Pannon Egyetem
University of Pannonia

INFORMATION TECHNOLOGY REGULATION OF THE UNIVERSITY OF PANNONIA

Adopted by the Senate on: 30th October 2025
Senate Resolution number: 170/2025.(X.30.)
Effective date: 10th November 2025
Person responsible for the maintenance of this Regulation: Director of the Directorate of Information Technology
Version number: 00

version number	date of publication	effective date	date of repeal	Senate Resolution number, Board of Trustees Resolution number*
00	10.11.2025	10.11.2025	-	Senate Resolution No. 170/2025. (X.30.)

* if the entry into force of the Regulation is subject to adoption by the Board of Trustees

Table of Contents

I. GENERAL PROVISIONS 6
1. § The scope of the Regulation 6
2. § Legal and internal regulatory background 6
3. § Definitions 7
4. § The general IT management of the University, responsibilities of the DIT 9
5. § System Administrators' Board 9
II. THE IT SYSTEM OF THE UNIVERSITY OF PANNONIA 10
6. § The structure and services of the IT system of the University of Pannonia 10
III. SECURITY CLASSIFICATION OF THE UNIVERSITY'S INFORMATION SYSTEMS 11
7. § Development of security categories 11
IV. SYSTEM OPERATION ACTIVITIES, CLASSIFICATION OF USERS 12
8. § Server systems 12
9. § Operating client-side equipment 12
10. § Developing service level-based IT user categories 14
V. THE DEFINITION OF SAFE IT USE 14
11. § Requirements for safe use 14
12. § Requirements for secure electronic communication 15
12/A. § Provisions applicable to Users employed by the University 15
12/B. § Provisions applicable to Users not employed by the University (Partners) 16
12/C. § Provisions applicable to Users engaged under a service contract 17
VI. HOW TO REQUEST IT SUPPORT 18
13. § Use of a central electronic technical support management system 18
14. § Obligation to report errors 19
15. § Troubleshooting, how to resolve a technical support request, documentation 20
VII. CHANGES TO THE IT INFRASTRUCTURE 20
16. § Relocation, development, upgrading, modification 20
VIII. RIGHTS AND OBLIGATIONS OF USERS 22
17. § User rights 22
18. § Obligations of users 22
19. § Provisions on keeping contacts through IT devices and the use of equipment 22
IX. DEVELOPMENT OF APPLICATIONS 25
20. § General provisions on the development of applications 25
X. COMPLIANCE WITH THE REGULATION, SANCTIONS 26

21. § Sanctions on Users 26
XI. PROCEDURES AND RECOMMENDATIONS AT THE LEVEL OF INSTITUTIONS AND ORGANISATIONAL UNITS 27
22. § IT standards and procedures 27
23. § List of IT recommendations 28
XII. IMPLEMENTATING PROVISIONS OF THE INFORMATION TECHNOLOGY REGULATION OF THE UNIVERSITY OF PANNONIA 28
24. § Entry into force 28

The Information Technology Regulation of the University of Pannonia (hereinafter referred to as the "**Regulation**") issued by the University of Pannonia (hereinafter referred to as the "**University**") on the basis of the University's Organisational and Operational Rules (hereinafter referred to as the "**OOR**"), Part I Organisational and Operational Rules of Procedure (hereinafter referred to as the "**OORP**") approved by the Senate of the University of Pannonia and adopted by the Foundation for the University of Pannonia acting as the operator exercising founders' and ownership rights (hereinafter referred to as the "**Operator**") and on the basis of the resolution by the Board of Trustees on the rules of procedure for adopting the regulations of the University of Pannonia by the Board of Trustees is as follows:

PREAMBLE

The University is committed to providing its staff with guaranteed quality access to its IT network and the services it provides, by building and maintaining a stable and efficient IT infrastructure.
The primary purpose of the Regulation is to define the tasks and responsibilities related to the establishment, maintenance and development of services required to support the University's educational, research, development, scientific, administrative and cultural duties with IT tools, the conditions for the use of IT systems, and the expected user behaviour that does not compromise the smooth performance of basic duties.

In order to achieve these objectives, the Regulation ensures that the basic expectations required of IT system operators are set out, that IT security procedures and ISO-based recommendations are communicated to the appropriate audience and that the internal procedures of IT system operators are consistent with the Integrated Quality and Environmental Management Policy.
The Regulation also sets out the rights and obligations of University Users, the responsibilities of Users and system operators and the ways in which they may be sanctioned.

The Regulation sets out the basic requirements, however, it also ensures for IT system operators that regulations for users be developed, compliance be monitored and, where necessary, users be sanctioned in accordance with the Regulation.

I. GENERAL PROVISIONS

1. § The scope of the Regulation

(1) The personal scope of the Regulation shall extend to all organisational units and employees of the University, whether employed or engaged in any other legal relationship with the aim of providing work, as well as to the students of the University who come into contact with any University IT property of any kind. It also extends to any third party to whom the University provides access to any of the University's IT systems or IT assets (hereinafter referred to as "Partners").

(2) The personal scope of this Regulation shall also extend to General Users and Key Users (see definitions).

