BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVO
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Pursuant to Article 35, paragraph 1, subparagraph 1.1 of the Law No. 03/L-209 on Central Bank of the Republic of Kosova (Official Gazette of the Republic of Kosova, No.77 / 16 August 2010), amended and supplemented by Law No. 05/L -150 on Central Bank of the Republic of Kosova (Official Gazette of the Republic of Kosova, No.10 / 03 April 2017), as well as Article 7, paragraph 7.4, subparagraph (c), Article 15, paragraph 15.7, subparagraph (e), and Article 22, paragraph 22.7, subparagraph (e) of Law No. 04/L-101 on Pension Funds of Kosova (Official Gazette of the Republic of Kosova, No.10 / 8 May 2012), amended and supplemented by Law No. 05/L -116 on amending and supplementing of Law No. 04/L-101 on Pension Funds of Kosova, amended and supplemented by Law No. 04/L-115 and Law No. 04/L-168 (Official Gazette of the Republic of Kosova No.3 / 17 January 2017), the Board of the Central Bank, in its meeting held on 28 February 2024, approved the following:

REGULATION ON SYSTEMS AND INFORMATION SECURITY FOR PENSION FUNDS

Article 1
Purpose and scope

1. The purpose of this Regulation is to determine the minimum criteria and conditions that pension funds must meet for the organization and operation of their information technology systems (hereinafter referred to as IT), which enable the reduction of the operational risk that may be caused by the misuse of IT systems, as well as to maintain the reliability of these systems in supporting the activities of pension funds. The minimum criteria and conditions determined in this Regulation are related to the management, security and operation of the information systems of pension funds, as well as to ensure the continuity of operation in case of any disaster event.

2. This Regulation shall apply to pension funds operating in the Republic of Kosova, hereinafter referred to as fund/s or pension fund/s.

Article 2
Definitions

1. All terms used in this Regulation shall have the same meaning as defined in Article 1 of Law No. 04/L-101 on Pension Funds of Kosova, and Article 1 of Law No. 04/L-168 on amending and supplementing of Law No. 04/L-101 on Pension Funds of Kosova and/or further defined for the purpose of this Regulation:

    1.1. **Information system** – means the entire technological set consisting of infrastructure (software and hardware components), funds (institution), people and procedures for the collection, processing, display and use of data and information, transmission and storage;

1.2. **Information system users** - means all persons authorized to use information systems (institution employees, employees of other companies who have access to the information of the pension fund system);

1.3. **Pension fund** - means the Pension Savings Trust, as well as other pension funds licensed by CBK.

1.4. **Software Components** – means all types of operating system, application software, software development tools and other software systems;

1.5. **Hardware components** – means computer equipment, network equipment, data storage media and other technical equipment, which serve as support for the operation of information systems;

1.6. **Assets** – means tangible and intangible assets that have value to the pension fund;

1.7. **Clean table** – means removing all documents and other confidential assets from the work desk during the unsupervised period and at the end of working hours;

1.8. **External service provider -** means any natural or legal person who, on the basis of a written agreement, provides service to the fund for the functions delegated by the fund;

1.9. **Incident** – means an unplanned event that is not a normal part of operations and that interrupts a process or a service or reduces the quality of service;

1.10. **Server area** – means the area where are mainly stored and located servers and other auxiliary equipment, which are needed for communication services, signalling and other electronic equipment where bank notes are stored.

1.11. **Internationally accepted standards -** means ISO/IEC 27000 series; NIST 800; COBIT; ITIL and similar.

1.12. **Cloud services** – mean infrastructure, space and application resources that exist on the Internet (eng. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The providers of these services/resources contract with the recipients of services to allow you to use computer resources without having to purchase or maintain physical or software equipment.

Article 3
Management of information systems

1. The pension fund must develop an appropriate information system, which must include the following requirements:

1.1. Must have the functionality, capacity and performance to provide support required by the processes of the fund's activities;

1.2. Provides timely, accurate and complete information for the institution's decision-making and risk management, to enable security and stable operation of the pension fund;

1.3. Provides appropriate data verification/validation control, during the processing process and during data extraction, to prevent inaccuracies and inconsistencies in data and information;

2. The pension fund monitors, adjusts and continuously improves the IT management process to reduce exposure to risk while maintaining its security and functionality.

