Annex EKR 10

Information Security Policy (IBSZ)

1. Preamble

1.1. The operation of information systems involves numerous risk factors and potential threat scenarios, with the understanding that these threat sources cannot be completely eliminated. Both the users who manage the **Dharma Gate Buddhist College** (hereinafter: the College) information assets and the system operators must strive to reduce risks, with the aim of keeping them at an acceptable level. To achieve this objective, the College continuously assesses the risk factors and manages them as appropriate to the situation.
1.2. This policy covers measures to prevent harm arising from the improper handling of information, the management of information security events and incidents, and—if an incident occurs—the minimization or remediation of damage.
1.3. To avoid information security incidents, the goal is to prevent and counter threat situations using administrative and technical measures. We ensure the objective is achieved through information security measures, their operational monitoring, and detective controls, in order to prevent or minimize adverse impact. Administrative measures (policies) also set out the steps to be taken in a given situation.
1.4. We provide the highest level of technical protection for information systems, while observing the principle of proportionality. To minimize human-related incidents, we implement policy and training measures.

2. Purpose of the Information Security Policy (IBSZ)

The purpose of this Information Security Policy (hereinafter: IBSZ) is to regulate the security measures applicable to the information systems operated by the College; to set the security rules for the procurement and use of IT equipment, for operation, development and deployment, and for data processing; to define IT roles; and to prescribe the information security duties attached to each role. The IBSZ provides the framework to achieve these objectives and to ensure the confidentiality, authenticity, and availability of data processed both within and outside the information systems. The policy is grounded in the information classification of the College's processes, data, and the systems that handle them.

The IBSZ sets out the following key tasks:

1. Assigning classification levels to the College's information systems.
2. Ensuring compliance with the requirements for protecting confidential information and information assets.
3. Protecting data subjects' rights.
4. Ensuring the intended use and proper operation of IT equipment, hardware, software, networks, etc.
5. Carrying out the technical upkeep and maintenance tasks that ensure operational reliability.
6. Preventing—and, where prevention is not possible, minimizing—harm arising from unauthorized access and misuse during processing operations and any subsequent use of output data.
7. Maintaining the integrity of datasets and their accuracy in both structure and content.
8. Ensuring the integrity and reliable operation of the software in use.
9. Securely backing up datasets.
10. Ensuring the proper handling of written documents used and created.
11. For the College's managers and staff who oversee IT-related work, this policy identifies the information assets tied to the systems in their remit and sets out their duties to protect those IT systems—ensuring their security and dependable operation.

12. Defining the access rights and access control framework for the information systems.
13. To meet these objectives, this policy must apply across the full life cycle of every system component—from design and operation through to decommissioning.

3. General Provisions

3.1. The scope of the IBSZ covers all employees and students of the College, as well as any person who enters into a relationship with the College under which they handle the College's IT infrastructure and information assets, or any part thereof, or use the College's information systems.
3.2. This policy also applies to any third party whom the College authorizes to handle any part or all of its information assets, or to use the College's IT infrastructure.

4. Information classification for IT systems and data

4.1. The systems operated by the College must be assigned to **one of the following five security levels**. Classification is based on the criticality of the processes the system and its data support, the value of the data, and the magnitude of harm if the system or its data become unavailable or are lost. Data sensitivity is also a key determinant of classification—especially where personal data and special-category personal data are involved.
4.2. Systems and data to be classified at **Security Level 5** are those that are mission-critical to the College, for which a compromise or outage would result in one or more of the following:

- A significant loss could occur, with the damage potentially amounting to up to 25% of the College's annual budget,
- Human lives may be at risk, or a large number of people could be injured,
- A large volume of personal data or special-category personal data could be publicly disclosed,
- Data assets that form part of the national data assets may be compromised or fall into unauthorized hands,
- The availability of a critical information system is not ensured,
- High-value, non-public information critical to the College's operations could be subject to unauthorized use or public disclosure,

For the College, these systems are:

- Student Information System. However, the Student Information System is operated under a third-party service arrangement, so the relevant requirements can only be fulfilled in part within the local IT environment.
- Financial Management System. However, the Financial Management System is operated under a third-party service arrangement, so the relevant requirements can only be fulfilled in part within the local IT environment.

4.3. Systems and data to be classified at **Security Level 4** are those that are critical to the College's operations, where a compromise or outage would lead to one or more of the following:

- A large volume of personal data or special-category personal data could be publicly disclosed,
- An information system that handles highly sensitive processes, or data linked to such a process, could be significantly compromised,
- The risk of personal injury may increase,
- High-value, non-public information critical to the College's operations could be subject to unauthorized use or public disclosure,
- Loss of trust ensues, or disciplinary action becomes necessary within the leadership of the service area concerned,
- The combined direct and indirect losses amount to 15% of the College's budget.

