Managing Council of
NAZARBAYEV UNIVERSITY

Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University" and its organizations

Version*	Authorized by decision of Managing Council*		Date of entering into force
	Decision	Approval date	
Status	□ Approved □ Approved subject to amendments (please, see the Abstract of the Minutes) □ Rejected □ Other_____		
Reference to the main documents (higher level), which served as the basis for development of the document	Security policy of the autonomous organization of education "Nazarbayev University" approved by decision of the Executive Council dated 25/04/14, #4.4.1		
Responsible Officer	Lonsdale Anne, Provost		
Contact Officer – initiator of the document	Gaukhar Yelemessovna Upusheva, General Director, Nazarbayev University Library and IT Services PE; +7(7172) 70 65 78; administration_nulits@nu.edu.kz		
Previous/overage documents	-		
Related documents	-		
Document language	*Kazakh -* *, Russian. - , English. -*		

1. General provisions

1. Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University" and its organizations (hereinafter – "Regulation") has been developed in accordance with the legislation of the Republic of Kazakhstan, including:

1) Law of the Republic of Kazakhstan "On personal data and its protection" (hereinafter – "Law");

2) Labor Code of the Republic of Kazakhstan;

3) Law of the Republic of Kazakhstan "On informational support";

4) Decree of the Government of the Republic of Kazakhstan "On approval of Regulation on drawing up by an owner and (or) operator a list of required personal data for performing tasks";

5) National Standard of the Republic of Kazakhstan ISO/IEC 27001-2008. "Information Technology. Protection tools of information security management system";

6) National Standard of the Republic of Kazakhstan ISO/IEC 17799-2006. "Information Technology. Security policy tools";

and in accordance with the internal documents of the University and Organizations.

2. Requirements of the Regulation shall be applied to all employees and students of the University and Organizations.

The following definitions and abbreviations are used in the Regulation:

1)	**University**	– the autonomous organization of education "Nazarbayev University";
2)	**NULITS**	– Nazarbayev University Library and IT Services private entity;
3)	**Operator**	– an operator of database containing personal data in accordance with the Law, an employee of any structural unit of the University or Organization collecting, processing and protecting personal data specified in Annex 6 to the Regulation;
4)	**Person**	– an employee or student of the University or Organization, or any other person entering into relation with the University or Organization, who is an owner of particular personal data;
5)	**Personal data**	– information relating to a certain person or a person determined based on such data, who is an owner of personal data, recorded using electronic, paper and (or) any other physical media, in information and telecommunications networks and any other information systems;
6)	**Helpdesk**	– IT Service of NULITS providing technical user support (one stop shop automated service to receive, record and process users requests concerning any failures in hardware, software, computer network of the University and Organizations, required equipment and IT services requests);
7)	**Department of Information Security**	– a structural division of NULITS responsible for information security control in information systems and technologies;
8)	**Student**	– a person taking courses under any educational programs of the University or Organizations;
9)	**Applicant**	– a person applying to any educational program of the University or Organizations;
10)	**Organization**	– non-profit organizations founded by the University and their subsidiaries.

2. Aims and objectives

3. The aim of the present Regulation is to ensure compliance with the legislation of the Republic of Kazakhstan while collecting, processing and protecting personal data in the University and Organizations;

4. The objectives of the present Regulation are as follows:

1) determining guideline principles in personal data processing;

2) determining terms of personal data processing and ways to protect them;

3) determining rights, duties and responsibilities for collection and processing of personal data.

5. The University and Organizations collect and process personal data provided by the following category of Persons:

1) employees of the University or Organizations;

2) applicants;

3) students of the University or Organizations;

4) other persons whose personal data is processed within University or Organizations activity.

6. Personal data processed by the University and Organizations is contained on the following media:

1) paper;

2) electronic media;

3) information and telecommunications networks and information systems;

7. The University and Organizations shall apply the following methods for personal data processing:

1) without using automated equipment;

2) combined processing (using computing hardware);

3) automated processing of personal data.

