Approved by
Chairman of the Management Board – Rector of NPJSC «Abylkas Saginov Karaganda Technical University»
_____ S.S. Sagintayeva
Board decision
No. 13 11 2025

INTERNAL REGULATORY DOCUMENT

INFORMATION POLICY SECURITY

IRD II-03-2025

Developed by: Information security engineer
_____ D.K. Chityan

Karaganda 2025

Contents

1 Scope

1.1 The Information Security Policy (hereinafter referred to as the Policy) of Abylkas Saginov Karaganda Technical University NJSC (hereinafter referred to as the University) has been developed in accordance with the requirements of the current legislation, regulatory legal acts of the Republic of Kazakhstan and the other internal regulations of the University.

1.2 This document expresses the University approach to ensuring information security within the framework of its activities. Information assets are protected within a strictly defined scope of the Information Security Management System (hereinafter referred to as the ISMS).

1.3 The provisions of this Policy apply to all the digital information resources and systems of the University used for processing, storing, transmitting and protecting information. Compliance with this Policy is mandatory for all the users of the University digital resources, including employees (full-time, temporary, part-time, under a contract, etc.), interns, trainees, as well as the third parties (contractors, auITDors, etc.) who have access to the University information systems and data.

1.4 The provisions of the Policy are also communicated to clients and the other third parties related to the University information systems and documents, to the extent necessary in the context of their interaction with the University.

1.5 Familiarization with this Policy is mandatory for each employee upon hiring.

1.6 The process of ensuring information security is considered continuous, requiring constant adjustment of protection parameters and adaptation to new threats arising from both the external and internal environment.

1.7 There should be no obstacles to the timely introduction of changes to this Policy, as well as to the other procedures and documents on information security, as the need arises.

1.8 The provisions of this Policy are applied in internal regulatory and methodological documents, and are also taken into account when concluding agreements with counterparties. The Policy is an internal regulatory document of the University.

2 Regulatory references

The following regulatory legal acts and standards in the field of information security were used in developing this Policy:

- Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V "On Informatization";
- Resolution of the Government of the Republic of Kazakhstan No. 832 dated December 20, 2016 "On approval of uniform requirements in the field of information and communication technologies and ensuring information security";

- Law of the Republic of Kazakhstan dated July 5, 2004 No. 567-II "On Communications";
- Law of the Republic of Kazakhstan dated November 16, 2015 No. 401-V "On Access to Information";
- RK ST ISO/IEC 27001-2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements";
- RK ST ISO/IEC 27002-2023 "Information security, cybersecurity and privacy protection. Information security management tools";
- State Standard of the Republic of Kazakhstan dated December 24, 2007 No. 691 RK ST 1699-2007. "Access control and management systems";
- State Standard of the Republic of Kazakhstan RK ST 34.005-2002 "Information technology. Basic terms and definitions";
- Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V "On personal data and their protection".

3 Terms, definitions, and abbreviations

1) Superuser – IS administrator with full rights to perform any operations;
2) ITD – information technology department;
3) rules – mandatory conditions for performing actions in the system;
4) unauthorized action – violation of established rules for processing information;
5) user – an entity using information within the established access rights;
6) local area network (LAN) – a group of nodes connected for data transmission;
7) information system (IS) – a set of ICT, personnel and documentation for solving functional problems;
8) information security (IS) – protection of IS and data from threats;
9) IS incident – a failure or violation that creates a threat to the operation of IS or data;
10) confidential information – information with limited access by law;
11) electronic information resources - information in digital form on electronic media or in an information system;
12) software - a set of programs and codes with documentation;
13) computer equipment - software and hardware elements of data processing;
14) utility - an auxiliary program for working with OS and equipment;
15) DBMS (database management system) - software designed to create, store, modify and manage databases, as well as to provide access to data in compliance with specified rules and restrictions. DBMS ensures the integrity, security, consistency and recovery of data during various operations.
16) OS (operating system) - software for managing computer resources;
17) PD (personal data) - information related to the subject of personal data;
18) ISPD (PD information system) - a system for processing personal data.

4 Responsibility and authority

4.1 This Policy is approved by Chairman of the Management Board, Rector of the University based on the decision of the Management Board.

4.2 The University Management:

- assumes responsibility for maintaining the required level of information security (IS) in general;
- provides IS activities with all the required resources (financial, personnel, technical);
- defines the criteria for assessing and accepting IS risks and regularly reviews them.