For the College, these systems are:

- Document Registration System,
- IT network,
- PBX (private branch exchange) and related network,
- Central email servers,

- Central storage servers,
- Central directory service

4.4. Systems and data to be classified at **Security Level 3** are those that are critical to the College's operations, for which a compromise or outage would result in one or more of the following:

- Personal data or special-category personal data could be compromised or publicly disclosed,
- A system or data underpinning a process sensitive to the College's operations could be compromised,
- Loss of trust may arise regarding the system and, as a result, toward the organizational unit that operates it,
- The fulfillment of obligations set out in the organizational regulations may be put at risk,
- The combined direct and indirect losses amount to 5% of the College's budget.

For the College, these systems are:

- Servers,
- Learning Materials Portal

4.5. Systems and data to be classified at **Security Level 2** are those that are critical to the College's operations, for which a compromise or outage would result in one or more of the following:

- Only a limited volume of personal data could be compromised,
- Only low-value data, or a non-critical information system, could be compromised or experience an outage.
- Any financial loss would not exceed 1% of the annual budget.

For the College, these systems are:

- Computer labs,

4.6. Information systems for which a compromise would result only in negligible harm must be classified at **Security Level 1**. Systems classified at Security Level 1 must not process a significant volume of personal data; any issue remains within the College and can be handled internally. Any financial loss would be negligible.

5. Information Security Principles

5.1. For the purposes of the IBSZ, a secure state is when the institution's information assets—and the systems that store them and support the processes—have their confidentiality, integrity, and availability safeguarded comprehensively and continuously, at a level proportionate to their classification.

5.2. For systems classified at Security Levels 3, 4, and 5, the protection of the data they process and the systems built on them must ensure confidentiality, integrity, and availability such that the information system and its environment are safeguarded on a continuous, comprehensive, closed, and risk-proportionate basis, and a closed-loop control cycle is established as follows:

- Protection is continuous when it performs its functions without interruption, even under changing environmental conditions. Continuous protection must be ensured throughout the information system's full life cycle—from procurement to decommissioning.
- Protection is comprehensive when security measures cover every element of the information system, including the network architecture in use and any devices operating between any two endpoints. Protection must be implemented across the physical, logical, and administrative domains as follows:
    - For every information security system component or group, including central, intermediate, and endpoint devices,
    - For the information system's infrastructure,
    - For the hardware components involved in the system's operation,
    - For the operating systems and the systems that support the processes,
    - For the communications system, with particular emphasis on computer network connections,
    - For the storage media that hold the system and its data,
    - For system-related documentation,
    - For the system operators,

    - For the data processors with access to the system's data,
    - For external partners involved in the system's operation.
- Protection is closed when, at the design stage, all relevant threats have been taken into account and defenses are implemented against each of them.
- Protection is risk-proportionate when, over the long term, the costs of protection are commensurate with the potential harm, and the protective measures reduce risks to a tolerable level. The objective is to minimize costs while keeping risk at a tolerable level.

6. Core areas of information security

6.1. Information protection, meaning the safeguarding of the College's information assets in terms of confidentiality and integrity, regardless of whether those assets are stored electronically or in any other form.
6.2. Reliable operation, meaning the availability of the College's information systems and their sustained ability to deliver the expected functionality.

7. The College's security policy

7.1. The College's security policy sets out for all operators and users the principles and rules needed to establish and maintain the confidentiality, integrity, and availability of the institution's information assets and the systems that process them.
7.2. The primary objective of the College's security policy is to maintain the College's operational processes by protecting its information assets and the components of its information systems. Endangering any element of the information assets may result in the user handling it being excluded from the system concerned or—depending on the severity—from the entire IT system.
7.3. In all areas, efforts must be made to minimize risks while observing the principle of proportionality. Responsibilities must be established for every area of the information assets. Information security responsibilities must be defined so that they are linked to the performance of specific operational and data-controller duties. Every effort must be made to comply with statutory obligations, with particular regard to the GDPR, Chapter 43 of Act C of 2012 (Btk.), and Act CXII of 2011 (Info tv.)
7.4. The ***Head of the IT Department (hereinafter: IO)*** is responsible for delivering information security training and ensuring the necessary resources are available. Ensuring adherence to—and maintaining—the organizational unit's information security culture as set out in the IBSZ is the responsibility of the unit's head. Based on the above, information security responsibilities are shared among the IO, the heads of the organizational units, and the users, in line with the following general principles.