(3) The material scope of this Regulation shall extend to all IT equipment and assets included in the University's inventory and the data stored in these systems, in particular:

a) all software and data bases,
b) all hardware,
c) infrastructures and network devices related to IT systems,
d) electronic or paper-based data and documents recorded or registered in or transmitted via IT systems.

2. § Legal and internal regulatory background

(1) The Information Technology Regulation has been developed with due regard to the following legislation and internal regulations:

a) Act CCIV of 2011 on National Higher Education ("NHE Act"),
b) Act LXIX of 2024 on the Cybersecurity of Hungary,
c) Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information,
d) Act V of 2013 on the Civil Code ("Civil Code"),
e) Act C of 2012 on the Criminal Code,
f) the Organisational and Operational Rules of the University of Pannonia,
g) Fire Safety Regulation,
h) Occupational Safety and Health Regulation,
i) Privacy and Data Protection Policy.

3. § Definitions

(1) For the purposes of this Regulation:

a) **User:** any employee, student or Partner of the University to whom the University provides any form of access to its IT system.

b) **General User**: any person who uses the University's IT system and devices within the framework of this Regulation with general user privileges.

c) **Key User**: a User who, in justified cases and in accordance with the procedure set out in Paragraphs (8) and (10) of Section 9 of this Regulation, is granted administrator privileges on a specified computer. In addition to the provisions of this Regulation, the Key User shall bear further responsibilities and obligations with regard to the device administered by them.

d) **Partner shall include in particular**:

da. any former employee retired from the University who continues to participate in the University's scientific, consultancy or outstanding community activities,

db. retired university professors holding the title of Professor Emeritus/Emerita of the University of Pannonia,

dc. any member of a research group maintained by the University of Pannonia who is not employed by, engaged under any contract for work by, or otherwise in a legal relationship with the University.

e) **IT System**: all IT devices listed in the University's inventory, including all hardware, software and databases.

f) **System Administrators' Board:** the body established at the University pursuant to Section 5 of this Regulation, intended to discuss issues relating to IT operation and development at the University.

g) **Training Location System Operator:** the organisational unit designated as a training location of the University which is responsible for the operation of the elements listed in Paragraph (1) of Section 6 of this Regulation relating to the given training location.

h) **Operational Requirement**: specifies the rules and guidelines to be followed during the operation of a given IT system element.

i) **Technical Database**: the database maintained and operated by the INI concerning the University's IT devices and IT licences, with the content specified in Paragraph (4) of Section 6 of this Regulation.

j) **Application Agent**: software running on suitable IT devices for the purpose of maintaining the technical database up to date, capable of collecting technical data and preparing software inventories.

k) **Multi-User Application**: software that may be used simultaneously by several users, typically with separate accounts and permissions, while data and functions remain jointly accessible.

l) **University Domain Server:** a server service that centrally manages user authentication, authorisations and access to resources.

m) **Central Endpoint Protection Management System**: a security solution enabling the centralised supervision, configuration and monitoring of the protection of devices connected to the network (endpoints), including the management of antivirus software, firewalls, intrusion prevention systems and device access rules.

n) **Applicant**: a User submitting a support request to the DIT.

o) **Electronic Support Management System**: a digital platform enabling the structured and automated registration, tracking and management of IT or customer service issues, requests and incidents.

p) **HBONE**: HUNGARNET Backbone, i.e. Hungary's academic network, operated by the Governmental Agency for IT Development.

q) **PRO-M:** one of the legal successors of the Governmental Agency for IT Development, providing comprehensive data network, content and Internet services for Hungarian higher education institutions and public institutions.

r) **NEPTUN UES:** the electronic student registration system of the University of Pannonia, the Unified Higher Education Study System.

s) **UNI-PANNON, *uni-pannon.hu*:** the website address of the University of Pannonia.

sz) **Incident Report:** reporting to the system operator of any actual or suspected malfunction or unusual event experienced during the use of an IT device. In the absence of network connectivity, prior notification may be given orally or in writing.

t) **System Operator/System Administrator:** responsible, on the basis of their job description, contract or temporary assignment, for ensuring the operability of the IT devices (hardware, software, network) registered in the inventory of the organisational unit(s) specified in their assignment and for user management within the institution.

u) **Abuse shall include, in particular,** the manipulation of another User's correspondence and the copying, transmission or deletion of personal data.

ü) **WiFi (Wireless Fidelity):** a standard wireless data transmission technology.

x) **Person Engaged in Research and Development Activity:** an employee actively participating or any other person engaged under contract in university research or IT development.
y) **Public Service:** a service which may be used not only by university users but also by others, with or without restrictions.

4. § The general IT management of the University, responsibilities of the DIT

(1) The IT regulatory, coordination and operational tasks relating to the University as a whole shall be performed by the Directorate of Information Technology (hereinafter referred to as the "DIT"). The DIT shall define and maintain the University's IT security policy.
(2) The DIT shall operate a website (hereinafter referred to as the "DIT Portal") on which it shall publish its contact details. The DIT website shall be accessible from the main portal of the University of Pannonia (https://uni-pannon.hu).
(3) The DIT shall establish procedures and policies relating to the operation or use of IT systems. The currently effective procedures and policies shall be published by the DIT on the DIT Knowledge Base portal.