3. Collection and processing of personal data

8. Collection and processing of personal data in the University and its organizations must be implemented only on the material and technical means of the University and its organizations, , in order to:

1) monitor employees vacations and benefits in case of temporary incapacity to work ;

2) keep records and manage study process, professional development and labor indicators;

3) ensure educational process, cultural advancement of students and employees;

4) keep records, identify and provide access to premises/buildings/offices/ information systems by issuing ID cards and creating accounts in the manner and in accordance with restrictions stipulated by the internal documents of the University and Organizations;

5) verify conformity and eligibility of employees and students, including identity and background check;

6) provide advanced selection of employees and students to be involved in educational, social, cultural and sports activities of the University and Organizations;

7) control payments and functions related to maintaining payroll record, bursaries and grants;

8) monitor maternity leave and payment schedules;

9) manage and maintain safe working and learning environment;

10) collect proposals on changing the internal documents of the University and Organizations;

11) monitor compliance with the principles of equality, generally accepted ethics, rights and freedoms of a person;

12) share information including that for consideration and (or) provision of responses to requests, proposals, recommendations, instructions of a Person (and/or any third persons), sending (receipt of) correspondence (mail) to a Person's address (to individual's address representing a Person), sending (delivery)/receipt via delivery service and express delivery, etc.;

13) record information materials provided to a Person including information about services rendered by the University and Organizations, and other notifications sent via telephone, fax and other communication channels, including insecure communication channels (SMS, E- mail, fax, etc.);

14) collect statistics and official reports in accordance with the internal documents of the University and Organizations;

15) for any other purposes which might be established by the legislation of the Republic of Kazakhstan.

9. List of required personal data for performing tasks by the University and Organizations (hereinafter – "Personal data list") is specified in Annex 1 hereto.

10. Collection and processing of employee's personal data shall be performed upon signing by a Person of consent for personal data processing as specified in Annex 2 hereto.

11. Collection and processing of student's personal data shall be performed upon completion of application by a Person adopted by the University and Organizations and signing of consent for personal data processing as specified in Annex 3 hereto.

12. In the event of entering into services agreement with an individual, the services agreement shall contain provisions stipulating personal data use of such individual and his/her consent to use his/her personal data.

13. If a Person giving his/her consent is under age, the consent for personal data processing shall be signed by his/her legal representative (guardian).

14. A Person's permission to collect and process his/her personal data is not required in cases stipulated by the law.

15. Based on the received information about a Person, the Operator records required information (personal data) about a Person in the information system, database.

16. Operators performing works directly associated with the education process of a current academic year shall have access to personal data of a Person after signing by the University of the relevant order on students enrollment to current academic year courses and only to the extent related to their work.

17. Personal data shall be stored within the period set out by internal documents and procedures of the University and Organizations.

18. Personal data placed on paper and removable storage media with barcode labels shall be filed in archive upon expiration of the storage period as prescribed in the internal documents of the University and Organizations.

19. Personal data, stored on media, embedded in hardware, information and telecommunication networks, databases of Operators' information systems, shall be destroyed upon expiration of the storage period based on a decision of the University's Expert Committee, which was established in accordance with the order of Executive Vice President of the University. .

20. Personal data while being processed without using automated equipment is revised by updating or modifying data presented on physical storage media, and if it is not feasible by technical features of the physical storage media, it shall be performed by making notes on the same physical storage media about amending personal data, or by creation of new physical media with updated personal data.

21. Part of personal data shall be destroyed or impersonalized, if feasible, to avoid further processing of personal data, but with possibility to process other data recorded on physical media (removal, cancellation).

22. If personal data cannot be destroyed, the Operator shall lock out or take necessary measures to impersonalize personal data.

23. While collecting and processing personal data, executive officers of the University and Organizations shall fully comply with this Regulation and their job descriptions.

4. Personal data protection

24. While processing personal data, the Operator shall ensure:

1) confidentiality of personal data;
2) proper storage conditions of personal data to prevent any loss or unauthorized access;
3) storage of physical media in office premises, filing-cabinets, safe boxes (storage) with protected and controlled access;
4) using only designated sections (folders) of media embedded in hardware or removable storage media with barcode labels;
5) prevention of any unauthorized removal of equipment from premises, as well as removal, installation or setup of software by any employees who are not authorized to do so;
6) elimination of any physical effect on hardware of an automated processing of personal data which could disrupt their functioning;
7) constant use of antivirus software to detect the infected files and immediate restoration of personal data modified or destroyed due to unauthorized access to them.

25. Computers with personal data files shall be protected by individual passwords in accordance with the password policy adopted by the University and Organizations.

26. Employees shall not use computers containing personal data without a password or use other person's password, or common (similar) passwords.

27. In the event if any failure of software or hardware is detected, employees shall send a request to HelpDesk in compliance with the rules adopted by the University and Organizations.