8. Operator's authority

8.1. For every information system operated by the College, responsibility for operation in accordance with the IBSZ rests with one of the following:

- The IO staff are responsible for operating the system's IT service components (servers, workstations, operating systems, client software), for the technical protection of information assets stored in electronic systems, and for operating the supporting systems.
- In justified cases—for example, when operating a research-support server, a network device, or a website—the above task may be performed by another employee of the College, provided they possess the operational, security, and data-security expertise required to run the system in question, and the Head of the IT Department has authorized it in writing. The same rules apply to the operator as to the IO staff, but responsibility for data protection incidents shifts from the IO to the head of the relevant organizational unit.
- System operation may also be performed by a person or organization engaged by the College under a service or mandate contract. In this case, the IBSZ applies to them and their subcontractors as well.

8.2. For every information system operated by the College, responsibility for managing the data stored in it rests with the head of the relevant unit. Their task is to define the scope of access to the data and the personnel scope of the processes implemented by the system, to review these regularly, and to update the system accordingly to reflect changes. For systems in Security Levels 5, 4, and 3, access rights are configured by the manager with the requisite IT expertise and authority—either personally, or on the basis of a written or email instruction issued by that manager to a designated IT Department staff member. The instruction must include the name of the employee authorized for access, the access rights or roles, the duration of the access, and a description of the principles for managing access rights.
8.3. Regulating the scope of access is the responsibility of the head of the unit even when the data are not stored in an electronic information system.
8.4. If the operation of the given information system is performed by an external person or organization, the head of the organizational unit is responsible for ensuring that the IBSZ requirements are enforced with respect to that party. To this end, the following must be included in the service contracts:

- The external party's assumption of responsibility for the information systems covered by the contract, including compliance with all applicable laws and regulations in force at all times and with the College's internal policies.
- The service-level agreement (SLA) undertaken by the service provider. It must cover the precise scope of commitments, the quality criteria, how they will be measured, and any applicable penalties. Service provider contracts must always address information security, confidentiality, and data security. Monitoring compliance with the service contract and taking the necessary measures are the responsibility of the manager of the system concerned.

9. Users' responsibilities

9.1. All users of the College's IT system must use it in accordance with the IT and Security Policy (IBSZ).
9.2. Every individual and application may access IT services only with the access rights assigned to them and may use the system strictly within the scope of those rights. Changes to access rights must be initiated with the owner of the relevant system, who will ensure that access permissions are set in the manner regulated by this IT and Security Policy.
9.3. Sharing personal access rights with another person is prohibited, and a personal access must not be assigned to multiple individuals.
9.4. If a service operator or user determines that an IT system provides them with a higher access level than necessary, they must report this to the head of their organizational unit; for systems operated by the IO, to the head of the IO. The reason for the elevated access level must be investigated.
9.5. The service operator or user bears full responsibility for complying with the obligations undertaken when using that service.
9.6. The College's data assets, whether stored in an information system or by other means, are the property of the College. All staff must use the information systems strictly within the scope of their job duties, following the system's operating instructions and any related procedures.
9.7. Unless otherwise provided by law, data classified at classification levels 5, 4, or 3—and data originating from systems in these levels—may be stored only on the College's infrastructure. Such data may be stored on portable computers or storage media only using full-disk/device encryption, to prevent access to the data in the event of loss.
9.8. Third-party data storage providers that may use the data hosted with them for their own purposes must not be used; verifying this is the responsibility of the person arranging the storage. In the event of an incident affecting College-owned data hosted with an external data storage provider, liability rests with the manager who authorized the placement and the staff member who executed it.
9.9. Operators of the information systems may process data solely to perform their job duties, only to the extent necessary, and in compliance with their confidentiality obligations.
9.10. Every user must conserve the IT system's resources, especially mailbox storage.
9.11. The provisions of the IT and Security Policy (IBSZ) must also be observed when users represent the College in any professional organization.
9.12. If a user's conduct endangers the College's data assets, IT infrastructure, or the operational processes that rely on them, the operator may exclude the user from the service and revoke their access rights.

9.13. Intentional breaches of the IT and Security Policy (IBSZ) may be sanctioned in accordance with applicable laws and the College's regulations.

