policy.

6. Sources of Information on the occurrence of a crisis situation:

1) users who have detected suspicious changes in the operation or configuration of the system, or its protection means in their area of responsibility;

2) protection means that have detected a crisis situation;

3) system logs that contain records indicating the occurrence or possibility of a crisis situation.

General requirements

1. All users whose work is disrupted as a result of a threatening or serious crisis situation are immediately notified by e-mail by the IS administrators. Further actions to eliminate the causes of the disruption of the IS, resume processing and restore damaged (lost) resources are determined by the functional responsibilities of the personnel and users of the system.

2. Each crisis situation is analyzed by the IO. Based on the results of this analysis, proposals are developed to change user powers, access attributes to resources, create additional reserves for changing the system configuration or security settings, etc., if necessary, an investigation is carried out into the causes of its occurrence, an assessment of the causal damage, identification of those responsible and the adoption of appropriate measures.

3. A serious and threatening crisis situation requires prompt replacement and repair of failed equipment, as well as restoration of damaged programs and data sets from backup copies.

4. Prompt recovery of programs (using reference copies) and data (using backup copies) in the event of their destruction or damage due to a serious or threatening crisis situation is ensured by backup (backup) copying and external (in relation to the main components of the system) storage of copies. External storage implies that copies are located in dedicated storage facilities (safes) located in specially designated rooms.

5. All programs and data that ensure the operability and execution of system tasks (system and application software, open data and other data sets), as well as archives, transaction logs, system logs, etc. are subject to backup copying.

6. All software used in the system have reference (distribution) copies.

7. The necessary actions of personnel to create, store and use backup copies of programs and data are reflected in the functional responsibilities of the relevant categories of personnel, as a rule, these are System Administrators, Administrators of automated workstations, OI employees, and are also recorded in the register.

8. Duties and actions of personnel to ensure continuous operation and recovery of information systems.

9. The actions of personnel in a crisis situation depend on its severity.

10. In the event of a threatening or serious critical situation, the actions of personnel include the following stages:

1) immediate response of responsible personnel;

11. In crisis (emergency) situations, users are immediately notified via internal e-mail, verbally by telephone or by electronic means of communication by employees of the Service Organization (hereinafter - SO), IO.

12. During the daytime, a user who has discovered an emergency (crisis) situation notifies the employees of the OO, SA in terms of technical support of information resources and systems.

13. At night, if an emergency situation occurs, the user who has discovered it must notify the IO employee, and the following are urgently notified by telephone: the responsible heads of structural divisions for this area of work, the management of the IO. The event must be registered in the log, indicating the exact time of the incident, a brief description of the

events, indicating the full names of the notified heads of structural divisions, and a description of the actions aimed at eliminating the crisis situation.

1) partial restoration of operability and resumption of processing;

2) full restoration of the system and resumption of processing in full;

3) investigation of the causes of the crisis situation and identification of those responsible;

4) development of solutions to eliminate the causes and prevent similar violations in the future.

14. Control over the organization of work in crisis situations is carried out by the IO.

Use of remote access

Prohibit installation of programs for work via remote access on workstations with Internet access.

Use of flash cards

Due to official necessity, allow the use of flash cards (E-token, KAZ-token, Save-Token, USB-drives) in computers intended for accounting staff, administrative staff, teachers, social workers.

Appendix 1
to the Rules of the Organization
of the Authentication Procedure

Password Requirements

1) The password must contain at least 8 characters;
2) The password must contain uppercase and lowercase letters, as well as numbers;
3) The password must not include easily calculated sequences of characters, such as commonly accepted abbreviations (e.g. admin, system, user, sys, god), as well as personal and other publicly available entries (e.g. dates, names, titles);
4) The password must not include groups of characters, the sequence of which on the keyboard is easily calculated (e.g. !234, qWErty, qwerty123, 321369);