28. Information systems used for personal data processing shall be set up in accordance with Annex 4 hereto.

29. Potential threats and their effects during processing personal data in information systems and taken measures shall be determined by Department of Information Security and set out as specified in Annex 5 hereto.

30. NULITS takes all reasonable efforts to protect personal data contained in information systems, including:

1) antivirus protection;
2) technical support of infrastructure;
3) telecommunication management;
4) server support;
5) available back-up equipment;
6) software and hardware support and IT development;
7) daily monitoring and services analysis;
8) data back-up;
9) applying encryption-based safeguards;
10) intrusion and attack detection tools;
11) virtual infrastructure protection tools;
12) applying digital signature;
13) log and record keeping;
14) central access management to information systems.

31. When Operators process personal data in information systems as specified in Annex 4, Department of Information Security shall ensure:

1) training of persons to use information security product properly;
2) keeping record of persons allowed to process personal data, rights and access passwords;
3) keeping record of information security products, their operating and technical manual;
4) control over adherence to specifications of using information security products provided by operating and technical manual;
5) description of personal data protection system.

5. Responsibilities and duties of the parties

32. The University and Organizations shall arrange required organizational activities for protecting personal data.

33. Head of a relevant structural division shall be responsible for arranging collection and processing of personal data of each structural division of the University and Organizations in accordance with the Regulation requirements.

34. If there is a query from the Subject of personal data or his/her legal representative, the University and its organizations must inform the Subject or representative about the availability of personal data and provide an opportunity for them to examine the data.

35. Head of a structural division which process personal data shall:

1) determine storage place of personal data (physical storage media);

2) provide within the structural division conditions to ensure safety of personal data and prevent unauthorized access to them;

3) inform persons processing personal data of the List of personal data and adopted rules for their processing by structural division.

4) ensure safety of physical storage media with a Person's personal data, his/her consent for personal data processing in offices, filing-cabinets, safe boxes (storage) with protected and controlled access.

5) manage collection, processing and storage of personal data of a Person in information systems and server rooms.

36. Each officer of a structural division involved in personal data processing in accordance with his/her position descriptions shall bear responsibility for collection and processing of personal data.

37. The Operators shall:

1) comply with the present Regulation requirements;

2) support relevant information systems in accordance with Annex 4;

3) ensure integrity and reliability of information during collection and processing personal data both on paper media and in filling of databases;

4) ensure confidentiality while processing personal data;

5) constantly check and update antivirus tools set up on computers.

38. Employees involved in personal data processing shall report immediately to his/her supervisor, and (or) Information security service about any revealed facts of obtaining by any third parties unauthorized access or attempts to access to personal data, any loss or lack of media containing personal data, licenses, permits, safe boxes (storage) keys, electronic keys and other facts that may lead to unauthorized access to personal data, as well as the reasons and circumstances of possible leak of such information.

39. Employees involved in personal data processing shall be guided by "clear desk policy" and control personal access to a computer.

40. Employees shall not create or store database with personal data without approval of a direct supervisor.

41. Employees involved in personal data processing shall not transfer any information verbally or in written to any third person, unless such information is given for the purposes of structural division in accordance with the regulation of structural division and position description of an employee.

42. Administrators providing software and hardware support of information systems shall:

1) timely perform scheduled maintenance;

2) take required technical measures to protect data;

3) timely take data back-up measures;

4) daily monitor information systems;

5) monitor network resources;

6) keep fault records;

43. Information security service shall:

1) monitor activity related to personal data protection;

2) annually inspect business processes related to collection, processing and protection of personal data;

3) keep records of incidents related to information security;

4) consult and conduct official investigations related to personal data protection;

5) control access to personal data information systems.

44. Persons related to personal data shall:

1) provide Operators with reliable personal data;

2) inform an Operator timely at least within 30 days of any changes in information or personal data;

45. Persons who fail to comply with the present Regulation governing collection, processing and protection of personal data shall bare disciplinary responsibility in accordance with the internal documents of the University and Organizations, and legislation of the Republic of Kazakhstan.

46. Any disputes arising during collection, processing and protection of personal data shall be settled in accordance with the legislation of the Republic of Kazakhstan and internal documents of the University and Organizations.

6. Final provisions

47. The Regulation is subject to revision, if the legislation relating to personal data protection is amended, or due to change in organizational structures and adoption of a new technology or other mechanisms and procedures requiring revision of the Regulation.

