ҚАЗАҚСТАН РЕСПУБЛИКАСЫ АСТАНА Қ. «АСТАНА МЕДИЦИНА УНИВЕРСИТЕТІ» АКЦИОНЕРЛІК ҚОҒАМЫ * РЕСПУБЛИКА КАЗАХСТАН Г. АСТАНА АО «МЕДИЦИНСКИЙ УНИВЕРСИТЕТ АСТАНА» * АСТАНА МЕДИЦИНА УНИВЕРСИТЕТІ

Approved by the decision of the Board of JSC “Astana medical University” №17, from 25 May 2012

______REGULATION_____

INTEGRATED MANAGEMENT SYSTEM

REGULATION ON INFORMATIONAL SECURITY OF JSC “ASTANA MEDICAL UNIVERSITY”

ASTANA

Illegal copying is prohibited!

Content

1. General provisions

1.1. This Regulation on informational security (hereinafter – Regulation) defines the modern position and the nearest perspectives of developing corporate data transmission network (hereinafter – CDTN) of JSC "Astana Medical University" (hereinafter – University), aims, objectives and juridical basis of use, functioning regimes and also analyses of security threats for its resources.

1.2. The Regulation's requirements are applicable to the structural subdivisions of the University, its subordinate organizations, where there automated information processing is implemented, including restricted information (internal information) or personnel data, also implementing maintenance, service and providing of the University's functioning. The Regulation is applicable to other organizations and enterprises, implementing relation with the University as providers and users of information and service.

1.3. Information technologies department and legal providing department are responsible for immediate organizing (constructing) and providing effective functioning of security system at the University.

1.4. The employees of information technologies department, chief lawyer-consultant of juridical department, chief of financial-economical department, chief of cadre work and legal providing hold all necessary technical and organization activities to provide information security.

1.5. Vice-rector for administrative and economical activities realizes measures towards securing corporate secrets, providing informational security and the regime of secrecy at the University and subordinate organizations.

1.6. Chief, chief engineer of informational technologies department (hereinafter – ITD) implement the organization of qualified working out (improvement) of information security system and organizational (administrative) provision of its functioning at the University.

2. Main part

2.1. Aims and objectives

2.1.1. The main aim to which all the paragraphs of the Regulation are directed is to provide safely information security as a result of preventing material, physical, moral or other damage to the University as the result of information activities.

2.1.2. The shown aim is reached through providing and constant maintaining the following conditions of corporate data transmission network:

- Accessibility of the information being processed for registered users,

- Sustainable functioning of the University's CDTN,

- Providing confidence of the information, kept and processed by means of computer technology (hereinafter – MCT) and transmitted by communication channels,

- Continuity and authenticity of the information, kept and processed by information system (hereinafter – IS) of the University and transmitted by communication channels.

2.1.3. To reach the settled aims, it is necessary to complete the following tasks:

- To prevent from interference of bystanders into the process of functioning information resources of the University
- To limit access of registered users to the information, apparatus, program and cryptographical sources of security, used in IS systems,
- To register users in the history list system when using net resources,
- To control periodically the correctness of activity of the system's users by analyzing this history lists by specialists of information security,
- To control continuity (providing constancy) of the program runtime environment and to recover it in the case of its disruption,
- To secure information from non-authorized modification, damage,
- To control the continuity of program resources in use, also to protect the system from input of rogue programs,
- To secure official secrets and personal data from spreading, non-authorized sharing and damage in processing, keeping or transmitting it through communication channels,
- To provide authority and authentication of users who participate in information exchange,
- To detect in time threats to information security, reasons and conditions, leading to make damages,
- To create mechanism of operative reacting for threats of information security and negative tendency,
- To create conditions and instructions to minimize and localize the damage by illegal actions of physical and juridical bodies, weakening the negative influence and liquidations of outcomes of breaking the information security.
- To create and provide continuous functioning of electronic document management,
- To carry out constantly audit of the security policy by internal audit not less than one time in 6 months and external audit – one time in a year.

2.2. Users of information system.

2.2.1. The users of the information system are:

- Employees –workers, implementing their activities at the University and having basic rights and duties according the law of Republic of Kazakhstan,

- Support personnel – maintenance or servicing personnel of subordinate and external organizations, working together with the University as a supplier and user of information and service.

