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

Pursuant to Article 35, paragraph 1, subparagraph 1.1 of the Law No. 03/L-209 of the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010), and Article 85, paragraph 1, of the Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions (Official Gazette of the Republic of Kosovo, No. 11/11 May 2012), the Board of the Central Bank of the Republic of Kosovo at the meeting held on 26 march 2020, approved the following:

REGULATIONS ON INFORMATION TECHNOLOGY FOR BANKS

Article 1
Purpose and Scope

1. The purpose of this Regulation is to establish the criteria and conditions that banks must meet for the organization and operation of their information technology systems (hereinafter refered to as IT), which enable the reduction of the operational risk that may be caused from the misuse of IT systems and to maintain the reliability of these systems in supporting the activity of banks.
2. This Regulation applies to all banks and branches of foreign banks licensed by the CBK to operate in the Republic of Kosovo hereinafter refered to as banks.

Article 2
Definitions

1. All terms used in this Regulation are as defined in the Law No.04/L-093 on Banks, Micro-finance Institutions and Non-Bank Financial Institutions (hereinafter: the Law on Banks) and/or as further defined herein for the purpose of this Regulation:
   1.1. **Information system** - means a complete technological group comprised of infrastructure (software and hardware components), organizations, people and procedures for the collection, storage, processing, transmission, display and use of data and information;
   1.2. **Software components** - means all types of operating system, application software, software development tools and other software systems;

1.3. **Hardware components -** means computer devices, network devices, data backup media and other technical devices that serve as support for the operation of information systems;

1.4. **Information system users -** means all persons authorized to use information systems (employees in the institution, employees of other companies who have access to system information and customers of a bank);

1.5. **External service provider -** means a natural or legal person who, based on a written agreement, provides provides services to bank for delegated banking functions;

1.6. **Assets -** means information (such as databases, contracts and agreements, system documentation, research information, user manuals, training materials, operation or support procedures, business continuity plans, audit tracks and information archived), Software Assets (software applications, software systems, development tools, etc.), Physical Assets (computer devices, communication devices, removable media) and other devices), Services (computer and communication service, general services), Personnel (along with qualifications, skills and experience), Intangible (such as Bank reputation);

1.7. **Clean desk -** means the removal of all documents and other confidential assets from the work desk during the period they are left unattended and at the end of working day.

Article 3
Information technology management

1. Information technology management should include the following requirements:

   1.1. Operationality, capacity and performance that provide the support required by business processes;

   1.2. During the processing process, and during data extraction, provides appropriate data validation control, to prevent inaccuracies and inconsistencies in data and information;

   1.3. Provide timely, accurate, and complete information on business decision making and risk management, to enable the security and sustainable operation of a bank;

2. Bank shall monitor, regulate and continuously improve the IT management process to reduce exposure against risk and maintain its security and functionality.

Article 4
Organizational structure for IT management

1. Bank should establish an organizational structure of the IT unit with sufficient and appropriate staff to ensure that the IT field is managed efficiently. The assignment of tasks should be done according to the ISO 27000 standard with clearly defined responsibilities and competencies for the IT management proces. This unit should document regular informative reports at least on a quarterly basis for the Bank's Senior Management.

2. In the case of delegating IT functions to the external service provider (outsource), the bank must assign at least one internal employee specialized in the field of information technology, as responsible for the coordination and smooth-running of the IT functions.
3. Bank shall assign responsible person for information security, who should manage the security of the information system and coordinate information security policies and processes related to technological functions and platforms. Responsible person reports to the Chief Executive Officer and must be independent of other organizational units. He also, must report through the Chief Executive Officer at least once a year and as needed to the Board of Directors, which must be informed of the operations and functions related to information security.

Article 5
Policies and Procedures on IT managment

1. Board of Directors is responsible for approving technology and information security policies and on an annual basis should assess the suitability of policies and review them.
2. Bank defines objectives, strategies and security requirements for the activity of IT systems, establishes policies for information technology and security, as well as procedures for the field processes. These procedures must be approved by the Senior Management.
3. Bank in compliance with the business strategy approves strategies for the development of IT systems.
4. If the bank caquires all or part of its IT activity (or systems) from external service providers, then the bank shall approve internal procedures on delegating functions for ensuring compliance with the requirements of this regulation on security and for the well-functioning of these systems.
5. Internal procedure on delegating functions under paragraph 4 of this Article shall include at least the following elements:
   5.1. Identifying the functions to be delegated and assessing the impact of the delegation of those functions;
   5.2. Procedures for delegating functions, including criteria for selecting the recipient of delegated functions;
   5.3. Time limits and methods of reporting the recipient of delegated functions to the bank;
   5.4. Methods of monitoring the recipient of delegated functions by the bank;
6. Policies and procedures on IT management should define at least the following elements:
   6.1. Administration and operation of IT systems;
   6.2. Organizational structure for IT management;
   6.3. Hardware infrastructure of IT field (configuration diagrams);
   6.4. Classification of documentation and protection of systems and data;