Annex 1
to the Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University"

List of required personal data for performing tasks in the autonomous organization of education "Nazarbayev University"

Ser. No.	Personal data
1.	Surname
2.	Name
3.	Patronym (if any)
4.	Information about change of surname, name and patronym
5.	Transcription of name and surname
6.	Birth information: Date of birth; Place of birth
7.	Nationality
8.	Sex
9.	Marital status information: Marriage status; Marriage Certificate details; Divorce certificate details; Spouse's full name; Spouse's identification document details; Qualification; Full names and birth dates, place of work, place of study, residence address, cellphone and office telephone number of other family members, dependents; Children (if any) and their age
10.	Citizenship (former citizenship)
11.	Social status
12.	Number, series and issue date of employment record book
13.	Professional experience: Title/position, structural division, organization; Total and continuous work experience; Addresses and telephones, names of previous employers with indication of positions taken
14.	Information about education, qualification and expertise or special training: Date of enrollment (expulsion); Series, number, issue date of diploma, certificate, general diploma or any other document certifying graduation from educational institution; Name and location of educational institution; School, department, qualification and major obtained upon graduation from the educational institution; Academic degree; Academic title; Foreign language skills
15.	Information about career development and refresher training: Series, number, issue date of professional development certificate or refresher training; Name and location of educational institution; Qualification and profession obtained upon graduation from the educational institution
16.	Residence address, address of registration

17.	Contact phone
18.	E-mail
19.	Individual Identification Number (IIN)
20.	Portrait image on paper as well as digitized photography
21.	ID details: Name of the document; Number of the document; Issue date of the document; Validity of the document; Issuing authority
22.	Details of medical examination
23.	Military service details of persons bond to military service and persons subject to military service: Series, number, issue date (exchange) of military service card; Name of authority issuing military service card; Military occupational specialty; Military grade; Details of registration/deregistration; Grounds for exemption from military service
24.	Details of state and departmental awards, honorary and special ranks, merits, certificates; Name of award, rank or merit; Date and type of award statutory act or date of merit
25.	Information about persons eligible for alimony (separate maintenance)
26.	Parents'/ guardians' occupation.
27.	Details of extracurricular activities and work experience
28.	Portrait image on paper as well as digitized photography for ID Card issuance

Full name_____ Signature_____
Date_____

Annex 2
to the Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University"

To_____
From Full name_____
ID, passport
No._____Date_____
Issuing authority _____

Consent
for employee's personal data processing

To comply with the Labor Code and the Law of the Republic of Kazakhstan "*On personal data protection"* Employee gives to Employer:_____, located at 53 Kabanbay Batyr ave., Yessil district, Astana (hereinafter – "Employer") permission for collection (including from third parties), processing, usage, storage of personal data recorded in soft and hard copy, and (or) other physical storage media which may contain (including, but not limited to):

1. Information necessary for proper identification

- Full name, transcription of name and surname.
- Information about change of surname, name and patronym.
- Birth information: place of birth, date of birth, nationality, sex.

Marital status details: marriage status; Marriage Certificate details; divorce certificate details; spouse's full name; spouse's identification document details; qualification; full names and birth dates, place of work, place of study, residence address, cell phone and office phone numbers of other family members, dependents; children (if any) and their age.

- Citizenship (former citizenship).
- ID details: name of the document; number of the document; date of issue of the document; validity of the document; issuing authority.
- Individual Identification Number (IIN)
- Portrait image on paper as well as digitized photography for ID card issuance

2. Information about education, professional activity, employment status

- Number, series, and date of issue of labor book.
- Information on professional experience for the present time: full name of title/position, structural division, organization; total and continuous length of service;
- Addresses, telephones and names of previous employers with indication of positions held.
- Information about education, qualification and expertise or professional development: date of enrollment (expulsion); series, number, issue date of diploma, certificate, general diploma or any other document certifying graduation from educational institution; name and location of educational institution; school and department, qualification, and major obtained upon graduation from the educational institution; academic degree; academic title; foreign language skills.
- Information about career development and refresher training: series, number, issue date of career development certificate or refresher training; name and location of educational institution; qualification and profession obtained at the educational institution.
- Details of state and departmental awards, honorary and special ranks, merits, certificates; name of award, rank or merit; date and type of award statutory act or date of merit.