4.3 The responsible IS employee:

- coordinates the development, implementation, support and updating of this Policy and related regulations;
- organizes monitoring compliance with IS requirements, prepares a report on the functioning of the ISMS for senior management;
- initiates an internal investigation of IS incidents and makes proposals for adjusting processes.

4.4 Heads of structural divisions should:

- promptly communicate to employees the requirements of internal IS documents;
- allocate information assets belonging to their departments, coordinate requests for access to them;
- ensure that employees of departments comply with the requirements of the Policy and other acts on information security;
- immediately inform the person responsible for information security of all incidents or suspicions of violation of information security requirements.

4.5 Employees and the faculty of the University:

- are personally responsible for compliance with information security requirements within the scope of their job responsibilities and when working with protected information assets;
- are responsible for violations of this Policy and documents developed on its basis in accordance with internal regulations and the legislation of the Republic of Kazakhstan;
- disciplinary, administrative or the other liability measures are applied by senior management based on the results of an official investigation, taking into account the nature and intent of the violation.

5 General provisions

5.1 Purposes and objectives

5.1.1 The purpose of the University information security is to protect information assets from threats, including malicious actions, accidents, personnel errors and technical failures, as well as to ensure the smooth operation of technological processes.

5.1.2 The information security direction was created in the information technology department, and its tasks and functions are performed by the person responsible for information security:

- development and updating of regulatory documents on information security;
- protection of confidential information and personal data;
- threat assessment and organization of technical protection measures;
- control over the state of information security, identification and elimination of vulnerabilities;
- conducting scheduled inspections and investigating incidents;
- interaction with departments processing personal data;
- training employees in information security issues;
- ensuring preparedness for incidents and prompt response to them.

5.2 Organizational and legal status of information security employees

5.2.1 Information security employees have the right to access premises with information systems and can demand that the data processing be stopped in the event of threats;

5.2.2 They have the right to receive the necessary information from users and administrators on the issues of using information technologies, in terms of information security;

5.2.3 Employees responsible for information security have the right to audit both existing and implemented information systems and software to verify compliance with the requirements for the protection and processing of information. If non-compliance with legal requirements is detected or there is a risk of significant security threats being realized, these employees have the right to suspend or prohibit the operation of the specified information systems and software until the violations are eliminated.

5.2.4 Information security employees are required to regularly undergo certification for compliance with information security standards and confirm their competencies in this area.

5.3 Principles of the Information Security Policy

5.3.1 The University information security policy is based on the following principles:

1) Ensuring information security by maintaining confidentiality, integrity and availability of information;

2) Confidentiality: providing access to information only to authorized persons (an authorized person is a website visitor who has registered and logged in under their account);

3) Integrity: making changes to publicly available electronic information resources (personal computers, corporate e-mail, Directum, etc.) only by authorized persons;

4) Availability: providing authorized users with access to electronic resources (PC, e-mail, Directum, etc.) to perform their official duties.

6 Measures to implement the Policy

6.1 At the University, information security measures are divided into:

1) legal: legislative and regulatory acts;

2) organizational: administrative procedures and regulations;

3) physical: protective structures and technical means;

4) technical: hardware and software protection methods.

6.2 Legal protection measures include regulatory legal acts governing the use of information, defining the rights and obligations of employees when processing it and ensuring liability for violating established requirements. These measures are aimed at preventing incidents and require regular informing of users and external contractors working with university information systems.

6.3 Organizational (administrative) protection measures establish rules for the operation of information systems, regulate user access, determine the work procedure of external contractors and prevent potential threats to information security. These measures minimize possible risks and losses in the event of incidents.

6.4 Physical security measures include the use of mechanical and electronic-mechanical devices designed to limit unauthorized access to the university's critical infrastructure. They include video surveillance systems, security alarms, access control, and other engineering and technical security measures.

6.5 Technical (hardware and software) security measures are implemented using specialized equipment and software built into the university's information systems. These measures ensure user identification and authentication, access rights delimitation, event registration, cryptographic data protection, and the other functions aimed at increasing the security level of the University information environment.

7 General requirements to confidentiality

7.1 The main requirements for ensuring the confidentiality of information at the University are preventing its leakage (disclosure) and ensuring access to it only for authorized persons.

7.2 All the user actions in the University information systems are subject to mandatory logging: the information about actions is recorded by administrators in text log files, stored on the University servers for at least three years and is available for operational access for at least two months.

8 Procedure for user access to the information systems

8.1. Access control to information systems is performed using standard OS tools (Windows Server, Linux) and DBMS, providing identification, authentication and registration of user actions.

