UNIVERSITY OF PANNONIA

INFORMATION TECHNOLOGY REGULATION OF THE UNIVERSITY OF PANNONIA

Approved by the Senate on: 9th December 2021
Senate Resolution number: 217/2021.(XII.9.)
Adopted by the Board of Trustees: 17th December 2021
Board of Trustees Resolution number: 86/2021 (12.17.)
Effective date: 1st January 2022
Person responsible for the maintenance of this Regulation: Head of the DDP Department of Information Technology

*The Information Technology Regulation of the University of Pannonia (hereinafter referred to as: “***Regulation***”) issued by the University of Pannonia (hereinafter referred to as: ”***University***”) on the basis of the University’s Organisational and Operational Rules (hereinafter referred to as: “***OOR***”), Part I Organisational and Operational Rules of Procedure (hereinafter referred to as: “***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: “***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:*

Table of Contents

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 Quality 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. § 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) For the purpose of this Regulation, User shall mean the persons listed in Section (1) above.

(3) The 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. § The University's general IT management

(1) The Department of Information Technology (hereinafter referred to as: "DIT") operated by the Directorate for Development and Projects (hereinafter referred to as: "DDP") shall be responsible for general University duties related to IT management, coordination and operation. It shall define and maintain the University's IT Security Policy.

(2) The DIT shall maintain a website (hereinafter referred to as: "DIT Portal"), on which it shall publish its contact details. The DIT website is accessible from the main University portal (https://uni-pannon.hu).

(3) The DIT shall define rules of procedure and policies for the operation or use of information technology systems. The DIT shall publish its currently valid policies and rules of procedure on the DIT Portal.

II. THE IT SYSTEM OF THE UNIVERSITY OF PANNONIA

3. § 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 paragraphs (a) and (b) of Section (1) above shall be carried out by the DIT.

(3) The DIT shall be responsible for the planning, development and operation of basic IT services.

(4) The operating policy of each training location belonging to the University shall define the organisational unit which, acting as system operator of the training location, is responsible for the operation of the components listed in Section (1) at the given training location. The system operator of the training location shall carry out its activities in accordance with the specifications and professional guidance of the DIT. The head of the DIT shall be involved in the IT design and development processes to be carried out at the location.

(5) The DIT shall maintain a technical database of the University's IT equipment and IT licences. The database shall include:

  (a) for hardware
    (a) the main technical characteristics of the device
    (b) the date of commissioning
  (b) for IT licences
    (a) the subject of the licence
    (b) the number of licences
    (c) the type of licence (named user licence, floating licence, etc.)

(d) the period of validity of the licence (start and end date)
(e) the eligible users

(6) 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.

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

(8) 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.

(9) Each User is assigned a Central Directory Identifier (hereinafter referred to as: “CDI”).

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

(11) 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

4. § 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, 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 parts of the University. Their temporary suspension of operation does not jeopardise the business continuity of the University 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

5. § 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.

6. § 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, except for the devices of the Directorate for Economic Affairs and the Technical and Operational Directory.
(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) All client-side devices must be included in the DIT technical database.
(5) 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.
(6) The organisational unit initiating the acquisition process may put the equipment into use after the conditions of Sections (4) and (5) have been met.

7. § Developing service level-based IT user categories

(1) Taking into account the services used by University Users and the roles performed by the Users or the students, the organisational unit operating the IT system concerned shall carry out the classification of Users, using the categories set out in Section (2), on the basis of the User's job description and/or the contract concluded with the University and the existing student status.
(2) In the case of a User with multiple roles, the User may be classified into more than one category. The classification does not affect the job description of the User and does not imply administrative tasks for the organisational unit concerned. This step only enables the registration of the User in the IT system and helps to set user rights necessary for the performance of the tasks.
(3) 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' Procedures issued by the DIT.

(4) IT user categories:
  (a) Internet user,
  (b) Intranet user,
  (c) user of an office application,
  (d) user of a library system,
  (e) user of an educational system,
  (f) user of educational software,
  (g) user of an economic system,
  (h) user of a management systems,
  (i) user of a senior executive system,
  (j) system operator,
  (k) a person carrying out research and development activities.

V. THE DEFINITION OF SAFE IT USE

8. § 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 GAID (Governmental Agency for IT Development). The relevant provisions of the GAID 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 antivirus solution in place and to be included in the central antivirus management system. The management system is operated by the DIT. Any attempt to remove the antivirus 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 Section (4) is only possible with the prior written consent of the Head of the DIT.

(6) Users using critical and priority systems 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.

9. § Requirements for secure electronic communication

(1) The University 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.

VI. HOW TO REQUEST IT SUPPORT

10. § 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 case.

(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 ETR 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) Average time to resolve technical support cases,
(d) Individual export of technical support cases.

11. § Obligation to report errors

(1) The User shall
 (a) 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
 (b) 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 his or her password has been disclose to or obtained by an unauthorised person, he or she shall immediately notify the DIT and the competent organisational unit acting as operator and, if he or she can, he or she shall immediately change or block his or her password with the competent service provider and shall cooperate with the DIT and the competent organisational unit acting as operator.