Article 4
Organizational structure for IT management

1. The pension fund in its organizational structure must establish an IT unit with the sufficient and appropriate number of staff to ensure that the field of IT is managed efficiently based on internationally accepted standards. The assignment of duties should be done according to internationally accepted standards with clearly defined responsibilities and competencies for the IT management process and information security. This unit must document regular informative reports, at least on a quarterly basis, for the senior management of the pension fund.

2. The pension fund must appoint the person responsible for information security that must manage the security of information system and align the policies and processes for information security related to functions and technological platforms. The responsible person reports to the managing director and must be independent from other organizational units. The responsible person must report through the managing director at least once a year and as needed to the Board of Directors who must be informed about operations and functions related to information security.

3. In the case of outsourcing the IT functions to the external service provider, the pension fund must appoint at least one internal employee specialized in the field of information technology, as responsible for the coordination and smooth running of the IT functions..

Article 5
Strategy, Policies and Procedures for IT management and information security

1. The pension fund defines the security strategy and requirements for the operation of IT systems, policies for technology and information security, as well as procedures for field processes.

2. The pension fund, in accordance with the strategy of the institution, adopts strategies for the development of IT systems.

3. The Board of Directors is responsible for approving the technology and information security policies and at least on an annual basis must assess the adequacy of policies and carry out their review.

4. IT strategy and policies are approved by the Board of Directors, while IT procedures are approved by senior management.

5. In cases where the pension fund provides all or part of its IT activity (or systems) from external service providers, then the pension fund adopts an internal procedure for the delegation of functions to ensure compliance with the requirements of this Regulation for security and proper functioning of these systems.

6. The internal procedure for the delegation of functions according to paragraph 5 of this article must include at least the following elements:

   6.1. Identifying the functions that are delegated and evaluating the impact of the delegation of those functions;

   6.2. Procedures for delegating functions, including criteria for selecting the recipient of delegated functions;

6.3. Deadlines and reporting methods of the recipient of delegated functions to the fund;

6.4. Ways of monitoring the recipient of delegated functions, by the pension fund;

7. Policies and procedures for IT management should define at least the following elements:

7.1. Administration and operation of IT systems;

7.2. Organizational structure for IT management;

7.3. Hardware infrastructure for the field of IT (configuration diagrams);

7.4. Classification of documentation and protection of systems and data;

7.5. System data backup;

7.6. System change management (eng. change management);

7.7. Incident management;

7.8. Risk management of IT systems;

7.9. Determination of security mechanisms of IT systems;

7.10. Management of third parties.

8. The pension fund must ensure implementation of all approved internal policies and procedures related to IT, as well as ensure that all IT users are informed of the content of these policies and procedures in accordance with their authorizations and responsibilities.

Article 6
Development and procurement of IT systems

1. To minimize the risk, the pension fund must follow the trend of system developments, making sure to use only updated versions supported by their providers.
2. The pension fund must ensure designing and approval of internal procedures on how it carries out developments, changes, testing, validation and quality assurance to mitigate potential vulnerabilities or operational disruptions in its IT systems. IT systems are put into live operation only after the specialized employee who performs the verification of the applicability of the procedures and proper functioning of the system gives his/her documented approval.
3. Before deploying the system, a risk assessment and compliance analysis should be performed to ensure that the system meets security, performance and functionality requirements.
4. In cases of purchasing the systems, the fund must follow a standardized procurement process. This process should include a thorough assessment of the supplier's reputation, financial stability and track record in providing secure and reliable software solutions. Agreements should clearly state the fund's expectations in terms of security measures, service level agreements and data protection requirements.
5. If the fund chooses in-house software development, it must establish a software development life cycle (SDLC) process. This process should include identifying and implementing secure coding practices, regular code reviews, vulnerability assessments, and testing at every stage of development. The Fund should also establish mechanisms for ongoing maintenance, updates and monitoring of software performance and security.

6. The external service provider during the implementation and work on the systems should not in any way have access to the system versions that are in production (live). Contractors and other external parties should test all changes in a testing environment.

