

«APPROVED»

Kimyo International University in Tashkent

_____A.B. Allakuliev

«____» _____ 20____

INFORMATION SECURITY CONCEPT OF KIMYO INTERNATIONAL UNIVERSITY IN TASHKENT

I. General Provisions

1. This Information Security Concept of Kimyo International University in Tashkent (hereinafter — KIUT) defines the strategy for ensuring information security in the course of creating, processing, transmitting and storing information in the KIUT information system.
2. The KIUT Information Security Concept (hereinafter — the Concept) is the fundamental document establishing the goals, objectives, principles and main measures for the protection of information.
3. The Concept applies to all employees and users who have access to the KIUT information system.
4. The following terms and definitions are used in this Concept:
 - **Authorization** — granting access rights to a user;
 - **Authentication** — confirmation of a user's identity;
 - **External data transmission channels** — data transmission channels that are not under the control of KIUT employees;
 - **Secrets** — information of particular importance;
 - **Demilitarized zone** — a special zone in the information system created for transferring data from one access level to another, with information security requirements specific to the nature of the operations performed in the zone (VLAN);
 - **documented information** — information recorded on a tangible medium with details that allow it to be identified;
 - **information protection** — measures to prevent threats to information security and to eliminate their consequences;
 - **information** — data about persons, objects, facts, events, phenomena and processes, regardless of their sources and form of presentation;
 - **KIUT information system** — the totality of KIUT hardware and software, taking into account the applicable requirements for their separate and joint operation;

- **confidential information** — documented information to which access is restricted;
- **unauthorized access to information** — access to information in violation of the established access control rules;
- **information system maintenance staff** — the employees responsible for supporting the information system;
- **information system user** — a person, regardless of place of employment, who connects to, receives or transmits information in the information system;
- **information security threat** — a potential for intentional or unintentional impact on the information system that may directly or indirectly cause damage to the users or owners of the information system;
- **physical network segregation** — division of a data transmission network into several independent networks not connected by hardware;

II. Purpose and Objectives of the Concept

5. The main purpose of the Concept is to establish an overall strategy for ensuring the information security of the KIUT information system.
6. The main objectives of the Concept are:
 - defining the basic principles for building the information security system;
 - defining the basic requirements for the operation of the information security system;
 - establishing the organizational and methodological framework for implementing the information security system;
 - identifying priority areas for the development of the information security system.

III. Basic Principles of the Concept

7. The Concept is based on the following principles:
 - protection of any information whose unlawful handling may cause damage to KIUT;
 - compliance of the information security system with the legislation of the Republic of Uzbekistan;
 - phased development of the information security system, taking into account the current organizational structure of KIUT and the priority of implementing information security measures;
 - ensuring adequate awareness and training of employees and users of the KIUT information system in the field of information security;
 - creating an effective system for financing information security measures.

IV. Legal Basis of the Concept

8. Regulatory documents developed in accordance with the Concept must comply with the requirements of legislation and with KIUT information security documents.
9. In general, the information technology and information security standards adopted by KIUT apply to the organization of KIUT information security systems.
10. KIUT ensures that the relevant employees are familiarized with legislative acts and with standards in the field of information technology and information security.

V. Objects of Protection and Risk Assessment

11. The KIUT information system is a distributed system united into a single information and telecommunication network in which information subject to protection is shared.
12. The operation and support of the KIUT information system is carried out by the Digital Technologies Center (hereinafter — DTC).
13. Information circulating in the KIUT information system is divided into the following levels:
 - restricted-access information in the KIUT information system;
 - publicly available information in the KIUT information system.
14. Confidential information includes:
 - personal data of employees;
 - official (internal) information;
 - information restricted by orders.
15. Internal publicly available information includes information created and used by employees in the KIUT information system in the performance of their job duties, except for information classified as internal restricted-access information.
16. The main threats to information security in the KIUT information system take the following forms:
 - unauthorized disclosure, leakage or theft of information;
 - unauthorized blocking or destruction of information, disruption of technological processes, disorganization of the information system's operation, destruction of the information system's information and software resources;
 - distortion, substitution or falsification of information;