12. § 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

13. § 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' Procedures.

(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: "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, upgradings 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

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.

14. § User rights

(1) The User shall have the right to use the University's IT services according to his or her job description, contract or, if applicable, his or her student status, and to use them as intended,

(2) to get the information necessary to use the IT infrastructure,

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

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

15. § 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.

(2) In 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.

16. § Provisions on IT contacts 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 anti-virus 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 located in the student computer rooms. Installation may only be carried out by the competent system administrator, unless the educational curriculum requires installation. 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 prescribed 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 mailing is to ensure the smooth performance of university tasks and to maintain official contacts.

(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 and that their correspondence is redirected or forwarded.

(3) Use of network devices, Internet, WiFi, 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 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’ Procedures.

(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’ Procedures).

(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 launching of any service that uses the resources of the university computer infrastructure, endangers its operation and serves purposes other than the University's purposes are not permitted (based on the GAID AUP).

(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 on the basis of the User's job description or contract by the DIT or the administrator of the organisational unit acting as operator.

(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) It is forbidden for a non-system operator user to intercept, decrypt or modify network packets or to interfere with network traffic in any way.

(4) Data protection

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 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.

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).

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

17. § General provisions of 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 Section (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

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

18. § Sanctions on Users

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

(2) 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.

(3) 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.

(4) 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 the Criminal Code or other legislation, the Chancellor shall be informed so that the necessary measures can be taken.

(5) 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).

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

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

19. § IT standards and procedures

(1) 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,

(2) The Central IT Operators’ and Service Providers’ Procedures shall include the following:
    (a) Requirements for the operation of central IT systems
    (b) Role, 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 student policies
    (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 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 student policies
    (d) Definitions
    (e) Annexes, forms.

(5) Student user manuals, policies on the use of student computer rooms, guidelines

20. § List of IT recommendations

The DIT shall develop, maintain and make available on the University's website the following general University IT recommendations in an easily accessible form:

(1) IT Security Recommendation

XII. INTERPRETATIVE PROVISIONS

HBONE: HUNGARNET Backbone, Hungary's academic network operated by the GAID.
GAID: Governmental Agency for IT Development, which provides complex data network, content and Internet services to higher education and public institutions in Hungary.
NEPTUN ETR: The electronic student registration system of the University of Pannonia, Unified System for Higher Education Studies
UNI-PANNON, *uni-pannon.hu*: address of the website of the University of Pannonia.
Error report: a report to the system operator of a suspected or actual malfunction or abnormal event that occurs during the use of an IT device. In the absence of a network connection, prior notification in verbal or written form.
Internet: the global IT network.
Intranet: the network and services within the institution, not accessible from outside.
User of office applications: Office applications are computer software needed to carry out everyday administrative tasks: writing letters, making presentations, creating reports, reporting IT equipment failures, etc.
Person carrying out research and development activities: an employee or other person employed under contract who is actively involved in university research or IT development activities.
Public services: services which may be used by university users and others, with or without restriction.
System operator/administrator: is responsible for ensuring the functionality and user management of the IT equipment (hardware, software, network) used at the institution and recorded in the inventory of the organisational unit(s) defined in his or her letter of appointment, on the basis of his or her job description, contract or temporary assignment.
The definition of misuse also includes, in particular, the manipulation of other Users' correspondence and the copying, forwarding or deleting of personal data.
WiFi (Wireless Fidelity): standard wireless data transmission technology.
Prolonged leave of absence: in particular, unpaid holiday, childcare allowance, childcare benefit, long-term research work abroad.

XIII. LIST OF RELATED LEGISLATION AND REGULATIONS

I.

(1) Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information
(2) GAID User Policy (AUP, 2020)
(3) Privacy and Data Security Policy of the University of Pannonia

XIV. INFORMATION TECHNOLOGY REGULATION OF THE UNIVERSITY OF PANNONIA

ENACTING PROVISIONS

21. § Review and entry into force

(1) Review of the Regulation:

a) review and possible amendment once every two years, on a date to be fixed when finalising the Regulation, or

b) in each case where there are significant changes or major developments in the content of the Regulation or the structure and operation of the organisational unit affected by the Regulation.

(2) This Regulation shall enter into force on 1st January 2022, after approval by the Senate and adoption by the Board of Trustees. At the same time, the Regulation adopted by Senate Resolution 230/2011-2012 (V. 31.) shall be repealed.

(3) This Regulation was discussed by the Senate at its meeting of 9th December 2021 and approved by Senate Resolution 217/2021.(XII.9.).

Place and date: Veszprém, 9th December 2021

Dr. András Gelencsér
Rector

Zsolt Csillag
Chancellor

Adopted by the Board of Trustees by Resolution 86/2021 (12.17.).

Place and date: Veszprém, 17th December 2021

Dr. Tibor Navracsics
Chairman