Article 7
Delegation of IT functions to external service providers

1. The pension fund shall be responsible for ensuring that the IT activity is carried out in accordance with all the requirements provided for in this regulation, even in cases where all or part of IT activities are provided by an external IT service provider.
2. Before selecting the external IT service provider, the fund should undertake the following activities:
   2.1. Determining the minimum standards that the external IT service provider must meet and which must be aligned with the business continuity plan;
   2.2. Carrying out risk assessment of pension fund operations that may arise from the use of external service provided during the processing of pension fund activities;
   2.3. Determining on how to monitor the service and quality of the company's operation, financial situation and risk profile through periodic testing of compliance with the information system security policy;
   2.4. Making proper determination of the activity of the external IT service provider from the legal and financial point of view, as well as from the aspect of how it manages the security of information system provided for in this regulation;
   2.5. Defining the coordinated management of security incidents;
   2.6. Determining the necessary measures to avoid conflict of interest;
3. The agreement between the pension fund and the external IT service provider should be defined through a written contract which, among other things, should include:
   3.1. Related party data (pension fund and external IT service provider);
   3.2. Description of delegated functions;
   3.3. Rights and obligations of related parties;
   3.4. Handling with and maintaining the confidentiality of data;
   3.5. Time limits for providing the service and the notice period for the termination of contract, which is sufficient for finding alternative solutions;
   3.6. Service level agreement;
   3.7. Provision determining that the external IT service provider shall be subject to supervision by the CBK regarding delegated IT activities;
   3.8. Provision determining that the IT service providers performs their activities in accordance with the applicable legislation, requirements, regulators, as well as policies approved by the pension fund and to cooperate with the CBK in terms of delegated functions;

3.9. The right of the pension fund to be informed about the progress of the functions delegated by the external IT service provider, as well as the right of the fund to give general or special instructions regarding the performance of the delegated functions;

3.10. The right of the pension fund to inspect and control the activity of the external IT service provider related to the delegated IT activities;

3.11. Obligation of the external IT service provider to immediately inform the pension fund of any fact that may have a significant impact on its ability to efficiently and effectively perform its activity according to the applicable legal requirements;

4. The external service provider may not subcontract the services unless specified in the basic agreement concluded between the pension fund and this service provider.
5. The pension fund shall be obliged to manage the risks deriving from contractual relations with external service providers whose activities are related to the information system used by the pension fund.
6. The pension fund shall be obliged to continuously monitor the method and the quality of activities contracted by the external service provider.

Article 8
Security of information systems

1. The security of information systems is based on determining the fulfilment of the following criteria:

   1.1. **Confidentiality**: information must be accessible only to authorized users;

   1.2. **Integrity**: maintaining the accuracy and completeness of the information system;

   1.3. **Availability**: access at any time to the information system for authorized users.

2. The pension fund must continuously manage the security process of the information system. The pension fund must identify and monitor the needs for the security of information system, at least based on the results of the risk assessment of that system and obligations arising from internal acts or contractual relationships.
3. The pension fund must determine the procedures, methods and criteria for classifying information according to the degree of sensitivity and relevance - in relation to the possible consequences of breach of confidentiality, their integrity and availability.
4. The pension fund must ensure that information security and all activities related to it are in compliance with all applicable laws that relate to the institution's information and operations.

Article 9
Security in *cloud* services

1. The recipient of *cloud* services must prepare and define policy and procedure for the management of *cloud* services.
2. *Cloud* service providers must have experience and an affirmative reputation in providing *cloud* services.

3. *Cloud* service providers must adhere to internationally accepted standards in order to ensure the security, integrity and confidentiality of data processed, stored or transferred through their platforms, always adhering to information security practices, procedures and policy of service recipients, as well as complying with all applicable laws and regulations. Providers of these services must establish comprehensive security measures that include data classification and protection, access controls, encryption methods, incident response plan and procedures, and disaster recovery and business continuity plan.

4. Recipients of *cloud* services must assess the security measures implemented by *cloud* service providers and regularly monitor their compliance to mitigate potential risks that compromise data security or unauthorized access.

5. The security controls of service recipient (operational, procedural or technical procedures to protect the integrity, confidentiality and accuracy of the service recipient's data and information systems) must be implemented by the *cloud* service provider correctly and effectively.

6. *Cloud* service providers must provide *cloud* space that is physically separated from other customers' spaces, and must have audit trail collection and retention procedures and policies to ensure that every activity is effectively monitored.

7. Remote access to information systems hosted in *cloud* spaces must be enabled with methods of authentication with two or more factors (multi-factor authentication). Device-to-device communication accessing *cloud*-hosted services/resources remotely must have *end-to-end* encryption measures in place for each communication session.