3. Contact details

- Telephone numbers.
- E-mail addresses.
- Residence address, address reference.

4. Other data necessary for Employer

- Medical examination details.
- Military service details of persons bond to military service and persons subject to military service: series, number, date of issue (exchange) of military service card; name of authority issuing military service card; military occupational specialty; military grade; details of

registration/deregistration; grounds for exemption from military service.

– Information about persons eligible for alimony.

Information provided will be used in accordance with business activity of the Employer including but not limited to performance of the following activities:

1) control of vacations and benefits for temporary disability;
2) accounting and managing education, personal development and employment indicators;
3) accounting, identification and granting of access to premises/offices/buildings/information systems, ID card issuance, creating accounts in the manner and in accordance with restrictions established by Employer's internal documents;
4) information sharing including that for consideration and (or) provision of responses to applications, proposals, recommendations, instructions etc. of persons (and/or third parties), sending (receipt of) correspondence (mail) to a person's address (individual's address representing a person), sending (delivery)/receipt via delivery service and mail delivery, etc.;
5) providing a person any information materials including information about services rendered by Employer as well as other notifications sent via telephone, fax and other communication channels, including insecure communication channels (including SMS, E-mail, fax, etc.);
6) calculation of vacation days;
7) verification of conformity and eligibility for work including identity and background check;
8) control of payments and functions for maintaining payroll records;
9) control of maternity leave and payment scheme;
10) management and maintenance of the occupational health and safety;
11) for other purposes that might be established by legislation of the Republic of Kazakhstan.

Employee's consent:

I hereby give my permission to Employer to process and use my personal data for performing activities specified by Employer.

I give my consent for use of data (full name; position; office phone number; cell phone number; e-mail) in the phonebook within the framework of my.nu.edu.kz information portal work.

I am aware of the video surveillance conducted to ensure safety and security.

This Consent has been issued to Employer for the Employment Agreement validity period and is subject to cancellation upon submission of a written request.

Full name_____

Signature_____ Date_____

Annex 3
to the Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University"

To_____
From Full name_____
ID
No._____date_____
Issuing authority _____

Consent
for student's personal data processing

To comply with the Labor Code and the Law of the Republic of Kazakhstan "*On personal data protection"* Student gives to Employer:_____, located at 53 Kabanbay Batyr ave. , Yessil district, Astana (hereinafter – "Employer") permission for collection (including from third parties), processing, usage, storage of personal data recorded in soft and hard copy, and (or) other physical storage media which may contain (including, but not limited to):

1. Information necessary for proper identification

- Full name, transcription of name and surname.
- Information about change of surname, name and patronym.
- Birth information: place of birth, date of birth, nationality, sex.
- Citizenship.
- Immediate family members (parents, brothers, sisters, guardians), full name of relative; place of work; place of study; residence address; cell phone and office phone numbers;
- ID details: name of the document; number of the document; issue date of the document; validity of the document; issuing authority.
- Individual Identification Number (IIN)
- Portrait image on paper as well as digitized photography for ID card issuance

2. Information about education

- Information about education, qualification and expertise or special training: date of enrollment (expulsion); series, number, issue date of diploma, certificate, general diploma or any other document certifying graduation from educational institution; name and location of educational institution; school and department, qualification and major obtained upon graduation from the educational institution; academic degree; academic title; foreign language skills.

3. Contact details

- Phone numbers: home phone number, cell phone number and additional contact number in case of emergency.
- E-mail addresses.
- Residence address, address reference.

4. Other data necessary for University

- Social status.
- Military service details of persons bond to military service and persons subject to military service: series, number, date of issue (exchange) of military service card; name of authority issuing military service card; military occupational specialty; military grade; details of registration/deregistration; grounds for exemption from military service.
- Occupation of parents/guardians.
- Details of extracurricular activities and work experience

Information provided will be used in accordance with business activity of the University including but not limited to performance of the following targets and purposes:

1) accounting and managing education, personal development and progress indicators;

2) educational process provision, student's cultural development;

3) accounting, identification and granting of access to premises/offices/buildings/information systems, ID card issuance, creating accounts in the manner and in accordance with restrictions established by internal documents of the University and its Organizations;

4) information sharing including that for consideration and (or) provision of responses to requests, proposals, recommendations, instructions etc. of student (and/or third parties), sending (receipt) correspondence (mail) to Student's address (individual's address representing a Student), sending (delivery)/receipt via delivery service and mail delivery etc.;

5) provision of any information materials to students including information about services rendered by the University and its organizations as well as other notifications sent via telephone, fax and other communication channels, including insecure communication channels (SMS, e-mail, fax, etc.);

6) verification of conformity and eligibility for study including identity and background check;

7) control of payments (scholarship, grants) and schedule recording functions;

8) management and maintenance of occupational health and safety;

9) for other purposes that might be established by legislation of the Republic of Kazakhstan.