10. Duties and Responsibilities of the IT Department

10.1. The head of the IT Department serves as the College's Information Security Manager. The head of the IT Department is responsible for the College's information security governance and for drafting, reviewing, and updating its Information Security Policy. The IO monitors compliance with the IT and Security Policy (IBSZ) and, in the event of an incident, takes steps to investigate it, eliminate the root causes, prevent further incidents, and restore normal operations.
10.2. The IO oversees, coordinates, and operates all IT equipment and services owned by the College and its organizational units. The IO coordinates the College's software procurement and maintains the software inventory.
10.3. The IO authorizes the deployment of new IT components. When granting this authorization, the IO assesses the component's compatibility with the existing IT systems, with particular emphasis on information security compliance. If any such deficiency is identified in the system, the head of the IO shall refuse authorization for deployment; in that case, the device must not be deployed.
10.4. Upon request, the IO provides technical assistance to the designated staff member of the organizational unit responsible for the service in formulating the IT specifications and parameters of contracts the unit intends to conclude.
10.5. The head of the IO, or staff designated by them, conduct compliance assessments of IT systems against the IT and Security Policy (IBSZ) and provide related advisory support.

11. Sanctions for Breaches of the IT and Security Policy (IBSZ)

11.1. Where the IT and Security Policy (IBSZ) designates an organizational unit as responsible for a given process, the head of that unit is responsible for ensuring compliance with the IBSZ, and the head of the unit providing the service shall be primarily liable for any resulting damage.
11.2. Under the IT and Security Policy (IBSZ), users may be subject to the following sanctions:

- The head of the IO determines the immediate measures to stop the violation. Based on the head of the IO's recommendation, the Rector decides on any further action, which may result in partial suspension of the service or exclusion from it.
- Determination of liability and compensation for the damage caused.

11.3. Sanctions may be imposed on users only if the operator of the relevant system documents the event or incident warranting the sanction, or if it is detected by the IO.
11.4. For persons in a civil-law relationship with the College, matters of liability and compensation must be handled in accordance with the rules of civil law.

12. Environmental and Physical Security

Physical Security Perimeters.

12.1. Critical components of systems classified at level 5—particularly servers, storage subsystems, routers, and patch panels—may be operated only in purpose-built rooms that meet the required security specifications. Rooms must be secured with high-security locks or an electronic access control system, and with fire protection. When an access control system is used, a system capable of logging access events must be implemented.
12.2. The head of the IO may grant entry authorization to rooms housing components of classification level 5 systems to IO staff or contracted partners. Entry authorization must not be transferred to another person. Responsibility for any unauthorized entry rests with the person who handed over access.
12.3. Information about the institution's IT system components may be disclosed only with the IO's authorization. Publishing any information about the IT system on public websites or social media platforms is strictly prohibited.
12.4. Physical Security of Offices, Rooms, and Other Facilities.

- Compliance with the "clear-desk, clear-board, and clear-screen" policy is required across all College premises. Accordingly, every computer must be locked whenever it is left unattended. Wherever possible, the operating system's automatic locking feature should be enabled. Only public-access computers may be operated without password protection.
- Documents may be left in view only for as long as necessary. Documents must not be left in or on printers or copiers. At the end of the workday, if no other work-related activity is running on the computer, it must be shut down, and all documents must be stored in lockable office furniture.
- The use of other work areas required to operate the IT systems follows the same rules as general secure areas. IT equipment and storage media containing special or protected data may be kept only in IO offices or in rooms secured by an access control system.
- The IO decides on the design and modification of rooms designated for IT use.

12.5. Protection Against External Environmental Damage.

- Critical physical components of classification level 5 IT systems may be operated only in rooms equipped with fire and lightning protection systems that comply with applicable legislation.
- On a case-by-case basis, the head of the organizational unit responsible for the service may set additional requirements.
- In accordance with fire safety regulations, electrical supply systems must be equipped with a fire-service main switch (emergency power-off) that enables safe firefighting.
- Each room must be provided with sufficient cooling capacity to remove the heat load generated there. Rooms housing components of classification level 5 systems must be equipped with redundant cooling systems.

12.6. Work Activities.

- In rooms housing components of classification level 5 systems, any work not carried out by IO-designated personnel that could endanger the IT systems or their operation may begin only after prior consultation with the IO.
- The consultation shall be conducted by the third party carrying out the work and the head of the IO or their designated representative. Work that could endanger the room's mechanical systems may be carried out only after prior consultation with, and approval by, the party operating those systems.
- All affected College staff must be notified at least 2 days in advance of any planned work that will result in a service outage.

12.7. In rooms housing components of classification level 5 systems, any transport activity may be carried out only under the supervision of a College staff member with entry authorization.

12.8. Any new system component to be installed in server rooms or telecommunications rooms (cable closets) must be approved in advance by the Head of IT. Approval may be refused if the room lacks the necessary free space, power supply capacity, or cooling capacity.