- system failures.
17. By the nature of their occurrence, information security threats are divided into the following groups:
- a) artificial threats, which in turn are divided into:
- **unintentional threats:** erroneous, accidental or careless violations, without malicious intent or self-interest, of the established regulations for the collection, processing and transmission of information and of information security requirements, as well as other actions of persons leading to unproductive expenditure of time and resources, disclosure of restricted-access information, loss of valuable information or disruption of individual workstations, subsystems or the information system as a whole;
 - **intentional threats:** violations committed for personal gain, under coercion by third parties or with malicious intent, and other violations of the established regulations for the collection, processing and transmission of information and of information security requirements, as well as other actions of persons leading to unproductive expenditure of time and resources, disclosure of restricted-access information, loss of valuable information or disruption of individual workstations, subsystems or the information system as a whole;
- b) natural threats:
- failures, accidents and malfunctions of hardware and software resulting from natural disasters, natural cataclysms, etc.
18. Hardware and software systems containing internal restricted-access information may be operated only after the necessary information protection measures have been taken. Protection procedures and engineering and technical measures must be aimed at:
- preventing a threat or localizing the impact of an information security threat;
 - restoring the operability of the information system when necessary.
19. Availability periods must be determined for each item of information and for each type of internal restricted-access information.
20. Appropriate procedures and demilitarized zones must be created for transferring information from one access level to another.

VI. Ways of Countering Information Security Threats

21. The main measures aimed at ensuring the required level of information security are divided into:
- physical protection measures;
 - organizational protection measures;
 - engineering and technical protection measures.

22. Physical protection measures are based on the use of various mechanical, electronic and electromechanical devices and structures specifically designed to create physical barriers on the possible paths by which potential intruders could penetrate and gain access to components of the information system and protected information, as well as technical means of visual surveillance and security alarms.
23. Physical protection of the buildings and premises housing the main components of the KIUT information system is provided by the security service.
24. Physical protection measures for premises must ensure:
 - prevention of unauthorized persons from entering the protected facility;
 - round-the-clock surveillance of the protected facility housing the main components of the information system;
 - identification of every person visiting the protected facilities and maintenance of a visitor log;
 - blocking of all possible paths of entry and access to the protected facility in emergencies.
25. Organizational (administrative) protection measures regulate the operation of the data processing system, the use of information, the activities of maintenance staff and the interaction of users with the information system in such a way as to make it as difficult as possible, or impossible, to carry out information security threats, or to reduce losses if they are carried out.
26. The main purpose of organizational measures taken at the top management level is to make decisions and develop documents in the field of information security, providing, among other things, for:
 - allocation of the necessary human and financial resources;
 - regular audits of the state of information security;
 - implementation of measures aimed at ensuring KIUT information security.
27. KIUT develops instructions, regulations and other normative documents defining the procedure for:
 - granting access to internal restricted-access information;
 - maintenance and modification of hardware and software, and repair of hardware corresponding to the access category;
 - maintaining databases in the information system;
 - use of the information system by users;
 - granting access to internal publicly available information;
 - support of the information system by maintenance staff;
 - taking measures in emergencies;

- KIUT employees and other persons must be granted access to the information system in accordance with the approved procedure;
28. The level of authority of each information system user is determined individually, subject to the following requirements:
- users are granted access only to information that falls within their job duties;
 - when granting users access to the information system, the principle «any powers and rights not explicitly permitted are prohibited» is observed;
 - administration and support of the information system must be carried out with a separation of duties, rights and powers between operating system and database management system administrators, application administrators, local area network administrators and information security administrators;
 - all employees authorized to work in the information system and the maintenance staff bear personal responsibility for violations of the established procedure for automated data processing and of the rules for storing, using and transferring the information, hardware and software at their disposal;
 - Upon hiring, each employee must sign an Agreement-Undertaking to comply with the established rules for working with protected information in the KIUT information system and acknowledging liability for their violation;
29. All database maintenance operations, any changes to the database, and changes to the composition and powers of database users (including maintenance staff) in the KIUT information system must be carried out in accordance with the approved procedure.
30. The safety of database information is ensured by maintaining a daily electronic archive in accordance with approved technological instructions. The following requirements must be observed:
- the database is archived in full, including the software package and auxiliary management tools;
 - electronic archives are stored on external non-volatile storage media;
 - scheduled or unscheduled checks of electronic archives are organized to determine their suitability for restoration;
 - a backup data processing system is organized that fully or partially duplicates the active data processing systems and is located away from the main data center.
31. All processes of maintenance and modification of hardware and software, the commissioning of new hardware, software and subsystems, and all changes to

the configuration of hardware, software and subsystems in the KIUT information system must be carried out only on the basis of the approved procedure.