Student's consent:

I hereby give my permission to the University and its organizations to process and use my personal data for the purposes stated above.

I give my consent for use of data (full name; position; office phone number; cell phone number; e-mail) in the phonebook within the framework of my.nu.edu.kz information portal work.

I am aware of the video surveillance conducted to ensure safety and security.

This Consent has been issued to Employer for the validity period of Agreement on educational services provision and is subject to cancellation upon submission of a written request.

Full name _____

Signature_____ Date_____

Annex 4
to the Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University"

List of information systems processing pernonal data

No.	Name of system	Brief description of system	Operator of system	Technical support operator	Number of users	Backup and restore of different system components	
						Name of component Reservation methods Restore methods	Time spent for restore
1	**Admissions System**	Registration of applicants on portal, submission of application forms, processing of applicant data by members of Admission Committee	Admissions Department	NULITS	18, 000 and more applicants including members of Admission Committee	Oracle Data Base, DB2, LDAP Database, application server. Oracle - Rman, on a daily basis. DB2 – built-in functions, reservation, on a daily basis. LDAP - built-in functions, reservation, on a daily basis. Application server - cloning, on a weekly basis.	20-60 minutes for database restore, 15-45 minutes for LDAP restore. Restoring from clone takes 4-8 hours.
2	**1C UPP System**	System for keeping accounting, tax and personnel record, salary calculation, registration of students, scholarship calculation, money management, receipt of financial, restricted and management accounting.	Financial and economic divisions, Human Resources Departments	NULITS	170 and more users	Microsoft SQL Server 2008 R2 Database. Database archivation by means of 1C – on a daily basis. Application server, Database server - cloning, on a weekly basis.	20-60 minutes for database restore. Restoring from clone takes 4-8 hours.
3	**Registrar's Office System**	Individual class and examination schedule review, review of current progress during semeter, total academic period. Allocation of grades of faculty	Registrar's Office	NULITS	5000 and more students 200 and more faculty members	MySQL database, application server MySQL Dump, zipping in TAR file, on a daily basis, application of MySQL Dump, unzipping from TAR file	15-30 minutes for database restore, 5-10 minutes for unzipping of reserve archive
4	**Moodle System**	Creation of Learning Resources and organization of learning activity	Schools of the University	NULITS	3500 and more including students, faculty members and	Oracle database, application server. Oracle Rman, on a daily basis. Application server, copying of files before changing.	20-60 minutes for database restore, 10-20 minutes for restore from copy

					international partners		
5	**CRM System**	Maintenance of database of candidates planning to enter master's programme of the University, to be a member, to pass probation, etc.	Graduate Admissions Department of the University	NULITS	20 and more	Oracle Data Base, DB2, LDAP Database, application server. Oracle - Rman, on a daily basis. DB2 – built-in functions, reservation, on a daily basis. LDAP - built-in functions, reservation, on a daily basis. Application server - cloning, on a weekly basis.	20-60 minutes for database restore, 15-45 minutes for LDAP restore. Restoring from clone takes 4-8 hours.
6	**ID card Management System**	Control management system for access to area and premises of the University. ID card preparation.	USM PE	USM	3 administrators More than 7000 ID card users.	SQL 2008 database. Database copy on a semi-monthly basis	2 hours and more
7	**ESUP**	Registration data, management of registration data, accounting records, and users' access to information resources of the University by providing transfer of unique information to target systems	NULITS	NULITS	3 administrators More than 7000 users.	Database – MS SQL Server 2008 R2 (differential backup – on a daily basis, full – on a monthly basis); Application servers are to be backuped by Windows Server Backup in-built means of Windows Server 2008 R2 on a daily basis(totally OS), and by VMware VSphere snapshots as well.	24 hours and more

Annex 5
to the Regulation for collection, processing and protection of personal data in the autonomous organization of education "Nazarbayev University"