8. Infrastructure configurations, the list of services/resources that are provided in *cloud* spaces, as well as the list of applications that run in *cloud* spaces should be transparent and documented in detail.

9. The *cloud* service provider must provide a procedure and policy for creating, testing and protecting the backup that is consistent with the policies and procedures of the service recipient.

10. In the event of unauthorized access or any security incident, *cloud* service providers are required to immediately report such incidents to regulatory authorities and service recipient.

11. *Cloud* service providers must provide transparent documentation about their security practices and make this documentation available for review during the examination or audit process.

12. A *penetration* test and assessment of vulnerabilities and possible security risks related to keeping data and information systems in *cloud* spaces must be done at least once a year.

13. The service provider must have a policy or procedure for secure data deletion and destruction of the infrastructure in the event of termination of the contract or removal of service resources from use.

14. CBK shall have the right to conduct regular examinations and assessments of *cloud* service providers in the pension industry to verify compliance with information security standards and best practices.

All requirements of this Regulation on information systems are also applied accordingly to *cloud* service providers related to services in *cloud* spaces.

Article 10
Risk management for information systems

1. The pension fund sets criteria for permissible risk in relation to the use of its information systems according to internationally accepted standards.

2. At least once a year or in any case of significant changes in information security requirements, the pension fund conducts risk analysis of information systems to ensure that this risk is kept within acceptable limits related to the fund's activity. The results of the risk analysis shall be documented.

3. The risk assessment process includes, but is not limited to, the following steps:

   3.1. Identification of system requirements and objectives.

   3.2. Assessment of vulnerabilities and potential security risks associated with the system.

   3.3. Assessment of potential impact on fund operations, data privacy and data subject confidentiality.

   3.4. Assessment of system compatibility with other systems and existing infrastructure.

   3.5. Evaluation of system extensibility, reliability and maintainability.

   3.6. Analysis of potential legal and regulatory compliance issues.

   3.7. Assessment of financial and resource implications of internal implementation, acquisition or development.

4. Based on the outcomes of the risk assessment, the fund must develop a risk mitigation plan that describes necessary measures to minimize the identified risks. The risk mitigation plan should include, but not be limited to:

   4.1. Implementation of appropriate security measures for data protection.

   4.2. Creation of data backup and recovery procedures.

   4.3. Integration of the system with other systems and existing infrastructure.

   4.4. Providing necessary training and support to employees involved in implementation, acquisition or development of the software.

   4.5. Compliance with relevant legal and regulatory requirements.

   4.6. Allocation of adequate financial and human resources to ensure successful internal implementation, acquisition or development.

5. Funds should regularly review and update the risk assessment and risk mitigation plan throughout the software lifecycle to address any emerging risks or changes in the fund's requirements and operating environment.

6. The pension fund must notify the CBK in writing in case of identification of incidents, in the information systems and changes in the key functions of important processes of the information systems which may hinder or endanger the institution, no later than one working day after the incident occurred.

7. The information system risk management should include the entire information system of the integrated fund at all stages of its development.

8. The information system risk management must include the annual awareness plan of the fund's employees for the adequate use of services provided through the fund's information system.

Article 11
Physical security of information systems

1. The pension fund must take necessary security measures to prevent any unauthorized physical access, interference or damage to information, information processing equipment and fund operations based on internationally accepted standards.
2. The pension fund must establish access and work procedures for security areas for all employees and external parties. Security areas must be protected through access controls to ensure that only authorized employees have access.
3. Security measures should also be set for the equipment used and placed outside the pension fund facilities, and depending on the location and the risks should be taken into consideration when determining the necessary controls.
4. Equipment must be maintained to protect against failures, to ensure continuous availability and integrity, and to withstand interruptions as a result of auxiliary equipment failures, natural disasters, malicious or accidental attacks, etc.
5. All devices containing information must be verified to ensure that all data and licensed software have been removed prior to disposal, destruction or reuse to prevent recovery of the original information.
6. All users must be made aware of the safety requirements and procedures for protecting unattended equipment.
7. The fund must define criteria, methods and procedures for a clean table in order to protect information.
8. Contractual obligations for employees and external IT service providers should reflect the pension fund's information security policies. All employees and external IT service providers must understand responsibilities for the roles being considered.
9. Where appropriate for application, the fund shall determine that employees and external service providers retain information obtained during the exercise of their activity for a certain period after the termination of the contractual agreement with the employee or external IT service providers.
10. The fund must determine the actions and measures to be taken in case of violation of security requirements by employees or external IT service providers.