Among those:

- Administrators of corporate data network, responsible for maintenance of tele-communication equipment,
- System administrators, responsible for maintenance of the general and applied software,
- Creators of applied software,
- Engineer – system technicians, technologists,
- Specialists of information security (special security sources) and others,
- Service users/ bodies and/or external organizations using the University's information resources
- Students, interns, residents, master's students MBA students and doctoral students.

2.3. Models of potential intruder

2.3.1. Potential intruder of informational security is a body or a group of bodies who are or are not in collusion that can create different fails of information security specially or occasionally, the actions of whom are directed into making moral and/ or material damage to the University's interests.

2.3.2. Potential intruder can be divided into internal and external. All University workers and support personnel are practically internal. They can be divided into the following groups, depending on the level of access for information resources of corporative network:

- People having access to the information with personalized and service secret,
- People having access to the information, which contains service secret, and who are involved into technology of processing, keeping information,
- People having no access to the information with personal and service secret, but who are involved into technology of treating/ keeping/ transmitting information,
- Serving personnel.

2.3.3. To construct a real model of potential intruder it's necessary to consider types of intrusion, aims of different people and organizations, and also interests of other physical bodies connected with the University.

2.3.4. There are the following types of intrusion, possible at the University:

- Non-authorized use of programs leading to negative work of CDTN of University (net scans, intensive wide traffic, etc),

- Use of the right of local administrators in working stations of users that gives possibility for ordinary users to set an unlimited program amount,

- Intrusions by workers because of the absence of knowledge in the requirements of information security and legal acts of University.

2.3.5. Potential external intruders:

- Former workers and support personnel,

- Representatives of organizations co-working in providing life-sustaining activity (energy, water, heating, etc.)

- Visitors/ invited organization representative, citizens);

- Representatives of firms supplying technique, software, services, etc.

2.4. Appropriation, normative and juridical basis of the Regulation

2.4.1. This Regulation specifies the requirements of solving the matters to provide information security in information tele-communication sphere, joining IS of the University.

2.4.2. The Regulation on the University's Information system is a methodological basis for:

- Working out and improving the complex of agreed normative, juridical, technological and organizational measures, directed into information secuity,

- Providing information security,

- Coordination of territorial and structural activities under-branches when caring out works on complying with the requirements of providing information security,

2.4.3. Scientific-methodical basis of the Regulation is a complex approach, suggesting holding researches, working out of the system of information security in processing it in information systems considering all factors, providing its influence and complex use of different measures and protecting sources.

2.4.4. The main requirements of the Regulation are based on qualitative analyses of matters of information security without paying attention to the economical (quantitative) risk analyses and validation of necessary expenses for information security.

2.4.5. Normative and juridical basis of the Regulation are: Decree of the President of Republic of Kazakhstan from November, 2011, №174 "On the conception of information security of the Republic of Kazakhstan till 2016 ", Laws of the Republic of Kazakhstan "On the national security of the Republic of Kazakhstan", "On governmental secrets", "On antiterrorism actions", "On electronic documents and electronic digital signatures", "On computerization", "On technical regulations", "On license", "On Mass Media", "On communication", "Program on information and communication technologies development" in the Republic of

Kazakhstan from 29 September, 2010, № 983 and other acts of the Republic of Kazakhstan and University regulating the maintenance of information security.

2.5.Means and measures of information protection

2.5.1. Means and measures of protection from data leak by communication channels.

2.5.1.1. Protection of information from leak by communication channels from/to the University is implemented by the use of complex programs, technical protection sources and organizational measures.

2.5.1.2. To detect data leak, it is necessary to control systematically possibilities of leak channels forming and evaluation of their danger throughout the control zones. Closing and locating the leak channel is provided by organizational technical measures.

2.5.1.3. According to the used channels of electronic information transmission at the University, necessary technical protecting sources (internet screen, etc.) are applied. There is the organization of system of registration, sharing, receiving and storage of information mediums. There is the consideration of necessary ways of destroying information mediums with the aim of preventing possibilities to restore saved data in them. Technical channels of transmitting the information are provided by appropriate protecting sources. Safe system of securing buildings and constructions is created; pass control inside the University building to prevent entrance of external people is organized.

2.5.2. Measures to protect means of computer technology.

2.5.2.1. Protection of MCT from non-authorized access at the University is constructed in several directions. Automated means of users’ registration, locking system of user accounts and informing employees on threats or breaking into MCT are created according to the Rules for users’ registration in the corporate data transmission network (AMU Rule - 08) and the Plan of providing continuous activity of the University’s information systems.

