REGULATIONS

on the IT Service and Digital Infrastructure
of Jalal-Abad International University (JAIU)

1. General Provisions

1.1. These Regulations define the status, goals, objectives, functions, and responsibilities of the JAIU IT Service (hereinafter referred to as the "IT Service"), as well as the general principles for managing the University's digital infrastructure.

1.2. The IT Service (IT Department) is a structural unit **of the Academic and Information Department (AID)** of Jalal-Abad International University (hereinafter referred to as the AID) and is part of the unified system for managing the University's academic process and digital infrastructure:

1. the University's local area network;
2. server and cloud infrastructure;
3. automated information systems (including the eBilim LMS);
4. official web resources, email, and communication services;
5. computer labs, multimedia equipment, etc.

1.3. In its activities, the IT Service reports to the Head of the Academic Information Office and, on strategic issues of digital development, to the Vice Rector overseeing educational and information activities and digitalization. the legislation of the Kyrgyz Republic in the fields of education, communications, information, and personal data protection;

1. the Charter of JAIU;
2. The Regulations on the JAIU Education Quality Management System;
3. Regulations on the Organization of the Educational Process Using the Credit System;
4. local regulations on information security and personal data protection;
5. these Regulations.

1.4. JAIU's digital infrastructure is considered a key resource for ensuring the quality of educational programs, research activities, and university management.

2. Goals and Objectives of the IT Service

2.1. The objective of the IT Service is to ensure the stable, secure, and efficient operation of JAIU's digital infrastructure and to support educational, research, and administrative activities using modern information technologies.

2.2. Main tasks of the IT Service:

2.2.1. Planning, deployment, operation, and development of network, server, and software infrastructure.
2.2.2. Support and maintenance of the University's key information systems (LMS eBilim, automated learning management system, electronic registrar's office, electronic library, etc.).
2.2.3. Ensuring information security and the protection of personal data.
2.2.4. Providing technical support to users (faculty, students, and administrative staff) regarding the use of digital resources.
2.2.5. Participation in digital transformation projects and the implementation of innovative educational technologies (including artificial intelligence).
2.2.6. Maintaining records and servicing computer and network equipment, as well as multimedia equipment.

2.2.7. Providing IT support during preparation for internal and external accreditation of educational programs.

3. Structure and Management of the IT Department

3.1. The structure of the IT service is approved by the Rector of JAIUand may include:

1. the network infrastructure and server administration sector;
2. the information systems and databases support sector;
3. the technical support and equipment maintenance sector;
4. Web Development and Website Maintenance Division;
5. other units depending on the University's objectives.

3.2. The IT Service (IT Department) is organizationally part of the Educational and Information Department of JAIU. The Head of the Educational and Information Department oversees the overall coordination of the IT Service's activities.

3.3. The Head of the IT Service reports to the Educational and Information Department (in accordance with the management structure of JAIU) and is responsible for carrying out the tasks defined by these Regulations.

3.4. The functional duties of IT Service staff are defined by job descriptions approved by the Rector of JAIU.

4. The University's Digital Infrastructure

4.1. The digital infrastructure of JAIU includes:

1. the University's local area network (LAN, Wi-Fi);
2. servers (physical and virtual), data storage systems;
3. cloud services used by the University;
4. software suites and information systems (eBilim LMS, Academic Information System, electronic document management system, testing systems, electronic library, etc.);
5. the University's official website and its sub-sites;
6. corporate email and communication platforms;
7. computer labs, multimedia classrooms, and video conferencing systems;
8. data backup and recovery tools.

4.2. The architecture and configuration of the digital infrastructure are approved by the University administration upon recommendation by the IT Department.

4.3. The IT Department is responsible for maintaining up-to-date technical documentation on the digital infrastructure (network diagrams, list of servers and services, list of licenses, etc.).

5. Main Functions of the IT Department

5.1. Network and Server Infrastructure

IT Department:

5.1.1. Ensures the uninterrupted operation of the local network, access to the Internet, and internal resources.
5.1.2. Maintains the operational readiness of servers, data storage systems, and backup systems.

5.1.3. Provides network segmentation, access rights management, and basic protection against external and internal threats (firewall, antivirus, traffic filtering, etc.).
5.1.4. Organizes monitoring of the load and availability of key services.