8.2. The University uses certified or permitted means of protection against unauthorized access, including access control, registration, anti-virus protection, firewall, security analysis and intrusion detection subsystems.

8.3. All the user actions are recorded in system logs, which only the administrator has access to. He is responsible for the completeness of the records and provides them to the person responsible for information security upon request.

8.4. Administrative access is granted by a memo with mandatory approval from the information security engineer. The use of shared or pre-defined accounts is prohibited. Elevation of access rights also requires approval.

8.5. Access to databases without registration in logs is prohibited. When superusers are dismissed, passwords are changed on the day of dismissal.

8.6. Changes to information systems are made taking into account security requirements, including planning, testing, implementation and subsequent monitoring. All the nchanges must comply with the Information Security Policy and be reviewed if necessary.

9 Network security

9.1 Access from the Internet to the University internal network

9.1.1 Access to the internal network is provided exclusively through a configured firewall.

9.1.2 Access from outside the network perimeter is permitted only by order of the Director of the Information Technology Department with the approval of the person responsible for information security, on a specific port and for a specific time.

9.1.3 Remote access to the local network using depersonalized, group and anonymous accounts is prohibited.

9.1.4 The following requirements are imposed when administering remote access to the University's corporate network resources:

- remote user access is provided exclusively on the basis of registered personal accounts, using VPN technology or the other encryption protocols.

9.2 Prohibitions and restrictions

9.2.1 To ensure security and stable functioning of the University's computer networks, it is prohibited to:

1) connect unauthorizedly any computer equipment (including wireless access points, routers, network printers, IP cameras, media players, personal laptops, etc.) to the University's local network without prior approval from the IT Department and the person responsible for information security;

2) move workstations, computers and the other network equipment between network sockets, VLANs or the other communication interfaces without approval from the IT Department. Use the University information resources (including the Internet) for:

- participating in network/online games;
- sending commercial, intrusive or unwanted advertising (including SPAM);
- storing or distributing malware, illegal content prohibited by law;

2) perform network scanning, intercepting traffic, attempting to bypass security measures (e.g. firewalls, proxy servers), as well as any actions related to the analysis of the network infrastructure, unless this is the employee's responsibility and has been agreed upon with the of Information Technology and Information Security Department;

3) use software or devices to create VPN tunnels, proxy connections or other channels to bypass filtering and traffic control systems without permission;

4) install and use unauthorizedly network services, such as DHCP, DNS, FTP, web servers and the other services that can affect the operation of the network infrastructure or violate information security requirements;

5) change network adapter settings, IP addressing, gateway settings, DNS and the other network parameters on work devices without the appropriate authority or instructions from the IT Department.

9.3 Acquisition of protection tools

9.3.1 The acquisition, implementation and operation of information security tools and systems at the University are carried out only with the consent of the person responsible for information security and the Information Technology Department (ITD) and the University management. This is necessary to ensure compatibility with the existing IT infrastructure, the effectiveness of application and compliance with the requirements of regulatory legal acts of the Republic of Kazakhstan in the field of information security.

9.3.2 When selecting information security tools, priority is given to solutions that have certificates of conformity or positive conclusions on applicability issued by authorized government agencies. The use of uncertified or unregistered tools in accordance with the established procedure is permitted only if there is justification and after receiving written consent from the person responsible for information security.

9.3.3 All the acquired information security tools must be accompanied by technical documentation, licenses, as well as contracts for technical support and updates, if this is required for the correct functioning and relevance of the security mechanisms.

10 Local security

10.1 Anti-virus protection

10.1.1 Anti-virus protection is designed to ensure protection of servers and workstations of the University users from malicious software.

10.1.2 On each computer or server put into operation, as well as after reinstalling the operating system, the ITD employees must install and activate an anti-virus program.

10.1.3 Disabling anti-virus protection or unauthorized disabling of anti-virus database updates is prohibited. Control over the installation and updating of anti-virus software is carried out centrally by the ITD employees.

10.1.4 In the event of a massive virus attack, the ITD employees determine the scale of the infection, localize the threat, block its spread and, together with the information security engineer, identify the source of the infection, the nature of the action and spread of the virus, and eliminate the consequences. If necessary, patches and software updates are installed to eliminate vulnerabilities.

10.2 Distinction of access rights to information systems and data storage systems, protection against unauthorized access

10.2.1 Access to the University information systems is provided only by registered logins and passwords.

10.2.2 When providing access to operating systems and applications, the principle of minimizing privileges is implemented.