2.5.2.2. Organization measures on preventing non-authorized access are determined (hereinafter – NAA), as well as in the case of losing pass words and MCT operational incident according to the passwording policy (AMU Rule-09).

2.5.2.3. In the case of detecting facts of NAA to information resources and systems of the University or finding out of potential risks to information security, employees of ITD inform urgently the chief responsible for connection.

2.5.3. Protection against hardware special enclosures, illegal incorporation and use of unaccounted programs

2.5.3.1. In order to protect against hardware special enclosures, measures of physical protection are used, sources of video observation and control of access to server room of the University are set up.

2.5.3.2. In order to protect against hardware special enclosures, illegal incorporation and use of unaccounted programs at the University except the actions, including physical protection, implementation of audit of use of MCT and monitoring of system journals, a base complex of software to be settled on the user work stations is installed. According to the user policy on exploring means of computer technologies and software of the University (AMU Rule - 10), the base complex includes license software (hereinafter – SW) necessary to provide work ability of MCT.

2.5.3.3. Productive use of applied SW, external data medium that is not a part of the base complex is regulated by ITD with agreement of the chief, coordinating connection, computerization and telecommunication matters.

2.5.4. Protection against illegal data copying

2.5.4.1. Service and other protected information that is processed and stored in information systems of the University is to be copied and transported to the third person only after allowance of the rector with consent of the chief coordinating connection, computerization and telecommunication matters according to the user policy on the use of means of computer technologies and software of the University (AMU Rule - 10).

2.5.4.2. For copying and transporting service and other protected information to the third person without permission, users are brought to disciplinary responsibility.

2.5.6. Protection of the information, displayed on the monitor of means of computer technologies

2.5.6.1. Protection is implemented by limited physical access to sources of displayed information, prohibition of watching displayed information by the third person, according the user policy on exploring means of computer technologies and software of the University (AMU Rule - 10).

2.5.7. Protection against rogue programs, viruses.

2.5.7.1. To protect against rogue programs and viruses at the University, programs with "strong immunity" are used, they are protected against non-authorized modification, special program analyzers, implementing constant control of defection forming in the sphere of applied program products, periodical check of possible influences of virus activities, as well as incoming control of new programs before using them.

2.5.7.2. Organization measures are explained in the Rules on anti-virus protection of computers and servers (AMU Rule - 11), rules of connection and use of Internet resources (AMU Rule - 12) and rules of working with electronic mail (AMU Rule -13).

2.5.8. Protection against stealing information media

2.5.8.1. There is a certain rule of storage and use of information media at the University, according the user policy on exploring means of computer technologies and software of the University (AMU Rule - 10).

2.5.8.2. When transporting digital information media to re-use outside the University, they are cleaned in order to prevent unauthorized sharing of protected data.

2.5.9. Protection of information in the means of computer technologies

2.5.9.1. Particular University employees are responsible for each MCT. On MCT a system of authorization or/and authentication of workers, working on it is used. Transferring MCT to the use of another person is implemented by the permission of the department chief. Necessary program technical sources of storing information that is processed on MCT are received.

2.5.10. Protection against intentional information modification

2.5.10.1. Except the means of permitted access to MCT, protection of information from modification is implemented by program, technical and organizational measures. In order to detect in time the shown intrusions, history list of acts of operators and administrators are used.

2.5.11. Protection against errors in hardware-software means

2.5.11.1 In order to check the workability, before being placed in operation, program products and hardware means are to be tested in the conditions as close as possible to real. Unusable software and hardware means are not to be exploited.

2.5.12. Protection against incompetent use, setting or lawless cutting out of protection means

2.5.12.1. CDTN protection means are used and exploited according to the settled regime. ITD controls this process providing information security.

2.5.12.2. Maintenance of the University servers is implemented by ITD.

2.5.12.3. When breaking regime, appropriate employees are brought to responsibility in accordance with the law of the Republic of Kazakhstan.

2.5.13. Protection of computer technologies means from intrusion of workability or intrusion of software, hardware and information resources

2.5.13.1. As a result of accidents, natural disasters or other unexpected situations there might be a break of MCT workability, destroying of hardware, and software and information resources at the University. In these cases appropriate protecting measures are implemented, according to the plan to provide continuous functioning of the information systems of the University.