5.2. Information Systems Support

IT Department:

5.2.1. Provides technical support for the eBilim LMS and other automated information systems (updates, backups, troubleshooting).
5.2.2. Participates in the implementation of new modules and integrations (e.g., linking eBilim with the electronic dean's office, library, testing systems, etc.).
5.2.3. In collaboration with functional departments (Academic Affairs Office, Quality Department, deans' offices, library), participates in developing requirements for information systems.
5.2.4. Provides technical support to users regarding system operation (in terms of IT expertise).

5.3. Technical Support and Equipment Maintenance

IT Department:

5.3.1. Provides maintenance and repair of computer hardware, peripheral devices, network, and multimedia equipment.
5.3.2. Installs, updates, and configures software in accordance with the University's licensing policy.
5.3.3. Maintains records of IT equipment and licenses (inventory, equipment movement).
5.3.4. Participates in planning the renewal and modernization of the equipment fleet.

5.4. Web Resources and Digital Communication

IT Department:

5.4.1. Ensures the technical operation of the University's official website and related services.
5.4.2. Provides technical support for corporate email and, where available, other communication platforms.
5.4.3. In collaboration with the responsible departments, ensures compliance with web resource accessibility and security requirements.

6. Information Security and Data Protection

6.1. The IT Department ensures a basic level of information security for the University within its scope of authority, including:

1. implementing technical measures to protect against malware, unauthorized access, and data leaks;
2. organizing backups of mission-critical systems and data;
3. participation in the development and implementation of local regulations on personal data protection and information security.

6.2. The IT Department:

6.2.1. Organizes regular backups of data from key systems (LMS, AIS, electronic document management, accounting, etc.) and the storage of backup copies in accordance with established regulations.
6.2.2. Participates in the investigation of information security incidents and the development of measures to prevent them.
6.2.3. Conducts educational activities with users (basics of digital hygiene, safe use of email and the internet).

6.3. User access rights to information systems are determined by functional responsibilities and are formalized in regulations and orders (cooperation between the IT department, the Information Security Office, the HR department, etc.).

7. Interaction with departments and support for educational programs

7.1. The IT Department interacts:

1. with the Academic Information Department—on issues related to the AIS for the educational process, the eBilim LMS, schedules, electronic grade sheets, etc.;
2. with the Internal Monitoring and Quality Department – regarding the provision of digital monitoring tools, reporting, and evidence for accreditation;
3. with the library – regarding electronic resources, access to databases, and integration with the LMS;
4. with the academic offices and departments—regarding the equipping of classrooms and computer labs;
5. with the accounting department and the procurement department – regarding the purchase of IT equipment and software.

7.2. When preparing for external accreditation (NAAR, AOPO, etc.), the IT Department:

7.2.1. Provides information on the digital infrastructure, LMS, electronic resources, and services.
7.2.2. Ensures technical readiness (expert access to eBilim, demonstration of digital services, network stability, etc.).
7.2.3. Participates in the implementation of digitalization and quality improvement roadmaps.

8. Procedure for registering and processing requests (service support)

8.1. The University may use a unified service desk (ticket system) or another regulated mechanism for users to contact the IT department.

8.2. User requests may be submitted:

1. through a dedicated ticket system;
2. via the IT department’s corporate email;
3. through the designated representatives of the faculties/departments—in accordance with established procedures.

8.3. The request must include: full name, department, contact information, a brief description of the issue, location (office, building), and, if necessary, screenshots or files.

8.4. The IT Department:

1. registers requests;
2. classifies them by type and priority (critical, standard, scheduled work);
3. sets response and resolution deadlines in accordance with the regulations (see Appendix 1).

8.5. Information on the request status (accepted, in progress, completed, requires further work) must be available to the user (via the request system or email feedback).

9. Monitoring and Evaluation of IT Service Performance

9.1. Key performance indicators (KPIs) may be used to evaluate the effectiveness of IT service operations, including:

1. response time for critical and standard requests;
2. the percentage of requests resolved within the specified timeframe;
3. uptime of key services;
4. user satisfaction (surveys of faculty and students);
5. the percentage of updated hardware and software.

9.2. The IT Department prepares an annual report on its work and proposals for the development of the digital infrastructure, which is submitted to the Vice Rector and the Quality Council.

9.3. Monitoring results are used for:

1. planning the IT development budget;
2. adjusting operational regulations;
3. preparing for program accreditation and institutional accreditation.