12.9. When third-party IT equipment is hosted, the College may charge its owner for the costs of electricity consumption, cooling, and storage.

12.10. Maintenance of IT Equipment.

- Each IT component's operator must assess its maintenance needs, determine its maintenance cycle, and follow it at the prescribed intervals.
- During maintenance, any identified vulnerabilities must be remediated, and the work must be carried out so that no new vulnerabilities are introduced. The device's operator is responsible for carrying out the maintenance.

12.11. Rules for Equipment Used Outside the College's Premises.

- IT equipment may be removed from the College's premises only with the written authorization of the head of the relevant organizational unit. Any movement of equipment must be accompanied by a handover-and-acceptance record or a delivery note. IO staff performing their job duties are exempt from this rule.
- The person removing the equipment is liable for any damage caused during or as a result of the removal—particularly harm to the College's data assets or data security—if the damage is attributable to their fault. Unless unavoidable, institutional data classified at classification levels 5, 4, and 3 must not be copied; instead, the relevant system must be used. If copying the data is

unavoidable, such data may be taken outside the institution only in encrypted form. Exporting the data requires authorization from the operator of the relevant system.

12.12. The data stored on storage media that are no longer in use or have failed must be destroyed in a manner that renders it unrecoverable. If the device has failed, the storage media must be handed over to IO staff so they can carry out its secure destruction.

12.13. To prevent the unauthorized disclosure of paper-based information, documents that are no longer needed must be destroyed so that their contents cannot be accessed by unauthorized persons; where possible, a document shredder should be used. It is strictly prohibited to place them in waste containers without prior destruction.

12.14. IT equipment must be decommissioned with the involvement of IO staff. During the procedure, the grounds for decommissioning are determined and, where necessary, the data content is securely removed.

13. Development and Support Tasks

13.1. Development tasks at classification levels 4 and 5 may be performed only in an environment separate from the original system. If access to protected data is indispensable for carrying out the development tasks, the development system must be classified at the same security level as the original, and access rights must not exceed those in force in the original system.

13.2. For any software whose service interface or feature set has changed, the testing procedure must be repeated. The testing requirement applies not only to applications but also to the environments in which they run (web servers, database management systems, etc.), but it must extend only to the functions in use. The results of the tests must be recorded in a test report.

14. Operations Management

14.1. Deployment of a New IT System.

- The IO will fulfill an organizational unit's service request only if the request complies with the IT and Security Policy (IBSZ). IO staff will meet the service request either using IO's own services or—after consultation with the head of the requesting organizational unit—using the software requested by the unit.
- If an organizational unit plans to deploy new software, its security classification must be determined at the design phase, and the operational rules must be set accordingly.
- If an organizational unit intends to deploy new software on the College's infrastructure, the software must comply with the requirements of the IT and Security Policy (IBSZ) and with legal requirements, in particular the GDPR. The software developer must provide a declaration of conformity, which an IO staff member will verify. The College will pass on to the software vendor any losses arising from non-compliance.

14.2. Cryptographic Principles

- Cryptographic controls must be implemented throughout the IT system wherever feasible and proportionate to the risk.
- Cryptographic controls are mandatory for system logins and for all data-transmission channels.
- Information systems must not store passwords in a form that can be decoded with low computational effort. No system using such encoding may be deployed; t treat replacing the password-hashing mechanism in existing systems as a high-priority task.

14.3. Legal Compliance

It is prohibited to use any College-owned IT equipment or services for unlawful activity, including the use of illegal or unlicensed software—especially any involvement in distributing such software.

14.4. Malicious Software

- Systems that may be exposed to malicious code must have anti-malware software installed to detect and remove it.
- Users may use personally owned devices and storage media on the College's infrastructure only if they subject them to this IT and Security Policy and comply with the rules governing their use. The person who connects a personally owned storage device to the College's IT system is liable for any resulting damage.