5. § System Administrators' Board

(1) In addition to the employees of the University engaged in IT system operation or development, the System Administrators' Board shall consist of the heads of the Chancellor's Office and the Rector's Office. The Board shall be chaired by the Head of the DIT.
(2) The purpose of the System Administrators' Board is to provide a forum for regular dialogue among its members on matters relating to IT operation and development. Planned developments and modifications may thus be discussed and reviewed by the members of the Board.
(3) The Board shall hold meetings on a monthly basis. Minutes of the meetings shall be prepared and made electronically accessible to the members of the Board within two weeks from the date of the meeting.
(4) In addition to meetings, communication among the members shall primarily take place electronically.

II. THE IT SYSTEM OF THE UNIVERSITY OF PANNONIA

6. § The structure and services of the IT system of the University of Pannonia

(1) The University shall operate an IT infrastructure necessary for the performance of its activities. The components of this infrastructure include:
   (a) on-site internal network infrastructure and telephone network (PANNON-NET),
   (b) central server rooms and hosting devices (PANNON-DC),
   (c) client-side devices (workstations, portable computers, printers, multifunctional devices, telephones),
   (d) other IT tools,
   (e) core IT services,
   (f) other IT services.

(2) The design, development and operation of the systems referred to in points (a), (b) and (e) of Paragraph (1) above shall be carried out by the DIT.

(3) The planning, development and operation tasks relating to other IT devices and IT services shall be carried out by the DIT. The DIT may delegate this authority to the faculty system administrator or to the IT operations staff member responsible for the relevant training location.

(4) The operating procedures of each training location belonging to the University shall define the organisational unit which, as the system operator of the training location, is responsible for the operation of the elements listed in Paragraph (1) relating to that training location. The system operator of the training location shall perform his or her activities in accordance with the instructions and professional guidelines issued by the DIT. The Head of the DIT shall be involved in the IT planning and development processes relating to the training locations. The DIT shall maintain a technical database of the University's IT devices and IT licences. The following data shall be recorded in the database:
   (a) in the case of hardware devices:
      aa. the key technical specifications of the device
      ab. the date of commissioning
   (b) in the case of IT licences:
      ba. the subject matter of the licence
      bb. the number of licences
      bc. the type of licence (named-user, floating, etc.)
      bd. the validity period of the licence (start and end date)

be. the authorised group of users.

(5) In order to keep the technical database up-to-date, an application agent shall be used to collect technical data and create a software inventory on IT tools capable of running this agent. The User shall not interfere with the operation of the application and shall not remove it.

(6) Automated data collection from devices that are not capable of running the application agent shall be enabled via SNMP or other standard protocol.

(7) The University shall maintain a central user directory, which shall be used to implement central identity management. The DIT shall be responsible for this directory.

(8) Each User is assigned a Central Directory Identifier (hereinafter referred to as "CDI").

(9) Using the directory, the DIT provides an authentication service (IdP) via industry standard protocols.

(10) For all multi-user applications requiring user identification used at the University, identification should be done using the CDI, preferably via the central IdP.

III. SECURITY CLASSIFICATION OF THE UNIVERSITY'S INFORMATION SYSTEMS

7. § Development of security categories

(1) All IT systems intended to be installed or already in operation at the University shall be classified into a security category. This classification shall be carried out by the DIT.

(2) A classification process shall be carried out before the installation of a new IT system. The request for classification shall be initiated by the head of the organisational unit intending to install the IT system with the Head of the DIT.

(3) Security categories:

(a) Critical systems: systems that are critical to the operations of the University and cover all parts of the University. They include systems that contain internal or business information relating to the University and personal data, as well as IT systems that are essential to ensure the business continuity of the University. They are of high priority for use and operation. Regarding data protection, they require a high degree of protection.

(b) Priority systems: technical systems which are of high priority for the operations of the University, which are closely related to critical systems and to the operation of the University's core IT infrastructure and which are not typically used to store personal or business information.
(c) Normal systems: IT systems being in daily use, not falling under categories (a) or (b) above, not critical for the operations of the University or covering only certain organisational units of the University. Their temporary suspension of operation does not jeopardise the continuity of the University's operations and they are of secondary priority with respect to their use or operation.
(d) Other systems: IT systems which are used at the University and which are not included in categories (a) to (c) above.

IV. SYSTEM OPERATION ACTIVITIES, CLASSIFICATION OF USERS

8. § Server systems

(1) Server system: an IT system that provides a service to other IT systems or allows for the downloading of data stored on it or for the use of its resources.
(2) A critical or priority server system may only be operated by the DIT or with the permission of the DIT.
(3) The DIT shall be the operator of server systems with 'normal' and 'other' security rating. Deviations from this are only possible with the permission of the DIT. Commissioning must be preceded by an authorisation process.

9. § Operating client-side equipment

(1) Client-side equipment: IT devices with IT systems running on them which are used directly and managed independently by the client User.
(2) The DIT shall be responsible for the system operation tasks relating to the client-side devices of the Chancellor's organisation. Any deviation from this is only possible with the approval of the Head of the DIT.
(3) The system operation tasks of the client-side devices of the Rector's (academic) organisation shall be performed by the faculties and the non-faculty comprehensive organisational units and organisational units:
(a) within their own organisation, or
(b) by entrusting the system operators of the DIT with such tasks.