Article 12
Management of computer networks

1. The computer network of the fund must be managed and controlled in order to protect the information of the systems and applications. The fund must implement controls to ensure the protection of confidentiality and integrity of information on the network and protection of services from unauthorized access based on internationally accepted standards.
2. For the management of computer networks, the fund must determine:

2.1. The procedure for the use and management of network services and equipment in order to limit access to network services and applications;

2.2. Establishing special controls to protect the confidentiality and integrity of data passing through public or wireless networks;

2.3. Technology applied to the security of network services, such: as authentication, encryption and network connection controls;

2.4. Groups of information services, users and information systems must be isolated from public networks;

2.5. Special controls should be devoted to the access of external service providers in cases of the need for interconnection (connections with third parties).

Article 13
Information systems asset management

1. The fund must identify all assets in the information systems.
2. The Fund must maintain an inventory of all assets with all necessary information, including asset type, format, location, backup information (where applicable), license information and business value.
3. The fund must determine and document the ownership and classification of all assets related to information processing.
4. The owner of the asset shall be responsible for:

   4.1. Ensuring that information and assets related to information processing are classified according to their sensitivity;

   4.2. Defining and regularly reviewing restrictions on access and classification.
5. The fund must determine the rules on the acceptable use of information and assets related to information processing.

Article 14
Managing of users access

1. The Fund manages access to information systems through relevant internal procedures for managing user access rights. Internal procedures must contain criteria for access, authorization, identification and authentication of users according to internationally accepted standards.
2. Each user must be unique and the system must define password setting criteria according to internationally accepted standards. Before granting access to information systems, both internal fund employees and external service providers must sign confidentiality and non-disclosure agreements.
3. The fund must ensure that the authorization of user’s access to information systems is done by the responsible persons of those systems and is based on the principle of the lowest possible access to the system, enabling the performance of tasks. The fund must at least on a 6-month basis review

the users access rights in the systems of high importance based on the risk assessment and at least on an annual basis all other systems.

4. In managing user access rights, the fund must specifically authorize privileged access and/or remote access to the information system. All access and activity of privileged users and remote access must be monitored.
5. Remote access to information systems must be enabled with methods for authentication with two or more factors (multi-factor authentication). Communication between device accessing the information system remotely must have *end-to-end* encryption measures in place for each communication session.
6. The pension fund must monitor and store information security events in their infrastructure based on internationally accepted standards.

Article 15
Information storage

1. Information storage (backup) must be done according to internal procedures of the pension fund.
2. Internal acts according to paragraph 1 of this article must contain at least the following elements:
   2.1. Setting the necessary level of information backup;

   2.2. Keeping correct and complete data on the information backup, as well as documented backup recovery procedures;

   2.3. The type (full, incremental, differential) and frequency of backups according to the complexity of the business.
3. Backups should be scheduled to ensure that all information and software can be recovered in the event of a disaster or equipment failure.
4. Backups should be stored in a second location, far enough away to not be vulnerable to the same threats as the central location.
5. Backups must be provided with the appropriate level of physical and environmental protection consistent with the standards applied at the central location.
6. Backups should be tested regularly, ensuring they are reliable and usable when needed.
7. Backups must be protected from unauthorized access through encryption.
8. The duration of information storage must be done according to the applicable legislation.

Article 16
Internal audit of the information system

1. The requirements provided for by regulation on internal controls and internal audit are applied to the audit of the information system.
2. The activity of the IT field should be subject to at least annual periodic review that focuses on the risk-based methodology.

3. IT audits must be performed by competent persons within the internal audit function or by external persons contracted for this purpose.

4. All requirements of this regulation and the rule provided for in paragraph 1 of this article shall remain applicable in cases where internal audit activities are contracted.

Article 17
Server room

1. The server room must be separate from other offices of the pension fund and must be located inside the fund's facilities.

2. In order to enable the record storage and business continuity (as a back-up) in case of disasters or natural disasters, the fund must designate another backup location, where the necessary servers are located. This backup location must be located at a distance from the main center of the fund, according to internationally accepted standards in this field.

3. The pension fund in its central server room and backup location for record storage must meet the following server room security requirements:

    3.1. have the necessary equipment for keeping the temperature at the right level;

    3.2. have the necessary equipment to keep the humidity at the right level;

    3.3. have electronic protection with:

        3.3.1. seismic sensors;

        3.3.2. motion sensors;

        3.3.3. smoke detectors.