14.5. The College may provide a portable computer to staff whose duties require it. For College-owned portable computers, full-disk/device encryption must be enabled.
14.6. A College-owned computer assigned for personal use may, where justified, also be used for private purposes—but only by the recipient. In the case of private use, personal data must be kept clearly separate from other data stored on the computer, under a folder specifically designated for this purpose named Személyes_adatok; storing personal data anywhere else is prohibited. IT staff may not perform any maintenance tasks in this folder, may not view its contents, and may not back it up. Private use and the storage of personal data must not impede the performance of institutional duties. When returning the computer, the user must delete the Személyes_adatok folder.
14.7. Only properly licensed software may be run on College-owned computers; in particular, running software from illegal sources or cracked software, and downloading illegal content, are prohibited. Running game software is not permitted under private use.
14.8. Every staff member is responsible for the security of College-owned equipment. Any fault or damage affecting College-owned equipment must be reported to the IO without delay. The user of College-owned equipment must not have it repaired without the authorization of the head of the IO.
14.9. If a College-owned IT device is stolen, the head of the relevant organizational unit or the device's user must file a police report. Based on the police report, the College determines the extent of the damage and the degree of the staff member's liability.
14.10. Each staff member may be issued only one portable computer for the performance of their duties, even if they hold multiple roles.
14.11. College email addresses must not be used for private correspondence or for accessing personal services. The contents of an institutional mailbox may be disclosed to another user only with the owner's written authorization, and solely to ensure the uninterrupted operation of the institution. The transfer of mailbox contents may be initiated only if no other means are available to maintain operational continuity.
14.12. Backup Procedures.

- The operations manual for every information system classified at levels 5 and 4 must include the backup procedure for the system and its data, covering the backup frequency, the backup method, the designation of the person responsible for backups, the period and frequency of backup verification, and the designation of the person responsible for verification.
- For systems classified at level 4 or lower, on-site backups are also acceptable.
- The backup strategy must in all cases be designed and implemented so that, in the event of any component failure or data loss, the system can be restored to operability with an acceptable level of data loss. The recovery plan must also include the procedure for restoring the entire system. The backup and recovery plans must be reviewed whenever systems are upgraded and at least once a year; responsibility rests with the IT staff member in charge of the system.
- The data of classification level 5 systems must be fully backed up at the end of each working day. The backup method must ensure that backups can be restored to a test system. For data of systems classified at level 4 or lower, incremental backups may also be used. Depending on their operational duties, application operators may also perform ad hoc backups.
- For every system classified at level 5, a restore test must be performed at least once a year to verify that the original system and its data can be reliably restored from the backups. The restore test must be performed in an environment that is functionally equivalent to the original. The restore test and its results must be documented in writing.

14.13. Network Security Management

- The College's entire network and telephony infrastructure is built according to a unified design and implementation strategy. The IO staff define the guidelines and perform the deployment, sometimes with the involvement of an external service provider.
- The IO operates a unified institutional Wi-Fi network. Because it poses a particularly high security risk, deploying any Wi-Fi endpoint (router or access point) without approval is strictly prohibited.
- Only IO-authorized and approved devices may be connected to the communications network.
- Only internet access authorized and approved by the IO may be used on the College's premises. Without the IO's authorization and supervision, it is strictly prohibited to have any external network connection terminate on an internal network service—for example, by hosting a VPN server or creating tunnels.

- Unused network ports must be disabled. The IO operates the College's firewall system. The firewall's default security configuration is to deny connections. Communication channels required for specific services may be opened in accordance with the operating requirements of the relevant system. Opening additional firewall ports may be done solely to enable the operation of software required for work.
- The firewall configuration must be reviewed regularly, and any communication paths that are no longer required must be closed.

14.14. Media Handling.

- Storage media holding backups of data from classification level 5, 4, and 3 systems may contain data protected by law, including personal data. The handling of these storage media is governed by the same rules that apply to the system components on which the data were originally stored.
- Storage media containing backups of data from classification level 5, 4, and 3 systems must be stored in a separate room designated by the IO, in a locked metal cabinet or safe. The person with access to the cabinet must keep records of the storage media and of any access to them.
- The IO is responsible for removing storage media from the backup set and for their secure destruction.

14.15. Service Activities.

Before handing over any IT device for servicing, measures must be taken to prevent unauthorized access to the data it contains.

14.16. Information Exchange.

- Establishing any connections or processes that implement automated data exchange for data of systems classified at levels 5, 4, and 3 requires authorization from the head of the IO and from the head of the organizational unit operating the system. In the connection request, operators must clearly detail the purpose of the data processing and the technical solution to be used, with particular emphasis on the technical measures that ensure the security of the data exchange.
- The operator of the application initiating the data exchange must document the data-exchange environment and the technical solutions.

14.17. Monitoring.

- The IT system is monitored by an external service provider.
- The monitoring system must cover the status and operational monitoring of servers, active network devices, managed printer–copier devices, and all other IT equipment that can be connected to the system.
- The monitoring system must send alerts about system events to the operations staff. Alerts must include the event time, severity level, and description. The alert-handling procedure must be hierarchical: when the response deadline for an event type expires, the task must be escalated to the supervising manager.
- The monitoring system must enable the annual availability of IT equipment to be calculated from its data.
- Events recorded by the monitoring system must be retained for two years.

