CORVINUS UNIVERSITY of BUDAPEST	**PROVISIONS OF THE PRESIDENTIAL COMMITTEE**	**10/2024** Version Number: **00.**
ON THE RULES OF IT SECURITY		

Person responsible for professional aspects:	**Tibor Sopronyi**	Head of IT
Professional aspects checked by:	**Barbara Bíró**	Head of Legal Affairs
Legal aspects checked by:	**Zsuzsanna Borbás**	Head of Economic Law, Procurement and Labour Law Services
Decision-making body:	**Presidential Committee**	
Person responsible for editing and publishing the text:	**Anikó Erős**	Higher Education Expert

Version Number	Publication date	Effective date	Version tracking
00.	29.04.2024	01.05.2024	**Publication** Resolution No. ET-51/2024 (25 April)

CORVINUS UNIVERSITY of BUDAPEST	**PROVISIONS OF THE PRESIDENTIAL COMMITTEE**	**10/2024** Version Number: **00.**
ON THE RULES OF IT SECURITY		

Table of Contents

CORVINUS UNIVERSITY of BUDAPEST	**PROVISIONS OF THE PRESIDENTIAL COMMITTEE**	**10/2024** Version Number: **00.**
ON THE RULES OF IT SECURITY		

Purpose of the provisions

1. §

(1) The purpose of the Presidential Committee Regulation on IT Security Rules (hereinafter: ITSR) is to define all systemic requirements, standards and procedures, tasks and activities and to set them out in a uniform and high-level regulatory framework, by means of which the IT security, proper and secure operation of Corvinus University of Budapest (hereinafter: University), the integrity and availability of the electronic systems used by the University (hereinafter: IT systems), as well as the confidentiality, integrity and availability of the data processed by the University in these systems can be achieved, preserved and further developed in a manner that is proportionate to the risks and continuously sustainable.

(2) The ITSR also aim to

a) identify the administrative, physical and logical security measures that support:
   - prevention and early warning,
   - detection,
   - reaction,
   - the management of security incidents,
   - subsequent incident reporting and analysis.

b) promote the development of a uniform approach to IT security within the University, to ensure compliance with the IT security requirements set out in the relevant legislation, and to develop operations in accordance with the best practices formulated in national and international standards and methodological recommendations, which have sufficient preventive effect and can reliably guarantee the protection of the University's digital information and data, and that the use of IT equipment is carried out with adequate security awareness and in a controlled manner.

c) To determine the technical and organisational measures to ensure a level of data security appropriate to the scale of the risk, taking into account the state of the art and the cost of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, including in particular the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data and the ability to restore access to and availability of personal data in the event of a physical or technical incident in a timely manner.

Responsibility sharing

2. §

(1) Responsibility for IT security is shared primarily between the University's management, Information Technology and other departments and individual staff members. The principles of responsibility sharing are discussed below.

a) Top-level responsibility for continuous IT security, regulations and organisational objectives related to IT security, for ensuring an appropriate level of IT security awareness at the University, and for the implementation of IT security measures rests with Information Technology. Legal, Administrative and Regulatory Services support Information Technology by channelling data security requirements under the GDPR.

b) The Chancellor of the University is the senior executive for coordinating IT security.

c) At the level of individual organisational units, the head of the organisational unit is personally responsible for maintaining IT security.

(2) Separation of responsibilities
The following IT security responsibilities should be defined at the University:

a) Key responsibilities of direct top management (Chancellor):

– Coordinating information on IT security tasks with Information Technology and Legal, Administrative and Regulatory Services.

– Providing the resources needed to carry out IT security tasks.

– The Chancellor is responsible for contracting internal and external audits of the IT security system.

b) Information Technology and Legal, Administrative and Regulatory Services
Main IT security tasks of the University's Information Technology department:

– Monitoring and logging data backups.

– Testing the software required to ensure that it is compatible with the university environment.

– Monitoring system logs, virus scan logs and other logs.

– Monitoring the proper functioning of devices (by machine or human methods).

– Monitoring and correcting incidents when staff members report incidents, involving Legal, Administrative and Regulatory Services, when necessary.

– Continuous review of security settings and correcting them, if necessary.

– Design and implementation of system access rights, access policies and specific access rules.

c) Heads of organisational units and their subordinates

– All executives of the University should require their subordinates and agents to comply with IT security standards and, in the event of non-compliance, should initiate the process of accountability in accordance with the relevant internal regulatory documents.

Scope of the Provisions

3. §

(1) Personal scope:

a) The personal scope of the ITSR extends to natural persons (e.g. external lecturers) who have an employment or additional employment relationships with the University, as well as to legal persons and organisations without legal personality who have a contractual relationship with the University, who are involved in the processing of data generated, used, processed, stored and transmitted at the University, and who are involved in the management (development, operation, maintenance, repair or supervision) of IT systems operated by the University. The provisions of the ITSR shall be enforced in the contract concluded with those who are in a contractual relationship with the University.

b) The personal scope of the ITSR also covers students and applicants of the University in all cases where they use the University IT system.

(2) Territorial scope:

The territorial scope of these Provisions extends to the registered seat of the University, all its business premises and areas of operation.

(3) Material scope:

a) The requirements of the Provisions on IT systems apply to information management and infocommunication equipment and its components.

b) The security and electronic property protection systems related to the functions of Campus Services are excluded from the material scope of the ITSR, with the understanding that the IT aspects of their operation are governed by the ITSR.