10.2.3 Organizationally and technically, the University divisions are divided by access level and type of processed information. This is implemented by means of the relevant IS, where user rights are limited in accordance with roles.

10.2.4 The IS administrator maintains an access log, records unauthorized access attempts (UAA) and informs the information security engineer of this.

10.2.5 Using the accounts of dismissed employees is strictly prohibited.

10.3 Use of e-mail, the Internet

10.3.1 It is prohibited to distribute materials prohibited or restricted by the legislation of the Republic of Kazakhstan.

10.3.2 Transfer of confidential information is allowed only through corporate e-mail.

10.3.3 E-mail at employees' workplaces is used exclusively for official correspondence.

10.3.4 The login and password for corporate e-mail to employees and students are issued by the ITD employees on the basis of a memo addressed to the Director of the ITD.

10.3.5 It is prohibited to open letters with suspicious attachments and from unknown senders. In such cases, it is necessary to immediately notify the information security engineer.

10.3.6 It is prohibited to publish confidential information on social networks and transfer it via instant messengers (WhatsApp, Telegram, etc.).

10.3.7 At workplaces intended for processing confidential information, the use of cloud data storage systems whose physical servers are located outside the Republic of Kazakhstan is prohibited.

11 Password policy

11.1 All the users who have their own password, keep it secret, remember it or record it in a place inaccessible to unauthorized persons.

11.2 Organizational and technical support for the processes of using, changing and terminating user passwords is assigned to the administration of the ITD employees.

11.3 Requirements for compliance with the Password policy apply to all users, including administrators (network, servers, information systems), without exception. All procedures for creating, changing and blocking passwords must comply with the established rules.

11.4 When entering a password, the user must ensure that it is not visible to unauthorized persons (for example, a person behind his back, a person observing the movement of fingers in direct line of sight or in reflected light) and technical means (stationary and built-in video cameras in mobile phones, etc.).

11.5 The user shall change the password independently in the following cases:

1) upon first authorization, when it is necessary to change the temporary password issued by the administrator;

2) upon expiration of the password;

3) when independently deciding to change the password.

11.6 If a password is compromised, the procedure for changing the user's password is carried out on the basis of a memo from the head of the structural unit where the user works (worked). The memo with justification of the reason for changing the password must be sent to the ITD, with subsequent approval from the responsible information security employee, who forwards the memo to the ITD employee for execution.

11.7 Blocking of user accounts of users who have been dismissed or quit, transferred to another structural unit, completed training, or expelled, is carried out by ITD employees upon signing the bypass sheet.

12 Physical security

12.1 Organization of the security zone

12.1.1 Critical and sensitive assets associated with information processing facilities are located in specially designated security zones. These zones are limited by a guarded perimeter and equipped with physical barriers and access control.

12.1.2 In order to protect information systems:

- the photo, video, audio equipment, as well as digital cameras of mobile devices can be used only with special permission;
- visitors enter the security zones accompanied by authorized University employees, subject to clearance, with mandatory registration of the date and time of the visit;

- access to important information and the equipment that processes it is controlled and provided only to those included in the approved list of employees admitted to the security zones;

- employees and external personnel must have means of visual identification; third parties are admitted only when accompanied by representatives of the University;

- access rights of employees and third-party personnel are regularly reviewed and updated;

12.1.3 Technical work in security zones is carried out according to internal regulations and instructions that determine the rules for being and performing tasks in these zones. Maintenance of critical equipment is permitted only by certified personnel.

12.2 Equipment safety

12.2.1 The workspace is organized in compliance with sanitary standards and requirements approved by authorized bodies in the field of sanitary and epidemiological welfare of the population.

12.2.2 Those responsible for information security conduct explanatory work among employees on issues of protecting equipment left unattended and liability for violating established rules.

12.2.3 The procedure for removing assets outside the protected area, their reuse with mandatory destruction of data, movement and disposal is determined by the internal Rules for inventory and certification of equipment and software.

12.2.4 The Information Technology Department regularly conducts an inventory of workstations and servers and checks their configurations.

12.2.5 Users must be aware of the rules for protecting equipment left unattended and understand the consequences of non-compliance with these rules.

12.2.6 To minimize the risks of unauthorized access, loss or damage to information, it is recommended to apply:

- a "clean desk" policy in relation to paper media and removable storage devices;
- a "clean screen" policy in relation to information processing devices.