14.18. Archiving.

- College systems that have been retired must be archived if so ordered by the head of the relevant organizational unit. The archived system must allow searching its stored data, but must not allow adding new data or altering existing records. Archived systems must be security-classified, based on the nature of the data they hold, in accordance with the rules applicable to systems in use.
- The same rules apply to archived systems as to systems in use, with particular emphasis on defining access rights.
- Regular backups are no longer required for archived systems, but an off-site backup must be maintained from which archived systems can be restored if necessary.

15. Human Resources

15.1. Access to the College's information system is based on the College's directory service, which is operated by the IO.

15.2. When a new staff member is hired, their data must be entered into the IO's directory service. The staff member designated by the head of the Financial Affairs Office sends the necessary data to the IO after the hiring decision.
15.3. As a rule, only employees of the College on indefinite or fixed-term contracts may be included in the directory service. For staff engaged under a service contract, only access valid for the duration of the engagement and appropriate solely to performing the specific duties may be granted. Access must be automatically revoked upon the expiry of the service contract or the employment relationship.
15.4. In every information system, College employees may be granted only those access rights that are necessary to perform their job duties.
15.5. Upon termination of a staff member's employment or engagement, their access rights must be revoked. The revocation is carried out by completing the designated clearance form. Upon approving the form, the IO staff member revokes the staff member's access to the IT systems effective on the termination date and retrieves any IT equipment issued to them. Following termination, the staff member may continue to receive messages sent to their institutional email address for one month, but may no longer send email.
15.6. If a staff member requires continued access to the College's information system after the end of their employment or engagement, it may be extended upon a written request by the head of the requesting organizational unit. The extension may be granted only for a fixed period; any access rights whose validity has expired must be automatically disabled.
15.7. Following termination of the employment or engagement, the staff member must not retain any copies of any part of the College's data assets. Confidentiality obligations survive the termination of the employment or engagement.

16. Access and Permissions Policy

16.1. Access Policy.

- Authentication. All data and services stored in the College's information system must be protected by access controls. Access rights must be provisioned on a per-user basis. Access rights may be used only by the individual to whom they were issued. Authentication may be performed using a username and password.
- Authorization. Roles must be defined in each subsystem for access control; where roles are not available, object-level permissions must be specified. Roles and access rights must be defined and configured according to the principle of least privilege, ensuring the user can still perform their duties. The principle of least privilege applies equally to heads of organizational units; they must not be assigned any access rights that are not required for their role.
- Without access rights, only publicly available data may be retrieved from each system.
- Roles and access rights must be reviewed once a year. The outcome of the review must be verified and approved by the head of the organizational unit that operates the system.

16.2. In every system, access passwords must be stored using one-way password hashing. Components that store passwords in plaintext or use outdated encryption are not permitted to operate within the College's IT system. The required encryption algorithm must be SHA-256 or more advanced.
16.3. The passwords required for systems with security classification levels 5, 4, and 3 must be changed at specified intervals.
16.4. The College's systems must be designed so they do not allow the use of weak passwords.
16.5. Every system must cap the number of consecutive failed sign-in attempts. Failed sign-in attempts must be logged. Beyond logging, systems with security classification levels 5, 4, and 3 must, where feasible, have the automated security monitoring and alerting system notify the operations team about sign-in attempts.
o16.6. When granting access to systems with security classification levels 5, 4, or 3, the head of the unit operating the system must explicitly brief the user to comply with the IT-Security Policy (IBSZ).
16.7. Directory Service.

- To implement a central register within its information system, the College establishes a central directory service. The directory service must include every person employed by the College.
- To avoid duplicate administration, each IT system should, where possible, authenticate against the directory service.

- Each user is responsible for keeping their information in the directory service up to date. If any of these details (phone number, email address, room number, job role, etc.) change, the employee must update them without delay.

16.8. Remote Access.

- The head of the IO oversees the College's internet access. Establishing any additional internet connections at the College is prohibited without the authorization of the head of the IO.
- To enable remote work, the College provides VPN access for its employees. The IO is responsible for deploying and overseeing VPN endpoints. Installing a VPN server without the IO's authorization is strictly prohibited.

16.9. Operating System Access.

- On any computer used to access systems with security classification levels 5, 4, or 3 with a privileged account, users must not have local administrator (full) rights.
- Where justified, full administrator rights may be held by a person designated by the head of the relevant organizational unit or by an IO staff member.

