I CONFIRM:

Rector of the nongovernmental educational institution "Termez University of Economics and Service"

_____A.E. Absamatov

10.10.2022

PERSONAL DATA PROTECTION AND PRIVACY POLICY

1. Purpose and scope

- This Policy establishes the principles and procedures for the lawful, fair, transparent and secure processing of personal data by Termez University of Economics and Service (TUES).
- It applies to all personal data processed by the University in relation to education, employment, admissions, research, student support, financial administration, library services, online learning, communications, partnerships, campus safety and other legitimate institutional activities.
- The Policy applies to university leaders, academic staff, administrative staff, students, applicants, alumni, contractors, service providers, partners, visitors and any other individual whose personal data are processed by or for TUES.

2. Legal and institutional basis

- TUES applies this Policy in accordance with the legislation of the Republic of Uzbekistan regulating personal data and data processing, including the relevant national regulatory acts on personal data processing and their amendments.
- Where TUES enters into international cooperation, contract, grant or mobility activities, the University will consider additional contractual and legal requirements applicable to the transfer and protection of personal data.

3. Principles of personal-data processing

- Lawfulness, fairness and transparency: Personal data shall be processed on a lawful basis and in a manner that is understandable to the data subject.
- Purpose limitation: Data shall be collected and used only for specified academic, administrative, legal, employment, service or contractual purposes.
- Data minimization and accuracy: TUES shall process only the data that are relevant and necessary for the stated purpose and shall take reasonable steps to keep data accurate.
- Retention limitation: Personal data shall not be retained longer than necessary, except where a longer period is required by law, archival obligations or legitimate institutional needs.
- Integrity and confidentiality: TUES shall apply appropriate organisational and technical measures to protect data from unauthorised access, disclosure, alteration, loss or destruction.
- Accountability: Units and persons processing personal data shall be able to demonstrate compliance with this Policy and applicable legal requirements.

4. Categories, purposes and lawful processing

- TUES may process identity, contact, educational, academic-progress, attendance, assessment, employment, payment, scholarship, library, access-control, research-participation, communications and support-service information when necessary for legitimate university functions.
- Sensitive or special-category information, including health-related information, shall be processed only when required by law, necessary for an authorised university service, supported by an appropriate legal basis or provided with valid consent where required.
- Personal data shall not be used for unrelated purposes unless the data subject is informed and a lawful basis exists.

5. Rights of data subjects

- Data subjects may submit requests regarding access to their personal data, correction of inaccurate or incomplete information, clarification of processing purposes, restriction or objection to processing where applicable, and deletion where permitted by law.
- Requests may be submitted to the Legal Service or through the relevant responsible university unit. TUES shall assess each request promptly, document the outcome and respond in accordance with applicable law and institutional procedure.
- Where a request cannot be fully granted, TUES shall provide an explanation where legally appropriate.

6. Consent, notices and communications

- Where consent is required, TUES shall obtain consent that is informed, specific, recorded and capable of being withdrawn in accordance with applicable law.

- Privacy notices shall state the categories of data processed, the purpose of processing, relevant retention rules, data-subject contact routes and the available rights procedures.
- Digital forms and platforms that collect personal data shall use clear notices and shall not request more information than is reasonably necessary for the service.

7. Security and access management

- TUES shall maintain organisational and technical controls appropriate to the nature of the data and the systems used. These include account-based access control, role-appropriate access, credential protection, controlled administrative privileges, secure system configuration, access review and incident documentation.
- University users must protect their passwords, avoid sharing credentials, use trusted devices and networks, report suspected phishing or unauthorised access, and follow approved rules for use of TUES systems.
- Digital systems in scope include the Student Portal, HEMIS Teacher, LMS, Digital Library, TISU Bot and the Sustainability Learning Platform, together with other systems processing personal data on behalf of TUES.

8. Personal-data incidents and breach response

- Any suspected personal-data incident, including unauthorised access, accidental disclosure, loss of a device, phishing compromise, malware infection or improper transfer of data, must be reported without delay to the responsible IT contact and the Legal Service.
- The responsible units shall contain the incident, assess the affected data and individuals, document the event, identify corrective actions and notify competent authorities or affected persons when required by law.
- Lessons from incidents and near misses shall be used to improve procedures, training and technical controls.

9. Roles and responsibilities

- The Legal Service coordinates legal review of this Policy, provides guidance on legal compliance, supports handling of data-subject requests and maintains the policy review record.
- The IT unit and system administrators implement practical technical and administrative safeguards within the systems they manage.
- All university employees, students and other users are responsible for respecting this Policy, using personal data only for authorised purposes and reporting suspected violations.

10. Awareness, monitoring and review

- TUES shall provide awareness activities on cyber hygiene, safe use of digital systems, password protection, phishing awareness, privacy and responsible handling of personal information.
- This Policy shall be reviewed at least annually, and earlier where there is a significant change in law, technology, institutional systems, data-processing activities or identified risk.
- The University shall document improvement actions arising from legal updates, internal monitoring, user feedback, audits, incidents and awareness activities.