10. Funding and Development of Digital Infrastructure

10.1. The IT Service is funded by:

1. funds from the Founder and the University budget;
2. extrabudgetary funds (additional services, projects, grants);
3. targeted programs and grants aimed at digitalization.

10.2. Areas of development:

1. upgrading and modernizing network infrastructure and server equipment;
2. development of the eBilim LMS and integration with other systems;
3. implementation of solutions based on artificial intelligence and data analytics;
4. expanding the use of digital educational resources, simulation, and distance learning technologies.

11. Final Provisions

11.1. These Regulations are approved by the Rector of JAIU and enter into force upon signing.

11.2. Amendments and additions to these Regulations shall be made at the initiative of the Rector, Vice Rectors, the Head of the IT Service, and the Department of Internal Monitoring and Quality, and shall be approved by order of the Rector.

11.3. These Regulations may be presented in Russian, Kyrgyz, and English. In the event of any discrepancy in interpretation, the version specified in the Charter of JAIU shall prevail.

Appendix 1

Regulations for Processing IT Requests

Appendix 1
to the Regulations on the IT Service and Digital Infrastructure of JAIU

1. Purpose and Scope

1.1. These Regulations establish the procedure for registering, classifying, and processing requests (IT requests) from structural units, faculty, students, and staff of JAIU submitted to the IT Service (IT Department of the University Information Office).
1.2. These Regulations apply to all types of requests related to the operation of the University's digital infrastructure, software, and hardware.

2. Channels for Submitting Requests

2.1. IT requests are accepted through the following channels:

1. specialized request system (if available) / internal "IT Support" service;
2. the IT Service's corporate email: _____;
3. the IT representative from the faculty/department (if such a procedure is established).

2.2. Verbal requests (by phone or in person) must be recorded by an IT service employee in the prescribed form if follow-up support is required.

3. Required details of a request

3.1. Each request must contain:

1. Applicant's full name;
2. department, position/status (faculty member, student, administrative staff);
3. contact information (phone number, email);
4. a brief and clear description of the problem or request;
5. location of the problem (building, lecture hall, office, computer lab);
6. if necessary – attachments (screenshot, error file, etc.).

3.2. If key information is missing (contact details, problem description), the IT department reserves the right to request clarification before processing the request.

4. Classification of Requests and Priorities

4.1. Requests are divided into categories:

1. **A. Critical (highest priority):**
   – eBilim LMS, the Academic Information System (AIS), or the University website is unavailable;
   – widespread network outage (no Internet in the building/on campus);
   – server failure affecting the academic process or accreditation activities.
2. **B. High priority:**
   – Computer lab malfunction during an exam/OSCE/test;
   – problems with access to email or key resources for a group of users;
   – issues with displaying grades/schedules in eBilim/AIS.
3. **C. Standard priority:**
   – a malfunctioning projector, individual computer, or peripheral device;

– software installation/updates on workstations;
– creation/modification of user accounts.

4. **D. Scheduled maintenance:**
– equipment upgrades, maintenance, and updates;
– Implementation of new services;
– data migration, etc.

4.2. Target response and resolution times:

Priority	Examples	Response time*	Target resolution time*
A	LMS, network, or server outage	up to 30 minutes	Up to 4 hours (if possible)
B	Computer lab, email, or eBilim failure	up to 2 hours	up to 1 business day
C	General technical issues	up to 1 business day	Up to 3 business days
D	Scheduled maintenance	To be agreed upon in advance	according to the agreed schedule

* Response time – from the moment the request is registered in the system/log.

5. Request Processing Procedure

5.1. An IT service employee registers the request, assigns it a unique number, category, and priority.
5.2. The request is assigned to the responsible person (or team), who:

1. clarifies the details (if necessary);
2. takes steps to resolve the issue;
3. if necessary, coordinates access/downtime with the department.

5.3. Upon completion of the work:

1. the operator records the result and closure time in the system (log);
2. a notification is sent to the requester (email/system/message).

5.4. If the issue cannot be resolved within the standard timeframe:

1. the request is set to "extended" status, with the reason and a new estimated timeframe indicated;
2. the priority may be revised in consultation with the requester and the head of the UIO.