Provisions concerning external partners

4. §

(1) Addressing security in external relations:

a) In their work, IT security considerations should be part of the training for employees who come into direct contact with external partners such as suppliers, service providers (hereinafter external partners) and customers, and the scope of information that can be disclosed should be clearly indicated.

b) When communicating with customers, only the data and information that are strictly necessary and do not harm the interests of the University may be disclosed.

c) Data relating to a customer or customer contract may be disclosed to the identified person only after the customer and his/her authorised representative have been identified.

(2) Addressing security in agreements with external partners:
The Head of IT is responsible for ensuring that the following obligations and duties relating to IT security are included in contracts with external partners concerning the University's IT systems to the extent justified by the subject of the contract:

a) confidentiality conditions;

b) data protection and data security rules and requirements for the data covered by the contract;

c) management of access rights, logical access to University systems, persons with access rights;

d) the University has the right to check the work done for it;

e) communication channels and escalation routes;

f) security measures expected of the partner;

g) how security incidents are handled;

h) the University's internal regulatory documents in force.

IT devices and authorisations

5. §

(1) Acceptable use of IT devices:

a) The services, systems, resources and devices provided by Information Technology are used primarily for their intended purpose, in accordance with the University's objectives, for teaching, research and the provision of services in support of these purposes. Intended use is the purpose and manner of use for which it was originally provided by Information Technology.

b) It is not allowed to interfere with similar use by others, to reconfigure, replace with own network devices, or to expand university devices for these purposes.

c) The University permits private use beyond the above, as long as it does not interfere with the use specified in paragraph a). Such is, for example, restricting and disabling the sharing of certain files.

d) In order to ensure the purposes described in paragraph a), Information Technology may restrict the private use in space, time or manner of use, and in the case of an IT incident, the use for the intended use in accordance with the University's objectives.

e) In the event of any IT incident, Information Technology staff members may take extraordinary temporary measures to limit traffic. This may be communicated afterwards, depending on the seriousness of the case.

(2) Authorisation requirements

a) Rule for monitoring authorisations:

aa) The basic principle for the allocation of authorisations is that everyone should have access to the information needed to do their job in a way appropriate to their tasks, but should have no more access of a different type of access (principle of least privilege) and that any access that becomes redundant should be terminated without delay. The allocation of authorisations, i.e. the process of authorisation management, should be such that the basic authorisations required to perform the work are always available for all tasks and that any additional requirements can be seamlessly met in a controlled manner through an appropriate approval process. The authorisation management process should ensure that the assigned authorisations are verifiable and that withdrawal is complete.

ab) Definition of content administrator: An employee with a good knowledge of the whole or, in the case of modules, part of a university IT system, who is familiar with the business processes, business and technological operations performed/supported by the system and who supports Information Technology and the development area (Digital Innovation, hereinafter: DI) with his/her work during operation and development. An employee with both IT and business knowledge of the module and responsible for communication between the organisational unit and Information Technology for the system/module. He/she plans the required number of users and monitors the availability of the required number of licences.

ac) The person exercising employer's powers or the employee designated by him/her is responsible for keeping employee authorisations up to date. This means that it is the person exercising employer's powers who must request new authorisations, arrange for the withdrawal of authorisations and have the authorisations to be provided on an ongoing basis extended. The content administrator of the IT system in question is the person who approves the authorisations to be assigned, and may request deletions for systems in live use. Content administrators must have accurate information about the authorisations recorded in the system they administer.

ad) In systems under development or in test systems, the area responsible for development, primarily the DI, may request or approve authorisation requests. Once the development has been completed, the area responsible for the development must also initiate the withdrawal of the authorisations. The content administrator shall review these authorisations annually, based on information provided by Information Technology.

ae) In the case of authorisations that cannot be assigned individually to a user, but automatically to a larger group of users according to a defined logic, the content

administrator shall in each case define, together with Information Technology, the conditions for the assignment of authorisations.

b) Access to networks and services:

ba) University public services are available on the network in specific ways, from inside or outside the University, to University citizens and others.

bb) The University's public and identified network is accessible from any device by those whom the University can identify and are authorised to do so.

bc) The University's protected network includes the devices and services that are accessible only to identified and authorised users of the University. Depending on the nature of the use, this may be further restricted per service.

bd) Access to the University's protected network, from both inside and outside the University, is only possible from a device managed by Information Technology. This is done externally via a VPN connection provided by Information Technology. It is strictly forbidden for employees and contracting partners to attempt any other solution.

be) The University may provide Internet access to University users on their own devices not controlled by Information Technology (mainly Wi-Fi service), to guests (e.g. Event and Guest Wi-Fi service) and to partner institutions (e.g. Eduroam). The connected devices are not considered secure for access to the University network, they do not reach the protected network.

bf) Users and external partners who do not have University access are prohibited from providing services or connecting their devices to the University's network without special authorisation. Suh an authorisation may only be granted by the Head of IT at least two working days before use.

c) Authorisations of employees of Information Technology:
Employees of Information Technology have all the authorisations necessary for the administration of IT systems and services. These authorisations may, where justified, include access to data created by employees. This may include correspondence, files created, network traffic, internet traffic, etc. No one at the University other than the employees of Information Technology may have such authorisations, which shall be accepted by all employees of the University, including executives. Furthermore, all employees of the University shall accept the above, namely that Information Technology employees with sufficiently high authorisations are aware of all operations carried out in all IT systems and have information on all data generated. Staff members of Information Technology may record and analyse network traffic and system log files in the interests of diagnostics, fault detection, operational analysis and compliance with/enforcement of the ITSR.