(4) The University's network telephone service and the related equipment shall be operated by the DIT.
(5) All client-side devices must be included in the DIT technical database.
(6) For each client-side device, the DIT or the relevant system operator of the University Centre shall carry out commissioning in accordance with the relevant policies.
(7) The organisational unit initiating the acquisition process may put the equipment into use after the conditions of Paragraphs (5) and (6) have been met.
(8) In order to perform operational tasks, client computers must be connected to the University domain server. By joining the domain, the DIT shall obtain administrator privileges. The DIT may delegate such privileges to the operator colleague of the relevant faculty/comprehensive organisational unit. Any deviation from this requirement shall require the permission of the Head of the DIT.
(9) Users may use client devices
  (a) only with restricted user privileges; any deviation from this shall require the permission of the Head of the DIT;
  (b) solely for work-related purposes; private use is not permitted.
(10) For research activities requiring a highly customised IT environment, the installation of bespoke software, specific software usage requirements or hardware intervention, the researcher may apply for administrator privileges on the computer used by them, subject to providing a detailed justification and the written support of the head of the organisational unit.
  (a) The granting of such privileges shall be decided by the Head of the DIT following prior professional consultation.
  (b) The privileges shall be granted personally and shall apply only to a specifically identified computer registered under a unique inventory number.
  (c) By accepting administrator privileges, the researcher acknowledges and accepts full responsibility for the stability, data security and operational functionality of the given device. In such cases, the DIT transfers responsibility to the researcher while continuing to provide the necessary technical support and guidance. This responsibility includes the secure handling of data, compliance with software licensing requirements, and adherence to security protocols.
  (d) The DIT may revoke such privileges with immediate effect where justified, if the use of the privileges does not comply with the requirements set out in this Regulation, in particular in cases of misuse,

improper operation or IT or data protection incidents. In all cases, the DIT shall endeavour to make its decision following careful consideration of the circumstances.

10. § Developing service level-based IT user categories

(1) Taking into account the services used by University Users and the roles or student responsibilities performed by them, the classification of Users into categories using the categories set out in Paragraph (3) shall be carried out by the organisational unit operating the relevant IT system, on the basis of the User's job description and/or contract concluded with the University, the existence of a student status relationship, and, in the case of Users not having a legal relationship with the University, on the basis of the activity performed in the interest of the University as indicated on the IT system access request form. In the case of Users performing multiple roles, more than one category may be assigned to the User. Such classification shall not affect the User's job description and shall not impose administrative duties on the organisational unit concerned; this step merely serves as the basis for registering users in the IT system and assigning the access rights necessary for the performance of their tasks.

(2) The organisational unit responsible for operation shall prepare an operating policy valid for the entire organisational unit. Based on this, it shall categorise the users of the IT system it operates and determine the rights and service level on the basis of these categories. The mandatory specifications of the organisational unit's operating policy shall be aligned with the Central IT Operators' and Service Providers' Rules issued by the DIT.

(3) IT user categories:
   (a) general user
   (b) key user.

V. THE DEFINITION OF SAFE IT USE

11. § Requirements for safe use

(1) The competent User shall be responsible for the proper use of the University's client-side equipment. In the event of improper use or operation, the University shall have the right to impose sanctions. When using client-side

equipment, the relevant provisions of the University's Fire Safety Regulation and its Occupational Safety and Health Regulation shall also be observed.

(2) The University's IT infrastructure provides the possibility to perform specific tasks in the Hungarian Academic Network (HBONE) – as a member institution of the PRO-M. The relevant provisions of the PRO-M AUP (Acceptable Use Policy) shall apply mutatis mutandis to University Users.

(3) The University's IT systems may only be used for the performance of tasks related to the User's job.

(4) All university client computers are required to have a central endpoint protection solution in place and to be included in the central endpoint protection management system. The management system is operated by the DIT. Any attempt to remove the endpoint protection solution is a violation of this Regulation. Network access to unprotected client computers may be terminated immediately, and the user and the head of the organisational unit shall be liable for any damage, loss or misuse of data on these client computers.

(5) Any deviation from Paragraph (4) is only possible with the prior written consent of the Head of the DIT.

(6) The Users shall ensure protection against unauthorised physical access and unauthorised logon to university client devices or shall report the lack of protection to the system operator.

(7) In the case of critical and priority systems, the head of the organisational unit responsible for operating such systems shall take the various aspects of business continuity of the university into account. The business continuity plan shall be laid down in the operating policy of the organisational unit responsible for operating the systems.

12. § Requirements for secure electronic communication

12/A. § Provisions applicable to Users employed by the University

(1) The DIT shall provide each university employee with an e-mail address in order to ensure that any communication by e-mail necessary for the employee's job-related duties is conducted using that e-mail address only. The e-mail addresses so created shall be used for work-related communication only and shall not be used for private purposes.

(2) The e-mail address is created and made available to employees by the DIT. E-mail addresses shall be based on a uniform nomenclature. The DIT shall be responsible for maintaining this nomenclature.