12.2.7 The following measures should also be taken into account:

1) media containing sensitive information should be removed and locked when not in use or when the room is empty;

2) computers, terminals and printers should be switched off when finished;

3) equipment left unattended should be protected by passwords or other means;

4) automatic screen locking should be set up after a certain period of inactivity;

5) documents containing confidential information should be removed from printers immediately after printing.

13 Organization assets management

13.1 Accounting and using assets

A tangible or intangible object that is a piece of information or contains some information, or serves to process, to store, to transmit information and is valuable to

the University, in the interests of achieving its goals and continuity of its activities (hereinafter referred to as assets associated with information processing facilities; assets) must be protected and managed.

13.1.2 The main objects (assets) of information security are the following elements:

1) information resources containing information of limited distribution and presented in the form of documents or records in magnetic, optical and other media, information physical fields, arrays and databases;

2) software (operating systems, database management systems, other general system and application software) of information systems used to process information;

3) automated communication and data transmission systems (telecommunication facilities);

4) communication channels through which information is transmitted (including information of limited distribution);

5) computer equipment intended for processing, storing and transmitting information resources (hardware).

13.1.3 To ensure asset protection, the following is performed:

1) determining the application boundaries;

2) asset inventory;

3) asset identification;

4) classification and marking assets in accordance with the classification system adopted at the University;

5) assigning assets to officials (owners) and determining their measure of responsibility for the implementation of asset information security management activities.

13.1.4 The asset owner ensures proper asset management throughout the entire asset life cycle.

13.1.5 To monitor the movement of the organization assets, their accounting, control and ensuring an appropriate level of protection, the organization maintains a list of assets associated with information processing tools that contains the information of the asset name, the asset class, the asset type, and the asset significance.

14 Human resources management

14.1 Personnel background check upon hiring

14.1.1 When hiring, as well as when engaging contractors and users from third-party organizations, a thorough background check is carried out in accordance with the internal regulations of the University and the current legislation of the Republic of Kazakhstan, while maintaining the confidentiality of personal data.

14.1.2 Particular attention is paid to checking candidates and organizations whose activities are related to the processing of official information with limited access, or with classified information and relevant technical means.

14.1.3 Employees and representatives of third-party organizations who gain access to the University's information systems are required to sign an agreement on compliance with information security requirements. This is necessary to reduce the risks associated with theft, fraud and misuse of resources.

14.1.4 Before providing access to the University information systems, equipment or resources, an employee, contractor or representative of a third-party organization signs a confidentiality and non-disclosure agreement.

14.1.5 Functions and responsibilities in the field of information security are fixed in the job descriptions of the University employees and/or in the terms of employment contracts.

14.1.6 The information of employees hired must be collected and processed in accordance with the labor legislation of the Republic of Kazakhstan.

14.1.7 Requirements and measures of responsibility for ensuring information security when interacting with third parties must be reflected in the terms of the concluded contracts.

14.1.8 When involving external organizations in work related to ensuring the information security of the University information systems, the owner (holder) of these objects concludes contracts regulating the conditions of access, use and measures of responsibility for their violation.

14.2 Raising awareness and training employees in the field of information security

14.2.1 All the University employees must be familiar with the provisions of this Policy, as well as with the approved rules and instructions on information security. Familiarization must be confirmed by signatures on the relevant registration sheets.

14.2.2 Any changes and additions to the requirements of the Policy and related instructions must be promptly communicated to employees with access to information systems, in accordance with their functional responsibilities.

14.2.3 Training or briefing on information security issues is conducted before an employee begins using the University information resources and systems.

14.3 Changes in the terms of employment and dismissal

14.3.1 Upon termination of an employment contract or change in the terms of employment of an employee, all the types of access, physical and logical, to the University information systems and resources are cancelled or revised. This includes disabling access identifiers, subscriptions, and revocation of documents confirming the status of an active employee.

14.3.2 The obligations of employees in the field of information security that are valid after the end of the employment relationship, must be fixed in the employment contract.

15 Replication, backup and storage of information

15.1 To ensure the physical integrity of data, as well as to avoid intentional or unintentional destruction or distortion of protected information and configurations of information systems, backup copies of databases, configurations, settings files and configuration files are organized, if the appropriate technical and software backup tools are available.

15.2 To ensure guaranteed recovery of particularly important information that may be lost as a result of hardware failures, virus attacks (including ransomware), daily backup copies of the disk contents are made. The process is performed automatically using incremental backups, if the appropriate software and equipment are available.