Types of threats and measures to take

No.	Type of threat	Probable consequences	Measures to take
1.	Network Traffic Analysis	Capturing of transmit data including users' identifying codes and passwords. Consequences: Identification by attacker of network services used in IC as well as some of their properties followed by their unavailability and breach of their confidentiality.	- Traffic coding; - Intrusion Prevention System (IPS) use; - Cryptographic security agent use; - Tracking and combating programs impeding or disrupting networks; - Control of network composition and structure arrangement.
2.	Network scanning	Definition of protocols, network service accessible ports, definition of creation procedures of connection IDs, active network services, users' identifying codes and passwords. Consequences: Identification by attacker of network structure and data flow direction.	- Use of fairvol and its resources to block unwanted addresses, blocking unused ports; - Network packet control; - Non-default ports use; - Use of bottleneck scanners with adviser; - Intrusion Prevention System (IPS) use; - Antivirus protection means
3.	Password detection threat	Action connected to unauthorized access obtaining. Consequences: Unauthorized access	- Password change once in 6 months; - Accounting records' activity control in log journals; - Regular movement relevancy of accounting records once in a month; - Storage of passwords in an encrypted form; - Use of complicated passwords in accordance with Password Protection Act; - Application of Security Policies for differentiation of rights of access to network sharable resources.
4.	Substitution of trusted network entity	Rerouting of messages, unauthorized change of routing and address data. Consequences: Unauthorized access to network recourses, false information attack. Violation of integrity, confidentiality, and accessibility of data transferred.	- Daily systems monitoring by administrators; - Routing of information flow within networked environment using distributed system on the basis of Cisco network hardware; - Use of network protocols with peer authentication; - Use of virtual channel.
5.	False network routing attack	Unauthorized change of routing and address data, analysis and modification of data transferred, false information attack.	- Routing of information flow within networked environment using distributed system on the basis of Cisco network hardware;

				- Use of network protocols with peer authentication, use of virtual channel; - Use of virtual infrastructure protection means.
6.	Implementation of false network object		Traffic capturing and viewing. Unauthorized access to network recourses, false information attack.	- Routing of information flow within networked environment using distributed system on the basis of Cisco network hardware; - Use of dual-sided multi-step authentication;
7.	Service denial	Partial run out of resources	Production threshing of communication channels of network devices. Consequences: Degradation of performance of server applications. Increase of time of information processing and decline of effectiveness of computing operations.	- Automatic update of software systems; - A full backup is performed once in two weeks, backup control; - Load distribution on servers; - Load distribution on network by Cisco hardware; - Control, update, increase of resources volume.
		Total run out of resources	Message passing failure due to lack of access to communication medium, connection establishment failure. Consequences: IC performance and processing stop.	- Preventive measures on operational stations upon demand; - Preventive measures on server once in a month; - Use of uninterruptible power system; - Load distribution on network by Cisco hardware;
		Violation of the logical consistency between attributes, data, and objects	Message passing failure due to lack of certain routing and address data. Impossibility to obtain service due to unauthorized modification of IDs, passwords, etc.	- monitoring and analysis of network logs and PE applications software.
		Use of errors in programs	Malfunction of network devices	- monitoring and activation of debug function in PE application software.
8.	Remote launch of applications	By mailing files containing destructive executable code, virus attack	Violation of integrity, confidentiality, and accessibility of data transferred.	- scanning of workstation computers for viruses and bookmarks; - antivirus protection, antivirus bases update; - means of detection and intrusion of attacks. - protection against unauthorized mass e-mailing.
		By server application' buffer overflow		- server status monitoring by administrators
		By using remote system control opportunities provided by hidden program and hardware bookmarks or used by authorized tools	System hidden control	- scanning of workstation computers for viruses and bookmarks; - monitoring and analysis of services. - traffic control and limitation in communication channels with other networks and Internet to prevent an authorized use of external communication channels resources.

Annex 6
to the Regulation for collection, processing and protection of personal data in the autonomous organization of education “Nazarbayev University”

Operators

Employees of the following Departments/Services of the University and Organizations are Operators for Regulation Purposes:

1) Admissions Department;
2) Graduate Admissions Department
3) Department of Student Affairs;
4) Registrar’s Office;
5) Human Resources Management Department;
6) Human Resources Departments of Entities;
7) NULITS IT Directorate;
8) Financial and economic divisions of University and Organizations;
9) Schools of University;
10) NULITS Library;
11) USM PE;
12) USM Astana, Low Current Safety Systems Service.