(3) Registration and deletion of employees

a) Registration:

aa) Employees shall be identified by a unique username. Group usernames are not recommended but are allowed in certain exceptional cases. Exceptions may be authorised by the Head of IT.

ab) The prerequisites to the registration of a new employee are the signed employment contract or engagement contract and the necessary data entered in the HR system (SAP). Without this, new employees may only be registered with the approval of the Chancellor. The registration of employees and the modification of employee data in the user management system is the responsibility of Information Technology employees.

ac) As a basic authorisation, all employees and students have the following access rights: O365 (mail, Teams, Onedrive, SharePoint), use of the University network (access to the Internet within the University service area), printing, etc. In addition to these, the other authorisations need to be requested by the person exercising employer's powers.

ad) For students, access rights are created after enrolment, and they can use the University's internal systems and the applications and facilities in the O365 cloud after registration.

b) Deletion of employees:

ba) In the event of an employee's exit, the person exercising employer powers over the employee is responsible for initiating the process. The employee's authorisations are deleted on the second day after leaving, including almost all his/her data and access. Mail and files stored in O365 can be restored for 30 days. Restoration may cause technical difficulties, so it is recommended to move the files until the employee has exited. If, for any reason, it is necessary to maintain the authorisations of an employee who has exited, the person exercising employer powers shall notify the Head of IT in writing, who shall arrange for the authorisations to be extended.

bb) At the same time, the executive exercising employer powers may, if the risks justify it, take extraordinary additional IT security measures (e.g. ordering an extraordinary suspension in the case of suspected abuse, etc.).

c) Ensuring employee access

The following general rules apply to the authorisation management process:

ca) Access should be granted only to the extent and for the duration necessary for the persons who need it in order to perform their duties and/or exercise their rights. The restriction to the extent and duration necessary minimises not only

the risk of access, but also the liability borne by the person who has access. This is the responsibility of the executive exercising employer powers.

cb) Access to the University's systems may be granted only in accordance with the authorisation management process. The process is as follows:

- Employees themselves may also initiate a request for authorisation, in which case the first step is the approval by the executive exercising employer powers, followed by the approval by the content administrator for live applications.
- In the case of a test system under development, the development area may also approve the request for authorisation instead of the content administrator.

cc) For external partners, access to the University's IT systems can only be granted on the basis of a valid contract. In this case, access requests may only be initiated by an employee of the University and shall be approved by the content administrator if the requested authorisation is to a system in live use (both for live and test environments)

cd) For external partners, access rights may be granted for a maximum of one year, renewable if necessary.

ce) Natural persons, legal persons and organisations with no legal personality who have been granted access to the University's IT systems may exercise such access rights on the basis of contracts concluded with them and/or non-disclosure statements made by them.

cf) In the event of suspected misuse of access authorisations, all employees of the University shall immediately notify their executive exercising employer powers, who shall immediately notify the Head of IT and the Head of Legal, Administrative and Regulatory Services.

d) Ensuring and maintaining student entitlements

da) *Granting authorisations to students*:
Students' authorisations are automatically created when they are registered in the Neptun Unified Education Administration System. A daily running automation creates student privileges in the IDM system and sets the appropriate default authorisations. These created authorisations allow the use of the following services:

- Access to Wi-Fi service
- Use of O365 services (mail, Teams, Onedrive, Sharepoint)
- Use of University infrastructure (laboratories)
- VPN
- Other services related to the university identity (e.g. Moodle, Library databases, Eduroam)

Student status	IDM authorisation
Registered	Provided
Active	Provided
Passive (suspended)	Provided
Academic requirements completed	Authorisation granted for 4 semesters from the last active semester, then cancelled
Final exam passed successfully	Authorisation granted for 1 semesters from the last active semester, then cancelled
Final exam failed	Authorisation granted for 1 semesters from the last active semester, then cancelled
Graduated with a diploma	Authorisation granted for 1 semesters from the last active semester, then cancelled
Dismissed	Deleted
Degree obtained	Deleted
Completed	Deleted
Changed or deleted institution or programme	Deleted

db) *Retention of student authorisations over time*:
For reasons of expediency and legislation, student authorisations should be treated in a different way from employee authorisations.

Exceptions: According to 5. §(3)b) it is also possible to maintain or extend the authorisations, if there is a request for this with good reason.

IT security awareness, education and training

6. §

(1) In order to prepare employees and students to recognise potential internal and external threats, awareness training on basic security requirements should be provided to users of electronic information systems. The training should be adapted to the role of the employee and the systems they use.

(2) IT security training should be provided on an annual and refresher basis. The executive exercising employer powers shall delegate employees to the trainings.

(3) The University conducts internal training of its employees to raise IT security awareness appropriate to their job titles on an ongoing and annual basis, based on training proposals, and through the provision of awareness programmes, awareness-raising and educational materials.

(4) The University supports the participation of employees and students in programmes (e.g. courses, specialist postgraduate programmes) necessary to maintain high standards of professional knowledge in IT security-sensitive jobs.