(3) Only the university e-mail address may be used for official communication between employees by e-mail.
(4) Work-related e-mail communication via a non-university private e-mail address is expressly prohibited.
(5) The manual or automated forwarding of e-mails received at a university e-mail address to a third party outside the organisation or to an external service provider is expressly prohibited, unless this activity is related to a workflow and is indispensable.
(6) It is expressly forbidden to process e-mails sent on behalf of a University employee from a non-university e-mail address.
(7) In the course of the communication, the provisions of the Privacy and Data Security Policy of the University of Pannonia shall also be taken into account.

12/B. § Provisions applicable to Users not employed by the University (Partners)

(1) The University may, upon request, provide a University e-mail address to Users who are not in an employment relationship, employment-related legal relationship, or any other legal relationship with the University, but who contribute through their activities to the work of the University community.
(2) Access to the e-mail address may be granted provided that the User concerned satisfies one of the following conditions:
    a) is a former employee retired from the University who continues to participate in the University's scientific, consultancy or community activities,
    b) is a retired university professor holding the title of Professor Emeritus/Emerita of the University,
    c) is a member of a research group maintained by the University who is not in an employment relationship, employment-related legal relationship, or any other legal relationship with the University.
(3) Procedure for submitting an application:
    a) Following completion of the application form constituting Annex 1 to this Regulation, the written request for establishing eligibility shall be justified by the head of the requesting faculty/comprehensive organisational unit/organisational unit linked with the User's activities, who shall then submit two copies thereof for the Rector's consent and subsequently for the Chancellor's approval.

b) Following the Rector's consent and the Chancellor's approval, the head of the requesting faculty/comprehensive organisational unit/organisational unit shall send one copy of the application form to the Head of the DIT, while the other copy shall remain with the faculty/comprehensive organisational unit/organisational unit. On the basis of the application form, the DIT shall take measures to provide the User with access to the e-mail address.

c) Access to the e-mail address shall be granted for a fixed term of no more than three years. Eligibility shall be reviewed annually, and following the expiry of access, an extension may be granted on the basis of a new application.

d) The provisions set out in Section 12/A of this Regulation shall apply mutatis mutandis to the use of e-mail addresses provided in this manner. The e-mail addresses concerned may be used exclusively for communication related to the tasks specified in the justification contained in the application form.

e) Prior to the use of the e-mail addresses, compliance with the University's IT, security, and data protection rules, as well as the signing of the confidentiality statement set out in Annex 2 to this Regulation, shall be mandatory.

f) The head of the requesting faculty/comprehensive organisational unit/organisational unit shall be obliged to notify the DIT without delay if the conditions of eligibility no longer exist (Annex 1, termination of e-mail address), or if any breach of the University's internal regulations is detected in connection with the use of the e-mail address.

g) The DIT shall be entitled to suspend or terminate access to the e-mail account with immediate effect if the eligibility conditions set out in Paragraph (2) of this Section cease to exist, or if the User fails to comply with obligations relating to adherence to the University's IT, security, or data protection regulations.

12/C. § Provisions applicable to Users engaged under a service contract

(1) The University may provide a university e-mail address, a Central Directory Identifier and access to the University's IT systems for the duration of the service contract.
(2) Access may only be granted to the extent necessary to enable the Contractor to perform their duties.
(3) Procedure for submitting an application
   a) Following signature of the service contract by both parties, the head of the organisational unit initiating the engagement shall request the creation of the necessary access rights by sending an electronic mail to the Directorate of Information Technology.
   b) The electronic mail shall contain the Contractor's full name, a list of the requested access rights, and the signed service contract, on which the service fee and other personal data may be redacted, but only to the extent that the identity of the Contractor remains identifiable. The duration of the engagement must in all cases remain visible.
(4) The DIT shall be entitled to suspend or terminate the Contractor's access rights with immediate effect if the entitlement forming the basis of such access ceases to exist, or if the User fails to comply with obligations relating to adherence to the University's IT, security or data protection regulations.

VI. HOW TO REQUEST IT SUPPORT

13. § Use of a central electronic technical support management system

(1) The DIT shall operate a central electronic registry application to record requests sent by Users for technical support and to track the entire lifecycle of such requests.
(2) Requests for technical support are received by the DIT by e-mail. The DIT staff shall contact the requester via the application by e-mail. The DIT shall publish the technical e-mail addresses created within the application on the DIT portal. Requests for technical support shall be sent to the technical e-mail addresses published there.
(3) Where it is not possible to request support by e-mail or in cases of urgency, the DIT will accept oral requests. In such a case, the requester shall be obliged to submit the request for technical support electronically afterwards, within a maximum of two working days, indicating the fact of the

previous oral communication in such a way that the DIT operators can unambiguously identify the communication.

(4) A request for technical support may only be made in relation to the University's IT equipment or systems.

(5) University employees shall send their requests from the e-mail address provided by the University.

(6) Students of the University shall send their requests from the e-mail address registered in the Neptun UES system.

(7) The University's Partners shall send their requests from the e-mail address they used when creating their Partner account.