2.5.14 Protection against wrong information insertion

2.5.14.1. Data, being inserted into appendices are checked by program and technical sources in order to guarantee their correctness and appropriate use. Information insertion is carried out by responsible for it personnel.

2.5.15. Measures to protect communicative sources

2.5.15.1. Basic and extra communication services are separated from each other in appropriate way in order not to be under similar risks according to the plan to provide continuous functioning of the information systems of the University, Rule of reserved copying of information (AMU Rule - 14).

2.5.16. Protection against illegal connection to corporate data transmission network

2.5.16.1. Protection of communication from illegal connection except the sources of sanctioned electronic and physical access is provided by program, technical sources and organization measures.

Necessary measures are held to find out and to prevent in time illegal actions of people to get access to communication. In the case of illegal connection and attempt to use illegally communication lines and net equipment, people are brought to responsibility in accordance with the legislation of the Republic of Kazakhstan.

2.5.17. Protection against net equipment damage, wrong function, partial or full failure

2.5.17.1. Damage, wrong function, partial or full failure of the University’s equipment can be first of all as a result of accidents, natural disasters, and other emergency situations.

2.5.17.2. There University takes measures connected with involving protection sources, which will be used in the case of natural disasters (fires, water floods and earth quakes) and other emergency situations.

2.5.17.3. The plan to provide continuous work and recover is worked out according to the plan to provide continuous activity of the University’s information systems.

2.5.18 Protection against illegal switching on/off the equipment

2.5.18.1. Net equipment of the University’s CDTN is used and exploited according to the settled regime. Switching on and off the equipment is made by responsible technique personnel with the agreement of ITD and the head responsible for connection, computerization and telecommunication matters.

2.5.19 Protection against illegal modification of transmitted data, technical and service information

2.5.19.1. Except the means of legal access to communication sources and net equipment, protection of transmitted data from modification is implemented by program-technical and organization measures.

2.5.20 Measures to protect archiving system

2.5.20.1. The order of backing up, storing and recovering of program products and information systems is prescribed. Storage of backup copies is placed into specially equipped room according to the plan of providing continuous information systems. Authorized access to the storage backup copies is provided to recover information and information systems in time in cases of damage, accidents or other emergency situations.

2.5.20.2. The plan to provide continuous functioning of information systems is worked out, where also the measures to protect achieves in case of accidents, natural disasters and other emergency situations are prescribed, according to the rule of information backing up (AMU Rule - 14).

2.5.21. Other information protection measures

2.5.21.1. It is necessary to take full measures of information protection on all storage devices when giving MCT for repairing to outside organizations.

2.5.22. Review of Information security regulation

2.5.22.1. Compliance with the requirements of Information security regulation is obligatory for all the University information system users. Implementation of planned information security audit is one of the best methods of checking effective measures to protect information. Audit result can be the basis to review of several Regulation points and to make necessary corrections in it.

2.5.22.2. Audit of information security of University is necessary to spend annually. As a result of SIT and main specialist of information secure there must be spent review of statement for coincidence of demands, in case it is necessary to make changes and additions.

3. Revision, amending, storage and distribution

3.1. Revision, amending, storage and distribution of this University Regulation are implemented according to the University standard requirements “Document management” (AMU-US-02).

3.2. The original of this University Regulation is registered and stored in the Quality Management department.

3.3. The scanned version of this University Regulation is put on server of general access.

3.4. Copies of present Statement are delivered to all University structural branches.

Chief of information technologies department **A. Maralov**

Agreement sheet

№	Position	Name	Agree date	sign
1	Vice-rector for education activity	G.A. Zhaksylykova	18.05.2012г	
2	Vice-rector for scientific and clinical activities	F.A. Galitskiy	21.05.2012.	
3	Vice-rector for educational and social activities	G.Z. Khairli	22.05.12	
4	Vice-rector for administrative and economic activities	M.O. Nurzhaubay	19.05.12	
5	Head of department of cadre work and legal providing	B.A. Syzdykov	16.05.2012г.	
6	Chief of quality management and strategic planning department	Z.S. Zhumasheva	15.05.12г	
7	Chief of legal department	O.S. Ustinovich	14.05.2012.	

Amendments sheet

№	Sheet (page) numbers				Total number of sheets	The number of chapter, subchapter, standard point with changes	The signature of the person who makes amendments	Amendment date
	changed	replaced	new	annulled				

Acknowledgement sheet

№	Position	Name	Acknowledgement date	Signature