(5) Information Technology may proactively assess the IT security awareness and qualifications of employees and students, even by running pre-announced simulations of real-life situations (e.g. sending phishing emails). Colleagues who are found to have a deficiency in such a survey are required to attend training on this issue.

Provisions on termination or change of employment (employment relationship, additional employment relationship or contractual relationship)

7. §

(1) *Responsibilities on termination of employment:*
It is the responsibility of the Head of IT to ensure that IT authorisations of exiting employees are withdrawn and terminated if the automatic process of termination is not sufficient. IT authorisations shall be deleted with the account on the second day after exiting. A different schedule may be requested in writing by the executive exercising employer powers.

(2) *Return of property:*

a) Upon leaving the University, the employee shall return the IT device given to him/her to the University. In all cases, the devices shall be handed in to the specialists of Information Technology, even if the relevant organisational unit still wishes to use them. In this case, the exiting employee's executive exercising employer powers shall notify Information Technology in writing of the other employee to whom he/she wishes to transfer the device. Information Technology shall reinstall all the devices returned, as it shall remove the profile of the previous employee, as well as any applications installed. The IT device can then be reallocated on a one-person-one-

device basis. Upon return of the device, the User declares that he/she has provided the device used by him/her to Information Technology after deleting all documents of a personal nature from it. The model declaration in accordance with this paragraph is issued by Information Technology. HR shall keep the declaration for 5 years.

b) If the device is returned in a complete and faultless condition, this fact is recorded in the records of Information Technology and these data are transferred to the Asset Management Unit of Finance.

c) If the employee does not fully account for the device used according to the records, Information Technology will not certify the proper returning of the device at the time of exit and will notify HR no later than 2 working days before the date of exit. If the employee is unable to account for the device in his/her possession according to the records, he/she shall reimburse Information Technology for the value of the device at the market price established by Information Technology.

(3) *Change or replacement of IT device:*

a) If an IT device provided by the University is replaced, either due to a failure or as part of the central PC replacement programme, the previously used IT device may be purchased. An IT device may be purchased if it has either been in service for more than 4 years and is not subject to a prohibition on disposal, or is in such a state of repair that it can no longer be used. In all cases, the price of the device is determined by the experts of Information Technology, taking into account market prices, which are not negotiable.

b) The University's IT asset management is based on the principle of "one person, one computer". Correspondingly, each employee is provided one computer. Exceptions to this may be made in justified cases, which shall always be authorised in writing by the Head of IT. The one computer provided is always a notebook, i.e. a portable computer.

(4) *Termination of access rights:*

a) All executives exercising employer powers shall immediately notify HR of their subordinates' intention to terminate their employment relationship, and HR shall forward this information to Information Technology, indicating how long the employee will be employed and what (possibly reduced) authorisations he/she will need during the transition period.

b) Executives exercising employer powers, or contract signatories for other contracts, in the event of an employee's exit or termination of employment or other legal relationship (such as contractor or temporary worker), etc., shall notify Information Technology of the exit and the necessary measures (access restriction, suspension, redirection of emails, etc.).

c) It is the responsibility of the Head of IT to ensure that the IT authorisations of the exiting employee are restricted to the level specified by the executive exercising employer powers for the notice period (or equivalent period) and permanently

withdrawn on the day of termination, unless Information Technology receives a written request to the contrary, initiated at least by the executive exercising employer powers.

d) The status of students is regulated in paragraph d) of Subsection (3) of Section 5. Authorisations may be extended for students as well, if justified and the request is submitted in writing by the lecturer or employer to Information Technology, stating the reasons.

e) Privileged authorisations: this includes all authorisations that give more rights than those of employees or students (e.g. system administrator). Main rules on privileged authorisations:

- Only staff members employed in a system administrator role may be granted administrator rights to administer systems, and only for systems that are appropriate to their role. System administrator authorisations shall be clearly personalised, and the use of group IDs is prohibited.
- System administrators should use their user IDs with elevated rights only to the extent strictly necessary for their work, and should use their normal user IDs in all other cases.
- Putting systems into operation that would require non-system administrator employees to be given administrator authorisations should be avoided by all means.
- In the event of the exit of an employee with privileged (e.g. administrator) access, the Head of IT shall ensure that the passwords known to the exiting employee are changed by the administrators in a documented manner, depending on the security classification of the data processed in the system and the risk associated with access.
- Users may have system administrator authorisations in accordance with the Provisions entitled "Review of authorisations" that came into force in January 2022. The Provisions are in Annex 1.
- Information Technology shall restrict and withdraw employee authorisations as recorded in the ticketing system.

(5) *Review of employee access rights:*

a) The justification and IT security adequacy of the authorisations requested by the employee shall be reviewed primarily by the executive exercising employer powers or by the employee appointed by the executive or the content administrator at least once a year.

b) The correctness of the data of already registered employees and the authorisations granted to them should be reviewed regularly, at least once a year, with the aim of detecting errors/mistakes in the administration. It is the responsibility of the Head of IT to initiate the review, prepare a report of current authorisations and send it to the

appropriate executives, and then implement the requests for changes. The data shall be checked for accuracy, filtering out the following:

- staff members who have already exited but remained in the system,
- former authorisations remaining after a change of job title,
- temporarily granted authorisations that have already expired.