6. Responsibility and Oversight

6.1. The IT Department is responsible for:

1. timely registration and processing of requests;
2. maintaining statistics (number of requests, resolution time, percentage of critical issues, etc.);
3. analyzing recurring issues and preparing proposals for their prevention.

6.2. The University administration and the UIO use these statistics to evaluate the effectiveness of the IT Service and to plan the development of the digital infrastructure.

Appendix 2

Minimum requirements for digital equipment in lecture halls and computer labs

Appendix 2
to the Regulations on the IT Service and Digital Infrastructure of JAIU

1. General Provisions

1.1. This Appendix establishes the minimum requirements for the digital equipment of JAIU lecture halls and computer labs in order to ensure a modern educational process and meet accreditation criteria.
1.2. Specific parameters (models, specifications) are determined based on the budget, but must not fall below the established minimum functional requirements.

2. Lecture Halls

For a standard lecture hall, the following is provided:

1. a teacher's computer/laptop with Internet access;
2. a multimedia projector or interactive whiteboard;
3. a screen (or projection surface) of sufficient size;
4. a sound system (speakers) if necessary;
5. power outlets and connection points (including for the instructor's devices);
6. stable access to the eBilim LMS, presentation materials, and video resources.

Recommended:

1. a spare HDMI/VGA cable and adapters;
2. Wi-Fi connectivity for demonstrating online resources.

3. Seminar and lab classrooms

Minimum requirements:

1. instructor's computer/laptop with network access;
2. if necessary – a projector or large monitor for displaying materials;
3. Student access to Wi-Fi for using eBilim and electronic resources.

For practical IT and analytics classes, see the requirements for computer labs.

4. Computer Labs

For educational computer labs (IT, medical informatics, testing, OSCE stations on PCs, etc.):

1. student workstations: the number of computers must be at least equal to the number of students in the group (or at least meet the established ratio—for example, 1 PC per 2 students, unless the course requires otherwise);
2. Specifications (minimum):
   – up-to-date operating system (licensed);
   – sufficient RAM and processing power to run the required software;
   – connection to the local network and the Internet;
3. a teacher's computer with class administrator privileges (control, screen sharing, etc., if such software is available);

4. educational software installed in accordance with course requirements (office suites, specialized software, clinical simulators, programming environments, etc.);
5. antivirus software with regular updates;
6. uninterruptible power supplies (UPS) for critical equipment—as needed.

5. Specialized classrooms and simulation centers

For specialized medical, engineering, and simulation spaces:

1. workstations for controlling simulators/training devices;
2. integration with audio and video systems (for recording and skill analysis);
3. access to digital simulators and 3D platforms (e.g., Complete Anatomy);
4. secure storage of training video materials.

Specific requirements are set forth in separate regulations governing the simulation center / specialized laboratories.

6. Responsibility and updating of requirements

6.1. The IT Department, in collaboration with the Academic Affairs Office, the deans' offices, and the Quality Department:

1. monitor compliance of actual equipment with established requirements;
2. prepares proposals for modernization and procurement.

6.2. This Appendix shall be reviewed at least once every 3 years or in the event of significant changes in educational technologies and standards.

Appendix 3

List of Major Information Systems and Digital Services at JAIU

Appendix 3
to the Regulations on the IT Service and Digital Infrastructure of JAIU

Template document: to be completed and updated annually by the IT Service and the Academic Affairs Office.

LIST
of Major Information Systems and Digital Services
of Jalal-Abad International University (JAIU)

No.	Name of system/service	Purpose (academic process / administration / research)	Primary owner (department)	Person in charge (Full name, position)	Brief description of functionality	Integrations (what it is connected to)
1	LMS "eBilim"	Learning process, independent study, assessment	UIO		Online courses, syllabi, tests, journals, reporting	Learning Management System, library
2	Educational Process Management System / Online Registrar's Office	Academic process management, student body, grades	UIO		Curricula, student body, orders, reports, rankings	eBilim, HR system
3	University's official website (jaiu.kg)	External communications, prospective students, accreditation	PR Department / Academic Affairs Office / IT Department		Structure, news, academic programs, documents, English/Russian/Kyrgyz versions	—
4	Electronic library / EBS	Information resources, textbooks, journals	Library		Full-text publications, database access	eBilim (links in courses)
5	Plagiarism detection system	Academic integrity monitoring	UIO / Quality Department / Library		Checking student and faculty work, reports	—
6	Corporate email	Communications	IT Department		@jaiu.kg email addresses	—
7	Video conferencing platform (if available)	Online classes, meetings, webinars	UIO / IT Department		Hosting online events	eBilim (links, integration)
8	Other specialized systems	By field (medicine, IT, finance, etc.)	Relevant department			