15.3 Responsibility for organizing the backup process, storing backup copies and restoring information is assigned to the administrators of information systems and authorized employees of the ITD.

16 Information security auditing

16.1 To ensure confidence in the adequacy and effectiveness of the organization's approach to information security management, an information security audit may be conducted in the manner and within the specified time frame.

16.2 The audit can be performed by specialists of the University structural unit responsible for ensuring information security, as well as by experts from third-party organizations with the appropriate qualifications.

16.3 Conducting an audit allows for an assessment of the current state of information security of the state body information technology facilities, its compliance with the purposes and objectives of this Policy, the requirements of the current legislation in the field of information technology, and international and state standards in the field of information security.

16.4 The audit program includes, among other things, an instrumental examination of the information technology facility and its components. An instrumental examination can include:

- auditing the security of the IT infrastructure and information systems;
- penetration testing (assessment of the security of the network perimeter);
- analyzing the program code for vulnerabilities;
- load testing (performance assessment).

16.5 The audit results should help identify weak points in the existing information security system and optimize it, improve the security measures applied. The audit results should be used as input data for risk analysis and assessment.

16.6 The results of the audit are documented and communicated to the management.

17 Policy requirements violation

17.1 The University information security management system provides for the application of disciplinary practices in case of violation of information security requirements, as a deterrent to prevent such violations by employees of the organization in the future.

17.2 Disciplinary practices should not be applied without preliminary checks, clarification of the circumstances and facts of the violations. In the event of establishing the fact of a violation by employees or groups of employees, measures are applied in accordance with the legislation of the Republic of Kazakhstan.

18 Coordination, approval and implementation of the internal regulatory documents

18.1 Internal regulatory documentation must be agreed upon with the head of the department responsible for the relevant area and the organization management. If the regulatory act concerns financial matters, it is agreed upon with the chief accountant. Coordination is carried out with officials determined depending on the content of the document and their competencies. The responsibility for determining the list of persons with whom the document must be agreed upon rests with the developer of the document.

18.2 The period for reviewing the documentation must not exceed five working days from the date of receiving. All the comments must be substantiated and set out in a specific form.

18.3 If there are no comments, the document is signed by the relevant officials and submitted for approval.

18.4 After approval, the document is subject to translation into the state language and, if necessary, into English for subsequent posting on the official resources of the organization.

18.5 The document signed by the developer and the approving persons, is submitted for approval to the head of the organization or an authorized person.

18.6 The date of entry into force of a document is the date of its approval. The document comes into force from the moment of approval and is mandatory for execution.

18.7 The approved document is transferred for safekeeping to the archive or the department responsible for documentation support, in paper and/or electronic format, depending on the internal requirements of the organization.

18.8 When an updated document is entered into force, the previous version of the document loses force and is considered invalid.

19 Safekeeping

19.1 After the electronic version of the internal regulatory document is posted on the University website, the executors familiarize themselves with it and put their signature on the familiarization sheet, which is mandatory for all the documents. In departments and divisions, the head of the department/division is responsible for familiarizing employees with the documents received.

19.2 The head of the division is responsible for replication, recording of copies, unauthorized use and safety of the document.

19.3 The full electronic version of the document is stored in electronic form, and the title page and familiarization sheet are in printed form.

20 Procedure for reviewing and updating the Information Security Policy

20.1 The Information Security Policy is revised at least once every two years and is aimed at bringing the protective measures defined by the Policy into line with real conditions and current requirements for information security.

20.2 Unscheduled amendments to this Policy can be made based on the results of an analysis of information security incidents, the relevance, sufficiency and effectiveness of the information security measures used, the results of internal information security audits and other control activities.

20.3 Specific regulatory documents, such as rules, instructions, technical requirements and others, are drawn up as Appendices to this Policy. They are developed and updated as necessary approved by the order of Chairman of the Management Board, Rector or an authorized official and have the same legal force as the main Policy, without the need for their approval at the Management Board level.

F.01-2022

Coordination Sheet

Position	Name	Date	Signature
Member of the Management Board, Vice-Rector for Strategic Development and Digitalization	Kanapyanov T.E.		
Head of the Legal Division	Ayazbayeva G.S.		
Director of the Economics and Finance Department, Chief Accountant	Abiltussupova A.H.		
Director of the ALD	Kozhukhova M.M.		
Director of the Information Technology Department	Aubakirov G.D.		

F.02-2022

Familiarization Sheet

Position	Name	Date	Signature