Employee responsibilities

8. §

(1) Using secret authentication information:

a) Every employee shall preserve the confidentiality of his/her secret authentication information and shall not share them with any other employee. These shall not be kept on paper.

b) The employee shall be liable for any damage resulting from the careless use of authentication information.

c) If the University's employees need to obtain authorisation from external partners, the expert of Information Technology may perform this activity in cooperation with the relevant area executive.

d) Employees are not encouraged to use unencrypted private data storage, such as: cloud-based data exchange portals, private email accounts or physical storage devices. These private tools include employees' personal email accounts. Cloud hosting subscribed to and used by the University is not subject to this prohibition.

(2) Register of employee authorisations:
It is the responsibility of the Head of IT to keep a record of authorisations in electronic systems, except for systems with non-central authentication (e.g. Neptun or SAP). No paper-based record of authorisations is required.

System and application access control

9. §

(1) The purpose of the ITSR is to define the processing, generation and modification of passwords and usernames that provide access to the University's IT systems.

(2) Restricting access to information:

a) Password: The password is one of the main tools used by employees and students to validate their access authorisations to IT systems and to prevent unauthorised access.

<u>The main rules for using passwords:</u>

aa) Disclosure or making accessible of a password to an unauthorised person constitutes a breach of a trade secret, which may give rise to labour law and

criminal law liability for employees and disciplinary and criminal liability for students.

ab) In non-core infrastructure systems, authorisations and passwords are managed by content administrators, while core infrastructure passwords are managed by Information Technology.

ac) Only the password of the employee or student who has requested a password change may be changed, provided that the request is made in writing and the person entitled to change the password requests it. In the event of an oral report, the password of an employee or student other than the reporting person shall not be changed, and an error ticket shall be generated for the oral report.

ad) Passwords shall not be stored in plain text or transmitted via any channel, except for the electronic transmission of the password created for the first time.

ae) The password creation rules set out in 9. §(3) are binding.

(3) Rules for password creation:
Only passwords meeting the following parameters may be used in the University's central IT systems. The rules for password generation are as follows:

a) It should be at least 8 characters long.

b) It should consist only of letters without accents.

c) The password may not be the same as the user ID.

d) Passwords should be complex and contain at least one lowercase letter, at least one uppercase letter and at least one number.

e) When changing the password, the new password shall not be the same as the last password.

f) The password shall expire in 1 year.

Managing communication and operations

10. §

(1) Change management

a) The governing organisation for change management is the Change Advisory Board (CAB).

– The CAB is made up of representatives of functional/technical departments, key decision makers and business stakeholders. The main task of the CAB is to evaluate the requests for changes submitted by the different departments and to take the necessary decisions on their feasibility, taking into account the objectives, plans and resources set by the University.

– The CAB should be convened by the Head of IT or the Head of DI, and it is up to them to decide when they consider it appropriate to bring a change to the CAB.

The CAB does not need to be convened at regular intervals, only when its decision is necessary to initiate change or when it has reached a point in the change process that requires a joint decision.

b) The CAB shall be convened in the following cases:
   - Particularly high-value development projects with a value of at least HUF 30 million.
   - A change or development that affects the tasks of several departments.
   - A change or improvement that affects several interconnected systems.

c) Members of the CAB:
   - Head of IT
   - Representative of the Finance area (appointed by the Head of Finance)
   - The Head of the DI Team
   - The heads or representatives of the departments concerned

d) It is not necessary to convene the CAB for matters that are technical changes and do not concern applications or fall specifically within the scope of competence of Information Technology. This could, for example, be changes to the server or network environment, or improvements to the mail system.

e) Changes or upgrades to IT systems and applications may only be initiated and implemented with the written approval of the Head of IT and the Head of DI.

f) If the change or development involves the processing/storage of personal data, the opinion of the Data Protection Officer should be sought in advance in order to identify the relevant data protection requirements and to channel them into the development process ("privacy by design").

(2) Security aspects:

a) The Head of IT proposes change management procedures and their modification, taking into account security aspects. If the change management procedure affects the CAB's scope of competence, the Head of IT shall convene the committee.

b) Changes to IT systems should only be made on the basis of written change requests approved by the Head of IT or an employee authorised in writing by the Head of IT. After implementation, changes shall be documented by the person implementing them.

(3) Separation of development, test and live systems

a) In the case of an external developer, the staging environment shall always be provided and operated by the developer. The Information Technology department does not provide a staging environment for external contracting partners, only service level access to the test environment, in an on-prem environment. In a non-on-prem

environment, it is the developer's responsibility to create and operate the development environment, especially if the development is purchased as a service. The specialists of Information Technology shall support the setting up of a test and live system.

b) The Head of IT shall provide the resources needed for separate testing and live environments where necessary. The test system should have the same level of security as the live environment, including the use of passwords.

c) Whether the development is done in-house or by an external contracting partner, they can only perform tasks in the designated development environment and can only test new versions of the development in the test environments. Testing in a live environment is not allowed if it can be done in a test environment as well. The performance and results of the testing shall be documented in a report. The development may only be deployed to the live environment after a documented successful test.

d) Where a test environment is not available, the Head of IT or the Head of DI may decide to deploy a development on the live system if this cannot be done with test data.