    3.4. have a camera monitoring system for:

        3.4.1. the entrance to this room; and

        3.4.2. the interior of this room.

    3.5. to have fire protection.

    3.6. be equipped with a backup and continuous source of electricity.

4. The server room must be restricted for access only to authorized personnel with methods for authentication with two or more factors and monitored through the entry / exit of staff and external persons in these premises.

5. The pension fund must determine the access conditions of personnel and third parties authorized for access to the server room in case of emergencies.

6. At the request of the fund, the Central Bank of the Republic of Kosova may make exceptions to some of the requirements set forth in paragraph 3 of this article, but at the same time the CBK may continuously request fulfilment of minimum security requirements for certain offices.

Article 18
Continuity of operation following an interruption as a result of extraordinary events

1. The pension fund must establish a business continuity management process in order to ensure uninterrupted and continuous operation of all critical systems and processes, as well as to limit losses in conditions of irregular operation based on internationally accepted standards.

2. The pension fund must manage the continuity of work based on the analysis of activity impacts and risk assessment, which must include:

   2.1. Determining the critical work processes necessary for the uninterrupted and continuous operation of the pension fund;

   2.2. Determining the resources and systems necessary to carry out individual work processes, as well as connections and dependencies between them;

   2.3. Risk assessment for each of the individual work processes, as well as the likelihood of the occurrence of unwanted cases and their impact on the continuity of work, financial losses and reputation of the pension fund;

   2.4. Determining the level of acceptable risks and techniques for mitigating identified risks;

   2.5. Determining the duration of acceptable work interruption for each of the processes.

3. The pension fund must approve a business impact analysis (BIA) plan that analyses the interruption of activities, containing at least:

   3.1. Processes that have the highest priority, as well as the resources needed for these processes;

   3.2. Service Delivery Objective;

   3.3. Recovery Time Objective;

   3.4. Recovery Point Objective.

4. The management board of the pension fund must, on an annual basis, approve the Business Continuity Plan, as well as the Disaster Recovery Plan, which regulates the creation of conditions for recovery and the availability of information system resources necessary to carry out critical business processes.

5. The Business Continuity and Disaster Recovery Plan should include at least the following requirements:

   5.1. the procedures to be undertaken in case of interruption of the system operation;

   5.2. an updated list of all necessary human and technical resources to restore business continuity;

   5.3. information about responsible persons and their deputies who are responsible for the recovery of operations in case of unforeseen events, including their defined duties and responsibilities, as well as the plan of internal and external lines of communication;

   5.4. an alternate location in case of business interruption and recovery in function of business processes at the primary location. This location should have the appropriate distance from the primary center, in order to avoid the impact of the same hazards on both locations.

6. For the implementation of the plans according to paragraph 5 of this article, the pension fund ensures that all employees are familiar with their roles and responsibilities in emergency cases.

7. The pension fund shall align the plans with business changes, including changes in products, activities, processes and systems, with changes in the environment, as well as with business policy and business strategy.
8. The pension fund shall test the plans, at least once a year and after the appearance of significant changes, and shall document the results of these tests.
9. In business continuity management, the pension fund shall take into account the activities entrusted to third parties and dependence on the services of these parties.
10. In case of circumstances that require the implementation of the business continuity plan and the plan for recovery activities in the event of a disaster, the pension fund shall notify the Central Bank of the Republic of Kosova, no later than the day after the occurrence of such circumstances. The Central Bank of the Republic of Kosova may request additional documentation related to the relevant facts related to these circumstances and shall set a deadline for the submission of these documents.

Article 19
Documentation of IT activity

The pension fund shall keep complete and up-to-date documentation of organization, equipment, systems, approaches and other important factors related to IT activity. Such documentation proves that compliance with the requirements of this regulation is continuous.

Article 20
Remedial measures

Any violation to the provisions of this regulation shall be subject to remedial and punitive measures as provided for in the Law on Central Bank of the Republic of Kosova and Law on Pension Funds of Kosova.

Article 21
Entry into force

1. This Regulation shall enter into force on the day of its approval.
2. Pension funds must ensure compliance with all applicable provisions by 30 June 2024.

Bashkim Nurboja
Chairperson of the Board of the Central Bank of the Republic of Kosova