Approved by
Chairman of the Board, Rector of
Abylkas Saginov Karaganda Technical University NJSC
_____ S.S. Sagintayeva
Board decision
No. 29 dated January 14 2026

INTERNAL REGULATORY DOCUMENT

RULES OF USING MEANS OF CRYPROGRAPHIC INFORMATION PROTECTION

IRD II-04-2026

Developed by: Information security engineer
D.K. Chityan_____

Karaganda

Contents

1 Scope

1.1 These Rules of using cryptographic information protection tools (hereinafter referred to as the Rules) establish requirements for the use of cryptographic information protection tools at Abylkas Saginov Karaganda Technical University NJSC (hereinafter referred to as the University).

1.2 Cryptographic information protection tools are used to ensure the confidentiality of electronic documents and data during their transmission over open communication channels, as well as to protect personal data and other confidential information from unauthorized access and leakage.

1.3 The requirements of these Rules apply to all the University information systems that utilize cryptographic information protection tools, as well as to employees and other persons authorized to use them.

1.4 These Rules are an internal regulatory document of the University and are binding on all users of cryptographic information protection tools.

2 Regulatory references

2.1 The following regulatory documents were used in developing the Rules:

1) Law of the Republic of Kazakhstan dated November 24, 2015, No. 418-V "On Informatization".
2) ST RK ISO/IEC 27002-2023 “Information security, cybersecurity and privacy protection. Information security controls”.
3) ST RK ISO/IEC 27001-2023 “Information security, cybersecurity and privacy protection. Information security management systems. Requirements”.
4) Resolution of the Government of the Republic of Kazakhstan dated December 20, 2016, No. 832 "On Approval of Uniform Requirements in the Field of Information and Communication Technologies and Information Security".

2.2 These Rules are an internal regulatory document of the University and comply with the University's Information Security Policy.

2 Terms, definitions and abbreviations

3.1 The following terms, definitions, and abbreviations are used in these Rules:

1) University — Abylkas Saginov Karaganda Technical University NJSC.
2) Cryptographic information protection tools.
3) Key information — data used to perform cryptographic transformations.
4) Key compromise — an event in which a private key has become or could become accessible to unauthorized persons or processes.

5) Cryptographic information protection tool user — a University employee authorized to operate cryptographic information protection tools.

6) ISS — University Information Security Service.

7) DIT — University Information Technology Department.

4 Responsibility and authority

4.1 The Information Security Service provides methodological support for the use of cryptographic information protection tools, participates in the investigation of incidents involving the compromise of key information, and makes proposals for improving cryptographic protection measures.

4.2 The Information Technology Department ensures the technical operation of cryptographic information protection tools, the management of key information, and the blocking and replacement of keys when a compromise is detected.

4.3 Users of cryptographic information protection tools are personally responsible for compliance with the requirements of these Rules, the security of key information and key carriers, and the prevention of unauthorized access to cryptographic information protection tools.

5 General provisions

5.1 Only authorized persons appointed by order of Chairman of the Management Board, Rector of the University or an authorized person are permitted to operate cryptographic information protection tools.

5.2 Key information must be stored in conditions that prevent unauthorized access, loss, copying, or unauthorized use. To ensure the safety of key information, backup copies are created and stored separately.

5.3 The use of software that could disrupt the functioning of cryptographic information protection tools is prohibited at workstations where cryptographic information protection tools are used. If such software is detected, work with cryptographic information protection tools must be immediately stopped until the violation is rectified.

5.4 Any compromise of key information must be immediately notified to the Information Technology Department and the Information Security Service. Compromised keys will be blocked in accordance with established procedures, and work can only be resumed after they are replaced.

5.5 Destruction of key information is carried out in accordance with established requirements with mandatory documentation of the fact of destruction.

6 Work with cryptographic information protection tools

6.1 Authorized persons appointed by the relevant order of the University's Chief Executive Officer are engaged to work with cryptographic information protection tools (CIPT).

6.2 Persons authorized by the relevant order to operate CIPT and to receive and to use encryption keys are personally responsible for:

1) maintaining the confidentiality of confidential information acquired during their work with CIPT;

2) maintaining the confidentiality of the contents of CIPT private keys;

3) securing key information media and other documents related to the operation of CIPT.

6.3 The University ensures storage conditions for key media that prevent unauthorized access, use, or copying of key information. Key media must be stored in cabinets (drawers, safes) for individual use.

6.4 To prevent the loss of key information due to media defects, backup copies must be created after receiving the media containing key information. Copies must be appropriately labeled and used in the same manner as the originals. Separate storage of active and backup key media must be ensured.