(4) System design and adoption:
The documentation procedures for applications and systems purchased in procurements not initiated by Information Technology and not implemented and managed by Information Technology shall be provided by the implementing or requesting area. In these cases, Information Technology only provides information on IT-related issues, mainly technological ones.

a) Information Technology may only take over the operation of systems where it has been involved in the project from the design phase and has accurate information on the system to be taken over.

b) Providing, organising and monitoring the testing infrastructure.

c) Data used for testing should be protected at the same level as it would be in a live environment.

d) New systems or new versions of systems may be put into service only in accordance with the University's approved testing procedures. The fact and circumstances of putting into service shall be documented in the operator's logbook.

e) Once the tests have been completed, the developer's authorisations in University systems shall be withdrawn, except for those required for the activities undertaken under the support and maintenance contract. Test completion is determined by the organisational unit conducting the test.

f) The employee acceptance test of the new IT systems shall be carried out by a designated employee of the organisational unit ordering the same (supported by

Information Technology if necessary), and the results shall be communicated to the designated contact person of Information Technology.

g) Similarly to the protocol to be followed in the event of an IT change or upgrade, if the new system affects the processing/storage of personal data, the opinion of the Data Protection Officer should be sought prior to purchase, but at the latest prior to the start of use, in order to identify the relevant data protection requirements.

Protecting software in use

11. §

(1) Installing software on the systems in operation:

a) The installation and alteration of software by appropriately qualified specialists shall be ensured.

b) The installation of thoroughly tested software and software packages that work together flawlessly shall be ensured.

c) Software without manufacturer support should not be run on business-critical systems.

d) Obsolete software that is no longer supported by the manufacturer should be replaced or updated as soon as possible.

(2) Protection against malicious and mobile codes:

a) The University operates protection software with virus scanning and antivirus functionality on all workstations, the installation and security configuration of which is the responsibility of Information Technology.

b) The experts of Information Technology monitor the availability and correct functioning of the virus protection system on an ongoing basis.

c) No software may be installed or run on University devices without written approval from Information Technology, unless the owner of the device has system administrator rights.

d) It is not allowed to bypass, interfere with the operation of, or change the configuration of the University's security systems (firewall, antivirus or content filtering).

e) It is not allowed to run files on University-provided devices for purposes or in a manner not approved by the University, or to import data files of unknown origin downloaded from the Internet on a data carrier.

f) External files received in the course of the University's business are automatically scanned by the anti-virus software before opening/running. It is the responsibility of Information Technology to make the necessary settings. In case of doubt, the data carrier containing the file shall be forwarded to Information Technology for virus checking.

g) All employees shall immediately report any suspected virus infection to the IT Helpdesk.

(3) Backup:

a) The Head of IT shall ensure that the IT systems used by the University and the data processed in them are backed up in accordance with business needs and in a documented manner. The confidentiality classification of the data processed should also be taken into account in the design of the backup procedure. The backup procedure should also cover the management of data carriers containing backups. The backup procedure is set out in *Annex 2*.

b) The staff members of Information Technology shall make the settings for backups and check the success of backups. Backups are documented (backup log or log file). If the backup can only be carried out by shutting down the IT system concerned, the content administrators of the area concerned shall be consulted in advance.

c) Personal data processed in backups are subject to the retention periods applicable to personal data processed in live systems, the enforcement of which requires the cooperation of Information Technology and the organisational unit processing the personal data, with the assistance of Legal, Administrative and Regulatory Services, if necessary.

(4) Network security management:

a) The Head of IT is responsible for the secure design, operation, maintenance and protection of the University's network.

b) The University's networks shall be kept separate from public networks. All Internet exits shall be protected by a firewall, the settings of which may only be changed by employees designated in writing by the Head of IT and with the responsibility recorded in the job description.

c) Wired or wireless network and Internet access on the business premises of the University may be installed and configured only by staff members of Information Technology.

d) Users are not allowed to bypass or interfere with the operation of the University's security systems (firewall, proxy, content filtering device or application) or to modify their configuration by employees not designated by the Head of IT.

e) It is not allowed to rearrange, replace, connect to another socket or modify the current connection of low-voltage power cables. These tasks are carried out by the staff members of Information Technology, based on a report to the helpdesk.

f) The operation of any system that provides a network service to a wider range of users is subject to the approval of the Head of IT. A broader set of users includes in particular a service that can be accessed by anyone on the network, a service that can

be accessed by university citizens on the network, or a service that can be accessed by a group of university citizens (e.g. a specific dormitory) on the network.

g) The University also helps to protect systems providing network services by filtering network traffic. Network filtering rules are developed by Information Technology in cooperation with the content administrators responsible for the operation of the systems. In order to enhance network security, network filtering rules may be modified by employees designated in writing by the Head of IT, with responsibilities set out in their job descriptions, at their own discretion. The minimum requirement for requests from outside this scope is documented approval by the responsible content administrator of the system providing the network service.