(8) Organisational units implementing IT operations outside the DIT shall operate an electronic technical support management system and their users shall record technical support requests in these systems. The system operator shall consult the Head of the DIT on the design of the electronic technical support system. The head of the organisational unit shall be responsible for its implementation. User logon shall be implemented using the CDI. The DIT shall be granted access to the technical support system for consultation and reporting. The system shall be capable of producing statistical reports, case summaries, exports, implementing at least the following queries:
   (a) Listing of technical support cases (both open and closed),
   (b) Number of technical support cases per month, per year,
   (c) Individual export of technical support cases.

14. § Obligation to report errors

(1) The User shall report its requests for technical support and any abnormal events or IT equipment failures that it experiences to the DIT system operator or the competent system operators, and use the electronic technical support management system operated by the organisational unit concerned.

(2) The organisational unit acting as operator shall provide Users with the possibility to use the electronic technical support system.

(3) The organisational unit acting as operator shall set out the method of electronic error reporting and the procedure for resolving technical support requests in its operating policy.

(4) If the User suspects that their password has been disclosed to or obtained by an unauthorised person, they shall immediately notify the DIT and the competent organisational unit acting as operator and, if they can, they shall

immediately change or block their password with the competent service provider and shall cooperate with the DIT and the competent organisational unit acting as operator.

15. § Troubleshooting, how to resolve a technical support request, documentation

(1) System operators shall prioritise requests for technical support and fix any error without delay, and comply with requests for technical support to the best of their knowledge and ability.
(2) The communication between the system operator and the Users during the resolution of the request for technical support shall be recorded in the electronic technical support system.
(3) The User shall be granted access to the documentation of the technical support case.
(4) The User shall cooperate with the system operators on an ongoing basis to resolve the issue.

VII. CHANGES TO THE IT INFRASTRUCTURE

16. § Relocation, development, upgrading, modification

(1) Relocation or rearrangement between or within rooms affecting PANNON-NET may be carried out after prior notification to and approval by the DIT.
(2) Changes to the elements of the PANNON-NET may only be made by DIT system operators or by a contractor with the permission of the DIT.
(3) The head of the organisational unit shall be responsible in the event of a relocation:
    (a) The head of the organisational unit initiating the change shall notify the DIT system operator in writing of the change request at least 5 working days before the planned implementation date. The relocating organisational unit shall cooperate with the DIT and/or the administrator of the organisational unit acting as operator when carrying out tasks relating to the IT and telephone network infrastructure during implementation.
    (b) The administration of access rights, IT equipment and network access shall be carried out in accordance with the provisions of the Central IT Operators' and Service Providers' Rules.
(4) The head of the organisational unit shall be responsible for the following in the event of development or modification:

(a) In the event of a request for development or modification that would lead to a change in the structure or assets of the PANNON-NET (hereinafter collectively referred to as the "change request"), the head of the organisational unit initiating the request shall submit the change request in writing to the Head of the DIT. The means of implementing the change request shall be developed in cooperation. The implementation of the change request and the start of the procurement and the installation process shall only start after the written approval of the Head of the DIT has been obtained.

(b) The organisational unit initiating the request shall cooperate with the DIT and/or the administrator of the organisational unit acting as operator when carrying out tasks relating to the PANNON-NET infrastructure during implementation.

(c) The Head of DIT shall in each case be involved in the technical acceptance process for the implementation of the change request. It is the Head of the DIT that approves its commissioning and determines the steps to be taken.

(5) Responsibilities of the organisational unit acting as operator of the IT system:

The contractor or the head of the relevant organisational unit shall be responsible for any damage to cables and connectors caused by relocations, improvements, upgrading or modifications.

The authorised system operator shall assist the users of the organisational unit affected by the change in the modifications done to the PANNON-NET infrastructure and carry out the following tasks:

a) He or she shall delete old network settings and access rights existing for the configuration used by the given organisational unit, based on the official authorisation of the organisational unit.

b) Based on the official authorisation of the organisational unit, he or she shall
   - take part in the installation of the IT infrastructure to be used in the new location,
   - check the infrastructure,
   - make a list of the missing or damaged infrastructure elements and inform the heads of the relevant organisational units of this,
   - set system and task-specific rights,
   - configure the necessary equipment,
   - provide access to the systems to be used.

c) The costs of the necessary equipment and materials shall be borne by the organisational unit making the request.

VIII. RIGHTS AND OBLIGATIONS OF USERS

17. § User rights

(1) The aim of the University is to ensure that its IT infrastructure provides the PANNON-NET central IT services as set out in this Regulation to all University Users.

(2) The User shall have the right to

a) use the University's IT services corresponding to the access rights established on the basis of their job description, contract, any existing student status relationship, or activities carried out in the interest of the University, and to use such services for their intended purpose,

b) get the information necessary to use the IT infrastructure,

c) depending on his or her user classification, be informed about local user rules, the identity of the IT operators, together with their duties and responsibilities,

d) receive university information of public interest necessary for the performance of his or her duties.

18. § Obligations of users

(1) The User shall comply with the provisions of this Regulation applicable to the User and the related University IT procedures on the basis of the User's contract concluded with the University or his or her e-mail address provided by the University.