Below:

Person responsible for maintaining the List:
Head of IT Services: _____ /Full Name, Signature/

Approved by:
Head of the UIO: _____ /Full Name, Signature/

Date of update: **“___”_____20**

Appendix 4

Data Backup and Recovery Policy

Appendix 4
to the Regulations on the IT Service and Digital Infrastructure of JAIU

1. Purpose and Scope

1.1. This Policy defines the principles and procedures for data backup and recovery in JAIU's information systems to minimize the risk of data loss and ensure the continuity of the University's operations.
1.2. This Policy applies to all key information systems and servers managed by the IT Service.

2. Backup Objects

2.1. The following are subject to mandatory backup:

1. the LMS eBilim database;
2. databases of the Academic Information System (AIS) for the educational process and the electronic registrar's office;
3. library system databases and the electronic catalog;
4. data from electronic document management and accounting systems;
5. server and service configuration files;
6. other critical data identified by the IT Department in consultation with the Academic Affairs Office and University administration.

2.2. The list of backup objects is maintained by the IT Department and updated annually.

3. Frequency and Types of Backups

3.1. The following types of backups are used:

1. **full backup** – copying all data of the selected object;
2. **incremental** backup – copying only the data that has changed since the last backup.

3.2. Recommended schedule (can be adapted to your resources):

1. full backup of mission-critical databases – at least once a week;
2. incremental backup – daily (outside of peak hours);
3. separate monthly full backup (long-term storage).

3.3. The backup start time should be chosen to minimize disruption to users (e.g., late evening/night).

4. Backup Storage

4.1. Backups are stored:

1. on separate disk arrays/a backup server within the local infrastructure;
2. if possible, on external media or in secure cloud storage (off-site copy).

4.2. Retention periods:

1. operational backups (daily/weekly) – at least 1 month;
2. monthly/quarterly backups – at least 6–12 months (the specific duration is determined locally).

4.3. Access to backup copies is restricted to authorized IT personnel; all restoration and deletion operations are logged.

5. Data Recovery

5.1. Data recovery is performed:

1. upon the occurrence of an incident (failure, database corruption, unauthorized changes);
2. upon a documented request from an authorized person (Head of the IT Department, Head of the Division).

5.2. Recovery procedure:

1. analysis of the cause of the incident;
2. selection of the most recent and complete backup;
3. creation of a temporary test environment (in the event of serious incidents);
4. data recovery and integrity verification;
5. restoring the system to operational mode.

5.3. In the event of serious incidents (loss of a significant amount of data, compromise), a report is prepared describing the causes, the extent of the loss, and the measures taken.

6. Testing of backup procedures

6.1. At least once a year, the IT department conducts a test data recovery from backups based on pre-selected scenarios.
6.2. Based on the test results, a brief report is prepared with conclusions and, if necessary, recommendations for improving the procedures.

7. Responsibility

7.1. The head of the IT department is responsible for organizing and overseeing the implementation of this Policy.
7.2. Failure to comply with data backup and storage requirements is considered a breach of official duties and may result in disciplinary action in accordance with local regulations of JAIU.

CHANGE LOG

Change No.	Basis for Amendment	Pages	Summary of the amendment	Revision	Signature	Date
1						
2						
3						

Edition:

Effective date: “ ” _____ 20

APPROVAL SHEET

№	Position / Role	Full Name	Signature	Date
1	Developed by	Kanetova D.E.		29.12.25
2	Approved: head of the responsible department	Ташиева Т.С		29.12.25
3	Approved: Head of the Educational and Informational Department	Kanetova D.E.		29.12.25
4	Approved: leading specialist for quality	Kalmuratova A.		29.12.25
4	Approved: head of the legal affairs and human resources department / lawyer	Sydykova B.J.		29.12.25
5	Approved: vice-rector for academic affairs	Sadyrova N.A.		29.12.25
6	Approved: vice-rector for science, SR and GE	Asilova Z.A.		29.12.25
7	Endorsed / considered in the established manner	JASU Scientific Council		29.12.25.