(5) Monitoring:

a) Audit logging

- For each system, the Head of IT, in agreement with the data owners, defines the activities to be logged, the method and purpose of logging and the retention period of the log files. Unless a longer retention period is required by law or the Data Protection Officer sees no reason to set a longer retention period, the maximum retention period is 6 months.
- All servers and network devices shall be connected to the monitoring system and the log collection and analysis system. The log collection and analysis system shall define the reports and monitoring that the software can perform automatically.

b) Monitoring system use

- Staff members of Information Technology, as required by the Head of IT, perform the necessary log file analyses using software tools or manually, and document and evaluate any indications of irregularities or system breakdowns, and report the results to the Head of IT.
- If the result of the analysis of the log files points to the possibility of a security incident, it should be reported to the Head of Legal, Administrative and Regulatory Services.

c) Logging errors

- Every three months, the Head of IT (or an executive appointed by him/her) reviews incidents in the Helpdesk system that are more than one month old and takes the necessary actions to resolve them, with a priority appropriate to the classification of the errors.
- Errors in IT systems should be recorded in the Helpdesk system following documented analysis. Staff members of Information Technology analyse the errors on a weekly basis and identify emerging or expected problems.

Rules for internet use at the University

12. §

(1) The University does not prohibit private internet use on devices connected to its network infrastructure. The rules of use are set out in 5. §(2)b).

(2) Electronic mail:

a) The purpose of this Section is to regulate the use of the University's electronic messaging and mailing system. The regulation defines acceptable and correct use, the IT security rules to be followed during use, and the roles and responsibilities associated with use.

b) The regulation applies to all employees and students of the University, as well as to all third parties who have been authorised to use the University's electronic messaging system.

c) The University does not prohibit the private use of the mailing system, however, there are limits to such use as detailed below.

(3) Rules and procedures for the transmission of information
The mail system and the messages produced, sent, transmitted, received, stored or archived on the system are the property and under the control of the University, which may monitor them in accordance with this paragraph and may inspect their contents in a strictly purpose-related manner where appropriate. Such purposes may include, for example, ensuring business continuity, gathering evidence when investigating IT security incidents and disciplinary matters, and responding to requests from statutory authorities. The University shall apply the principle of graduality in the inspection, whereby if there is no doubt from the subject/recipient or other circumstances of an email that it contains personal data of either the employee or a third party, even without opening the email, the contents of the email shall not be viewed. An exception to this is when the University has reasonable grounds to suspect that the employee's mailbox contains data that is harmful to the rightful economic interests or business reputation of the University, in which case the University is entitled to know the content of such e-mails after conducting a special balancing of interests test. In such a case, the data subject shall be informed of the inspection of the mailbox, his/her personal presence shall be ensured, including through a representative, and a report of the inspection shall be recorded. In all cases, such an inspection may take place in the presence of the Head of IT and the Head of Legal, Administrative and Regulatory Services, or persons designated by them. In order for email account inspection to be lawful, the University must provide detailed information to employees in advance.

The information shall include the following:

a) the purposes and employer interests for which the email account may be inspected;

b) the person carrying out the inspection on behalf of the University;

c) the rules that apply to inspections (application of the principle of graduality) and what the procedure is;

d) employees' rights and legal remedies in relation to the processing in connection with the monitoring of their email account.

It is prohibited to use the service to transmit or store any content that is illegal or even partially illegal, including copyright infringements.

When sending electronic mail, it is also important to ensure that confidential or personal data is not transmitted to unauthorised persons.

Particularly sensitive attachments in correspondence should be password protected and the password to open the attachment should be sent to the recipient via another channel (e.g. SMS).

(4) The following is not allowed when using the electronic messaging system:

a) sending messages of unreasonably large volume and size (sending files larger than 35 MB by mail is not recommended);

b) publishing advertisements and announcements;

c) distribution and transmission of chain letters;

d) sending or forwarding messages or attached files that contain any violation of law or any invitation to violate law in any way or harm the reputation of the University.

(5) Agreements for the transfer of information

a) The University will take all reasonable steps to ensure the reliable and secure operation of the email service, but cannot accept liability for any loss, delay or failure in transmission of a message. It is therefore the responsibility of all employees to ensure that their critical messages reach their destination. The read confirmation function or verbal enquiry can be used for this purpose.

b) The employee should be aware that the University is not in a position to monitor the routing of messages sent beyond the boundaries of its network or to ensure their security.

(6) Electronic messaging

a) Only the electronic mailing address provided for this purpose, the service authorised for the employee, may be used for the exchange of messages on behalf of the University. Email services provided by another organisation or service provider may not be used for official purposes.

b) The employee shall acknowledge that the sender, recipient and subject of his/her correspondence may be visible to duly authorised staff members of Information Technology during the technical operation.

c) The employee shall acknowledge that in the event of termination of employment, his/her mailbox may be archived at the request of his/her line manager and the messages contained therein may be used for the smooth continuation of business.

(7) Confidentiality or and non-disclosure agreements

a) In accordance with general IT procedures, confidential information should only be sent by email or as email attachments in encrypted form.

b) Emails or email attachments containing confidential information shall not be forwarded without the express consent of the sender.

c) It is prohibited to send a message containing confidential information to a mailing list.

d) Information leaks shall be protected against. Protection is primarily achieved by implementing the technical measures and rules of conduct listed elsewhere in this Regulation. The best way to prevent information leaks is for staff members to behave in an IT security-aware manner.