(2) In the case of irregular or unauthorised use, he or she shall cooperate during the IT audit (identification of irregularities, repair of damage) proposed by the Head of the DIT or the system operator and the head of his or her organisational unit and ordered by the Chancellor of the University.

19. § Provisions on keeping contacts through IT devices and the use of equipment

(1) General requirements for the use of electronic devices

(a) The use of IT equipment covered by the material scope of this Regulation may only be used for the activities specified in the Deed of Foundation of the University.
(b) Newly purchased university IT equipment shall be properly configured and protected by the competent system administrators, in particular with a firewall and a university endpoint protection application. The DIT shall be responsible only for the IT equipment it installs, configures and maintains.
(c) Users shall not install software on the University's IT equipment. Installation may only be carried out by the competent system administrator, unless the educational curriculum requires installation and installation takes place in the computer rooms of the faculty. Additional regulations may apply to the use of student computer rooms. These student computer room policies shall be developed by the organisational unit acting as operator and shall be included in the operating policies which shall be made available in the computer rooms. Any violation of the policy shall constitute a breach of this Regulation.
(d) Changes to the system files of university-owned IT devices are not allowed without the permission of the system administrator and the owner of the client computer (in this case, the user of the IT device).
(e) Users may not view, read, copy or delete the applications and files stored on the IT device used by any other University User without the consent of the owner (in this case, the user of the IT device).
(f) No applications that may compromise the operation of the University's IT infrastructure shall be used on university-owned IT equipment.
(g) No applications without a licence ensuring lawful use shall be installed on university-owned IT equipment.
(h) Users shall report any errors, incidents or damage experienced in the course of use as defined in this Regulation to the system operator in the form specified in the Regulation.
(i) In the event of a longer leave of absence, Users shall switch off the IT device they use and cut it off from the mains, provided that the function of the IT device makes this possible.

(2) Use of the Central Mail System:
(a) The primary purpose of electronic mail communication is the performance of university-related duties, the efficient support of tasks carried out in the interest of the University, and official communication.
(b) Users shall use shared resources as intended. Documents that are unnecessary or take up too much storage space (documents containing

images, presentations, large files), as well as e-mails shall be periodically saved and deleted.

(c) Users shall not compromise the University's mail system, in particular by opening, forwarding or replying to unsolicited e-mail.

(d) In the event of a prolonged leave of absence, Users shall ensure that an automatic reply is set up.

(3) Use of network devices, Internet, WiFi and Intranet (PANNON-NET, HBONE):

(a) Users may only use the IP address assigned to the university IT device they use. IP addresses are allocated and registered by the DIT. Changes to IP address configurations may only be made with the prior written permission of the DIT.

(b) Non-university IT devices that are capable of active communication with the University's network may only be connected to the University's network with the prior permission of the Head of the DIT. Written authorisations are issued by the Head of the DIT or the local network operator, in accordance with the Central IT Operators' and Service Providers' Rules.

(c) Non-university IT devices that are capable of active communication with the University's network may be connected to a wireless public network or a network requiring personal identification without any special authorisation (e.g. eduroam). This exception does not include password-protected (e.g. WPA2 PSK) networks established for organisational units.

(d) Users may operate a network hosting services on the IT device they use only with permission. Requests shall be submitted to the DIT on a valid Service Request Form (Central IT Operators' and Service Providers' Rules).

(e) Users should note that the primary purpose of using the University's Internet network is to facilitate University activities, and therefore Users shall carry out their study or work activities accordingly. Regarding, in particular, the use of IT labs (student computer rooms), User shall comply with the procedures applicable to student computer rooms.

(f) Users shall avoid websites with unsafe content, as the responsibility for any damage resulting from visiting such sites and the obligation to remedy the damage rest with Users.

(g) University computers shall not be used for private purposes that interfere with workplace activities. The performance of any activity or the launch of any service that uses the resources of the University's computer

infrastructure, endangers its operation and serves purposes other than the University's purposes shall not be permitted.

(h) The internal IT services of the University are subject to access authorisation, which authorisation is valid for the given User only and shall not be transferred. Access is granted by the DIT or the administrator of the organisational unit acting as operator on the basis of the User's job description or contract, or the Request Form constituting an annex to this Regulation.

(i) Users shall be responsible for all the data moved by them using the resources of the PANNON-NET.

(j) Users shall not disable network connections, network devices or devices providing network services, change settings or log on to the network device without authorisation.

(k) Users who are not system operators are prohibited from intercepting, decoding or modifying network packets, or from interfering with network traffic in any manner whatsoever. An exception shall apply to activities carried out within computer laboratories in connection with teaching activities on the network of the PC room.

(4) Data protection and security:

a) Information which can be obtained through user or system administrator privileges or which is collected by activity logging, traffic monitoring and with other IT tools may be used only to improve the functioning of the University’s IT system, to detect abnormal use and to detect violating behaviour. In the event of misuse of information, the procedures set out in this Regulation shall be applied.

b) Access rights to data shall be based on university job descriptions, contracts concluded with the University, the decision of the head of an organisational unit and the written recommendation of the designated professional user or key user (if any).

c) The protection of data on IT systems shall be designed in a way that it complies with the Privacy and Data Security Policy of the University.