16.10. Logging.

- Log events generated in the IT components of systems with security classification levels 5, 4, and 3, as well as in server software and applications, must be logged.
- In systems with security classification level 3 and below, system-level log events from the operating system and server software must be recorded.
- Log events must also be stored on a dedicated log server.
- Log events must be retained for one year.
- Logging shall use TCP connections, and timestamps shall be recorded with millisecond precision.
- All event logs affecting the security of the IT system's components shall be retained on the log servers. Log collection and retention must be capable of evidencing any unauthorized access and enabling the determination of responsibility.
- The contents of the event logs shall be reviewed regularly, by automated or manual means.
- In the event of an incident, log events shall be reviewed without undue delay and shall form the basis for developing the incident management measures.

17. Compliance

17.1. Ensuring ongoing compliance with applicable laws and regulations is the responsibility of the head of the relevant organizational unit.

17.2. The head of the relevant organizational unit is not liable for violations of law committed by the system's users, including unauthorized data processing and copyright infringement.

17.3. Upon a lawful request by a competent authority, the College shall disclose the data prescribed by law and, where necessary, shall cooperate with the authorities in the matter to the extent required by law.

17.4. For any system operated in non-compliance with the IT-Security Policy (IBSZ), responsibility for any incident rests with the head of the relevant organizational unit.

18. Acceptance Procedure for New Information Systems

18.1. Before any new information system is rolled out, consultation with the service operators must take place during the design phase, covering the following points:

- The system's developer, its operators, and its lifecycle must be specified.
- The operators must approve the system's functions and procedures related to data storage and secure operation. If secure operation cannot be ensured, the operators may refuse to operate the system.
- The scope of support tasks, the responsible personnel, and the service-level agreement (SLA) must be defined and approved for the system's entire lifecycle.
- Ensuring Continuity of Operations

18.2. Systems with security classification levels 4 and 5 must have a Business Continuity Plan (BCP) in place. The plan must include incident management procedures; the operating procedures for the organizations

using the system in the event of an outage of individual components or of the entire system; the backup plan; and a description of the verification procedures.
18.3. The preparatory items, standby services, and resources specified in the Business Continuity Plan must be provisioned during normal operations. The staff of the relevant organizational unit must be briefed on the applicable sections of the Business Continuity Plan.

19. Information Security Incident Management

19.1. Any unusual events—or any deviations from normal operation—affecting the College's information system or data assets must be reported to the service operator.
19.2. The service operator and the IO shall establish communication channels for receiving incident reports for all IT systems and data assets under the College's management. For the IO, the channels are: email, phone, or in person with the head of the IO.
19.3. Upon detection or discovery of any security issue relating to an IT system, it shall be reported to the operator of the system concerned and to the IO. Exploiting a security vulnerability constitutes an offence under the Criminal Code. The College will initiate legal proceedings whenever the person who discovered the vulnerability fails to report it to the operators or publicly discloses it.
19.4. When reporting a security incident, the reporter shall attach all information in their possession that may be required to handle the incident.
19.5. In the event of widespread impact, the operators shall provide updates through the standard communication channels. Systems with security classification levels 4 and 5 must have a Business Continuity and Incident Management Plan in place. Operators must classify reported incidents by severity and, accordingly, initiate and conduct the incident management procedure.

20. Transfer of Data Outside the College

20.1. Data from assets classified at security levels 4 and 5 may be disclosed only with the Rector's authorization, except for disclosures mandated by law.
20.2. Personal data may be disclosed only by authorized persons, in compliance with applicable legislation, with particular regard to the relevant provisions of the GDPR, and in accordance with the College's internal regulations.
20.3. Under applicable law, the receiving party is responsible for protecting the transferred data. Before the transfer, the disclosing party may seek guidance from the head of the IO on data protection and information security matters.

21. Review of the IT-Security Policy

21.1. This IT-Security Policy shall be reviewed every three years. The date of the next scheduled review shall be set when the document is finalized. The IT-Security Policy shall also be reviewed whenever:

- a change in law affecting it enters into force, or a technical or information-security change occurs that requires amending the IT-Security Policy,
- new business processes, organizational units, or services are introduced or discontinued,
- a new material risk is identified,
- to implement measures following the analysis of a security incident.

21.2. Comments and change requests regarding the IT-Security Policy shall be submitted to the head of the IO. The request must include the submitter's details, the number(s) of the paragraph(s) proposed for amendment, the proposed new text, and the justification.

22. Closing provisions

This IT-Security Policy was adopted by the College Senate by Resolution No. 30/2025 (07.10.).

Budapest, 10 July 2025

Gábor Karsai rector