6.5 The user is responsible for ensuring that the computer on which the cryptographic information protection system is installed is free of any programs (including viruses) that could interfere with the operation of the software-based cryptographic information protection system.

6.6 If third-party programs or viruses are detected at a workstation equipped with a cryptographic information protection tool (CIPT) that disrupt the operation of said tools, work with the information protection tools at that workstation must be stopped, and measures must be taken to analyze and eliminate the negative consequences of this violation.

6.7 Users of the CIPT are prohibited from:

1) disclosing the contents of key information media or transferring the media themselves to unauthorized persons, or displaying key information on a monitor or printer;

2) inserting the key media into the disk drive or USB reader of a personal computer (hereinafter referred to as a PC) during work that is not considered standard key use procedures (encryption/decryption of information, verification of an electronic digital signature, etc.), or into disk drives or USB readers of other PCs;

3) writing third-party information to the key media;

4) making any changes to the CIPT software;

5) use previously used key media to record new information.

7 Actions in case of key compromise

7.1 Compromise of private keys means:

1) their loss (including subsequent discovery),

2) theft,

3) disclosure,

4) unauthorized copying,

5) their transmission over communication channels in cleartext,

6) dismissal for any reason of an employee with access to key media or key information on such media,

7) any other types of disclosure of key information that could result in private keys becoming accessible to unauthorized persons and/or processes.

7.2 The User is responsible for independently determining the fact of a private key compromise and assessing the significance of this event. The User is responsible for organizing and implementing measures to identify and localize the consequences of a compromise of confidential information transmitted using cryptographic information protection tools.

7.3 If the User's key is compromised, they must immediately cease communication with other subscribers over the network and notify the Head of the University's Information Technology Department and the information security officer. No later than one hour after receiving a key compromise notification, the IT Department must block the User's key in the system. Resumption of system operation will only be possible after the compromised keys are replaced.

8 Destruction of key information

8.1. Destruction of key information from single-use storage media is accomplished by causing irreparable physical damage to them, preventing their use and preventing recovery of the key information.

8.2 Destruction of key information from reusable storage media is accomplished by erasing the key information without damaging the key media (to ensure its repeated use). Key information is erased using the technology adopted for the corresponding reusable key media.

8.3 Actions performed by Users during the destruction of key information are recorded in a corresponding report and signed by the user and an ISS employee.

9 Coordination, approval and implementation

9.1 These Rules are subject to approval by the heads of the University structural divisions whose activities are related to the operation of information systems and the use of cryptographic information protection tools. If the provisions of the Rules affect matters of financial liability or the accounting of key information carriers, approval is obtained from the relevant responsible divisions.

9.2 The list of officials and structural divisions with whom approval of these Rules is required is determined by the document developer, taking into account its content and scope of application.

9.3 The review period for the draft Rules shall not exceed five business days from the date of its receipt. Comments and suggestions shall be presented in a reasoned and specific manner.

9.4 If there are no comments, or after they have been taken into account, the document is signed by the approving persons and submitted for approval to the executive body, the Management Board.

9.5 The date of these Rules' entry into force shall be the date of their approval. From the date of approval, the Rules are binding.

9.6 When a new version is approved or amendments are made, the previous version of the Rules becomes invalid and is considered null and void.

10 Safekeeping

10.1 The original of these Rules is stored in the University Information Security Service.

10.2 An electronic version of these Rules is posted on the University corporate information resources, ensuring access for interested structural divisions and authorized employees.

10.3 University employees are familiarized with these Rules in the manner established for internal regulatory documents, with the completion of a familiarization sheet.

10.4 The heads of structural divisions are responsible for maintaining records of copies, preventing unauthorized use, and maintaining the document's safety within their respective divisions.

11 Procedure for revising and updating

11.1 These Rules are reviewed by the Information Security Service at least once every two years and are aimed at bringing the document's requirements into line with

the current operating conditions of cryptographic information protection tools, the development of the IT infrastructure, and the requirements of the Information Security Management System.

11.2 Unscheduled updates of the Rules are carried out in the event of changes in the scope of the Information Security Management System, changes in the requirements of the legislation of the Republic of Kazakhstan and information security standards, the introduction of new cryptographic protection tools, as well as based on the results of incidents, internal audits, and information security audits.

11.3 Amendments and additions to these Rules are issued as a new version or a separate administrative document and are approved in accordance with the procedure established for the approval of these Rules.

F.01-2022

Coordination sheet

Position	Name	Date	Signature
Member of the Board, Vice-rector for Digitalization	Amirov A.Zh.	9.12.25	
Head of the Legal Service	Ayazbayeva G.S.	9.12.25	
Head of the Software Center	Shtefan K.B.	9.12.25	

F.02-2022

Familiarization sheet

Position	Name	Date	Signature