IX. DEVELOPMENT OF APPLICATIONS

20. § General provisions on the development of applications

(1) The University may use its internal resources or engage external service providers to perform tasks related to the University's core and ancillary activities and to develop software, applications and IT systems to facilitate the performance of such tasks.

(2) In the preparatory phase of the development of software, applications and IT systems to be used at the University, as referred to in Paragraph (1), the intention to do so shall be notified to the Head of the DIT. A system design for the application shall be drawn up and it shall be approved by the Head of the DIT. The system design shall define the following as a minimum requirement:
   (a) the purpose of the application, a summary description,
   (b) the users,
   (c) connections to other systems,
   (d) data source requirements,
   (e) the data stored,
   (f) the technologies used,
   (g) the application architecture,
   (h) the planned date of commissioning,
   (i) the developers (employee, external developer),
   (j) the operators and contact persons of the system as planned.

(3) When an application or IT system is completed, its integration into the university system shall be authorised by the Head of the DIT.

X. COMPLIANCE WITH THE REGULATION, SANCTIONS

21. § Sanctions on Users

(1) The University will enforce the following sanctions based on the employment relationship.

(2) In the event of a suspected breach of the Regulation, the Head of the DIT shall have the right to start an investigation.

(3) The sanction for intentional, gross violation of the Regulation is temporary or permanent exclusion from the network services. The Head of the DIT shall notify the User and the head of the organisational unit of the exclusion in writing.

(4) If there is minor or unintentional violation of this Regulation, the User and the head of the organisational unit shall be informed of the improper use by the Head of the DIT in writing. If, after such notification, the User commits

the same violation again, the improper use shall be deemed to be intentional.

(5) Any misuse of the University's non-public data or IT infrastructure shall result in University proceedings depending on the manner in which it is committed. In the case of suspected violations of Act C of 2012 on the Criminal Code or other legislation, the Chancellor shall be informed so that the necessary measures can be taken.

(6) In the event of negligent or intentional damage, the User shall be liable to pay compensation depending on the extent of the damage, in accordance with the relevant provisions of Part II of the OOR (Employment Requirement System) and of Act V of 2013 on the Civil Code.

(7) For students, Part III of the OOR (Student Requirement System) shall apply.

XI. PROCEDURES AND RECOMMENDATIONS AT THE LEVEL OF INSTITUTIONS AND ORGANISATIONAL UNITS

22. § IT standards and procedures

(1) Regarding IT procedures at institutional level:
  (a) the DIT shall take part in their development and maintenance
  (b) the Head of the DIT shall be responsible for their development and maintenance.

(2) The Central IT Operators' and Service Providers' Procedures shall include the following:
  (a) Requirements for the operation of central IT systems
  (b) Roles, rights and obligations of system operators
  (c) IT change management
  (d) Other IT tasks
  (e) Business continuity plan
  (f) Use of student computer rooms and house rules for students
  (g) IT licence management
  (h) Sanctioning
  (i) Definitions
  (j) Final provisions.

(3) IT requirements at the level of organisational units:
  (a) Mandatory specifications to be developed by the organisational unit operating the IT system:

(a) a staff member of the organisational unit operating the IT system shall participate in their development and maintenance,
(b) the head of the organisational unit operating the IT system shall be responsible for their development, and
(c) the Head of the DIT shall provide professional assessment and shall approve them,
(d) The DIT shall develop recommendations on the specifications.

(4) The operating policy at training location or organisational unit level shall include:
(a) Requirements for the operation of information systems
(b) Responsibilities of system operators
(c) Use of student computer rooms and house rules for student
(d) Definitions
(e) Annexes, forms.

(5) User manuals for students, policies on the use of student computer rooms, guidelines.

23. § List of IT recommendations

(1) The DIT shall develop, maintain and make available on the University's website the following general University IT recommendations in an easily accessible form:
(a) IT Security Recommendations.

XII. IMPLEMENTATING PROVISIONS OF THE INFORMATION TECHNOLOGY REGULATION OF THE UNIVERSITY OF PANNONIA

24. § Entry into force

(1) This Regulation shall enter into force on 10th November 2025, following its adoption by the Senate.

(2) Upon the entry into force of this Regulation, the Regulation approved by Senate Resolution No. 217/2021 (XII.9.), as well as the Joint Directive No. 8/2025 (VIII.01.) of the Rector and the Chancellor on the procedure for granting e-mail access to Users not having a legal relationship with the University of Pannonia, shall be repealed.

(3) This Regulation was discussed by the Senate at its meeting held on 30th October 2025 and adopted by Senate Resolution No. 170/2025 (X.30.).

(4) Annexes to this Regulation:

Annex 1: Application Form for Requesting an E-mail Address for Users not Having a Legal Relationship with the University of Pannonia

Annex 2: Confidentiality Statement

Dated in Veszprém, on 30th October 2025

Dr. János Abonyi
Rector

Zsolt Csillag
Chancellor

Approved by

Approved on behalf of the Foundation for the University of Pannonia, as Operator:

Dated in Veszprém, on 7th November 2025

Dr. Péter Bartus
Executive Director