Management of IT security incidents

13. §

(1) *IT security incident reporting*

a) A security incident is any unintended or unexpected single event or series of events that causes an adverse change or a previously unknown situation in an IT system, resulting in the loss of confidentiality, integrity, authenticity, functionality or availability of the information carried by the IT system, or in the corruption of the information. An incident is any event that is not part of the University's day-to-day business, cannot be resolved through the normal troubleshooting process and could compromise the security of the University's IT systems and the data they handle.

b) All employees shall report immediately any security incident and any indication of a security incident to their executive exercising employer powers and the Information Technology Helpdesk.

c) In the event of a security incident, the Head of IT conducts an investigation based on a report received or on his/her own observation, involving the Head of Legal, Administrative and Regulatory Services if necessary.

d) The rules for handling a personal data breach are laid down in the Provisions of the Presidential Committee on the Rules of Data Protection.

(2) *Security vulnerability reporting*

a) Staff members of Information Technology shall report the details of the notifications they receive and the events they detect to the Head of IT, as necessary.

b) The reporting obligation of employees includes the reporting of signs of a possible security incident that could compromise the security of information systems. Such signs could, for example, be:
   - an increase in the number of unsolicited emails. In this case, the employee shall block the sender in the mail system, thus teaching the mail system to
   - the arrival of unsolicited email attachments suspected of being viruses;
   - the possibility of unauthorised access to data, data leaks from the IT systems they use;
   - the visible damage to IT devices (PCs, network devices, printers, peripherals);

(3) *Handling IT security incidents and remedial improvements*

a) Responsibilities and procedures:
   - The Head of IT shall ensure that there are documented procedures for handling high-risk security incidents (e.g. large-scale virus infections, network intrusions, destruction of critical assets, etc.) that are known to and tested by the staff members of Information Technology.
   - In the event of a report concerning IT security, the employee receiving the report shall immediately forward it to the administrator of the system(s) concerned.
   - System administrators shall immediately start investigating the incident and take any action deemed necessary. Actions involving other systems require prior consultation with their system administrators.
   - If the threat was successfully eliminated, the Helpdesk entry for the incident should be completed with the elimination process.

b) Lessons learned from IT security incidents:
   - In the event of a significant incident, the Head of IT evaluates the IT security incidents and their impact immediately, otherwise on a monthly basis, with the involvement of employees of Information Technology, and initiates the necessary measures with its approval.
   - A report is drawn up of the evaluation, sent to the data protection organisation for information, and can be used as a basis for comparison in the next evaluation.

Miscellaneous and final provisions

14. §

(1) The present Provisions shall enter into force on 1 May 2024.

Annex(es)

Annex 1: Review of authorisations

Annex 2: Corvinus backup procedure

Annex 1

Review of authorisations

Considering requests from several sources, in particular from the Academic organisational units, Information Technology has started to review the system of authorisations for notebooks. Gathering information from various sources (including contacting universities abroad), we consider it advisable to introduce the possibility for lecturer colleagues to have full local administrator access to the university-owned laptop they use.

We intend to introduce it on the basis of the following criteria:

(a) Full administrator rights may only be provided to portable devices owned by the University (this category includes all devices provided by Information Technology and devices purchased from grant funding).

(b) Devices with administrator rights will be allocated with a special sign in the ITSC registration system.

(c) In addition, such rights may retroactively be requested for devices currently in use, which will also be subject to the conditions mentioned above. Information Technology will perform the necessary changes on devices currently in use (e.g., remove the BIOS password). Such computers will then be taken out of the University systems. The new devices do not have an operating system and no applications installed on them, which must be taken care of by a staff member with administrator rights.

(d) Colleagues with full administrator rights will be free to install and uninstall applications on the computers administered by them, while observing the requirement of using licenced software and assuming legal responsibility.

(e) All restrictions on the device will be removed, everything becomes freely configurable.

(f) These devices will be removed from the administration environment of Information Technology, so their software maintenance and possible reinstallation must be carried out by users with full administrator rights. They will be supported by Information Technology to the same extent as devices in users' own ownership.

(g) In the event of a (physical) failure during the warranty period, the staff members of Information Technology will continue to take care of repair services, if requested.

(h) For security reasons, devices with full administrator rights are not allowed to enter the University domain. Shared repositories will also be accessible only via a VPN connection.

(i) For security reasons, devices with full administrator rights are not allowed to connect to the University's internal wired network, and may only use WiFi and VPN.

(j) Users will be required to sign a declaration in relation to the above. This declaration will detail all relevant conditions, limits and options.

Such rights may be requested by any researcher colleagues who receive approval from the Head of their Institute for the issue of the rights. Without such approval, the ITSC will not carry out any modification to rights. Requests may be submitted by using the following electronic form: https://forms.office.com/r/ezftQj203B

Colleagues who do not wish to take advantage of full administrator authorisations can continue to use their tools in their current environment.

Annex 2

Corvinus backup procedure

Oracle

Frequency: Log per hour. Daily incremental and weekly full backup.
Method: Timed from Oracle
Retention period: 28 days

The following systems are backed up daily:

Systems running under Solaris

Method: Timed from operating system
Retention period: 30 days

TSMSRV

Method: Timed from the operating system; /save on the TSM server
Retention period: 30 days

SAP systems

SAP ABP database HANA

Log saving: max. every 15 minutes
Retention period: 365 days

SAP ABT database HANA

Log saving: max. every 15 minutes
Frequency: weekly
Retention period: 365 days

Application and web servers

Method: Timed from operating system
Retention period: 30 days

Backing up VMware virtual machines

Method: by scheduling from a backup server
Retention period: 30 days

Backing up databases under VMware

Method: by scheduling from a backup server
Retention period: 30 days