32. All KIUT hardware and software must be categorized by access level in the established manner (for information stored and processed using the relevant hardware and software, the required access level must be determined and assigned to that hardware and software).
33. The configuration of hardware and software must correspond to the duties assigned to users and to information security requirements based on the nature of the information and its access level.
34. Information not related to the employee's duties (software, games, films, clips, etc.) must not be stored on hardware and software connected to the KIUT information system and must be deleted immediately upon discovery.
35. Engineering and technical protection measures must be based on the use of various electronic devices and special programs that are part of the KIUT information system and perform information protection functions (independently or in combination with other means).
36. Subject to compliance with the applicable information security requirements and procedures, engineering and technical information protection measures must ensure:
 - the availability, integrity and confidentiality of information circulating in the KIUT information system;
 - control of access to the information system and logging of all events; rational use of information system resources;
 - the integrity and operability of the information security system;
 - detection and prevention of information security threats;
 - data backup and recovery.
37. Engineering and technical protection measures must include:
 - means of identifying and authenticating users (including administrators) and information system elements (workstations, terminals, database elements, etc.), and means of controlling and restricting access to the information system;
 - means ensuring uninterrupted operation of the information system;
 - means of archiving and storing information;
 - anti-virus information protection tools;
 - other modern software and hardware information protection tools.
38. User authentication must be performed using passwords, depending on the nature of the information and the access category.
39. Access control tools must authorize a user after the user has been recognized by the information system.

40. User authorization must be carried out using the following access control mechanisms:
- discretionary access control based on attribute schemes, permission lists, etc.;
 - mandatory access control based on information confidentiality labels and user access levels;
 - provision of a closed environment of trusted software;
41. Technical access control tools must be an integral part of a unified access control system.
42. The KIUT information system must include means ensuring uninterrupted operation (redundant system elements, uninterruptible power supplies, electric generators, etc.).
43. The main requirements for means ensuring the uninterrupted operation of the information system are:
- automatic response to failure or shutdown (start-up) of a main node of the information system or of the power supply, and ensuring uninterrupted operation of the information system for the established period;
44. Information archiving and storage tools must ensure reliable operation of the information system by restoring information when necessary.
45. The main requirements for organizing an electronic archive in the KIUT information system are:
- appointment of an employee responsible for electronic archiving and backup;
 - reliable storage of archived data;
46. The main requirements for organizing anti-virus protection of information in the KIUT information system are:
- use of licensed anti-virus software;
 - organization of continuous anti-virus scanning;
 - keeping the anti-virus databases (signature lists) of the anti-virus software up to date, both on the administrative side (servers, etc.) and on the user side (users' personal computers) of the information system, through automatic or manual updates;
 - organization of regular checks of the anti-virus system's operability;
 - organization of identification of the source of computer virus propagation in the information system;

VII. Implementation of the Concept

47. To implement the Concept, it is necessary to:
- a) apply a multi-layered information protection system depending on the nature and category of information:
 - first layer of protection — physical restriction of access to the hardware and software of the information system;
 - second layer of protection — user identification and authentication;
 - b) inform users of changes in information security legislation that directly concern them;
48. The information security unit is assigned the following functions:
- control of user access to the information system, including setting passwords and changing them periodically;
 - control of the storage of backup copies of information system databases and of the creation and storage of the information security systems database;

IX. FINAL PROVISIONS

49. The Concept is subject to regular review and updating.

50. Amendments are approved by KIUT management.

Vice-Rector for Strategic
Development and Digitalization

U.A. Vosikov

Head/Director of the
Digital Technologies Center

I.G. Li