6.5. System data backup;

6.6. Change management systems;

6.7. Incident management;

6.8. IT system risk management;

6.9. Defining the security mechanisms of IT systems;

6.10. Third party management.

Article 6
Development and procurement of IT systems

1. To minimize risk, the bank should follow the software developments trend, by making sure to use only the updated and supported versions by their providers.
2. Bank shall approve internal procedures on the maner how it implements developments, changes and tests in its IT systems. IT systems are put into live operation, only after the specialized employee who conducts the verification of the applicability of the procedures and the well-functioning of the systems gives his documented approval.
3. External service provider during implementation and work in the systems must in no way have access to the system versions that are in the production (live) except the read-only access with special approval and supervision by Bank. Contractors and other external parties must test all changes in a testing environment.

Article 7
Delegation of IT functions to external service providers

1. Bank is responsible for ensuring that the IT activity is carried out in accordance with all the requirements provided in this Regulation, even in cases where all or part of the IT activity is provided by an external IT service provider.
2. Before selecting the external IT service provider, the bank must undertake the following activities:

   2.1. Conducting risk assessment of the bank's operations that may arise from the use of the external service provided during the processing of the bank's activities;

   2.2. Defining minimum standards that the external IT service provider must comply with and which must be harmonized with the business continuity plan;

   2.3. Defining necessary measures to avoid conflict of interest;

   2.4. Defining the way of monitoring the service and the quality of the company's operation, financial state and risk profile through periodic testing of compliance with the information system security policy;

2.5. Conduct proper assessment of the external IT service provider's activity in terms of legal and financial aspect, as well as in terms of how it manages the security of the information system defined in this Regulation;

2.6. Defining coordinated security incident management.

3. Agreement between the bank and the external IT service provider shall be established through a written contract which, inter alia, shall include:

3.1. Data of the parties concerned (bank and external IT service provider);

3.2. Rights and obligations of the parties concerned;

3.3. Description of delegated functions;

3.4. Time limits for service delivery;

3.5. Service level agreement;

3.6. Engagement of the IT service provider to conduct its activity in accordance with applicable law, requirements, regulators and policies approved by the bank and to cooperate with the CBK in terms of delegated functions;

3.7. Notice period on the termination of the contract which shall be sufficient to allow for the finding of alternative solutions;

3.8. Treating and maintaining data confidentiality;

3.9. Provision stipulating that the external IT service provider shall be subject to CBK supervision regarding delegated IT activities;

3.10. Obligation of the external IT service provider to immediately inform the bank regarding any fact that may have a significant impact on its ability to efficiently and effectively conduct its activity in accordance with applicable legal requirements;

3.11. The right of the bank to be informed regarding the well-going of the functions delegated by the external provider of IT services, as well as the right of the bank to provide general or specific instructions regarding the performance of the delegated functions;

3.12. The right of the bank to inspect and control the activity of the external IT service provider related to the IT delegated activities.

4. External service provider may not subcontract the services unless specified in the basic agreement concluded between the bank and this service provider.

5. Bank is obliged to manage the risks deriving from the contractual relations with the external service providers, whose activities are related to the information system that is in use by the bank. Bank is also obliged to continuously monitor the method and quality of activities contracted by the external provider.

Article 8
Risk management for information systems

1. Bank sets criteria for permissible risk regarding the use of its IT systems according to ISO 27005 standards.
2. At least once a year or in any case of significant changes in IT security requirements, the bank performs risk analysis of IT systems to ensure that this risk is maintained within acceptable limits regarding the activity of Bank. The results of the risk analysis shall be documented.
3. In case of identification of incidents in the field of IT and changes in key functions of important IT processes which may hinder or endanger the business, bank should notify CBK in writing, no later than one working day after the incident.
4. Information system risk management should include the entire integrated bank information system at all stages of its development.
5. Information system risk management should include the annual awareness plan of bank employees for the adequate use of the services provided through the bank's information system.

Article 9
Information systems security

1. IT systems security shall be based on the determination of the fulfillment of the following criteria:

   1.1. Confidentiality: information should 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 in the IT system for authorized users.
2. Bank should continuously manage the security process of the information system. It also should identify and monitor the security needs of the information system, at least based on the results of the risk assessment of that system and the obligations arising from internal acts or contractual relations.
3. Bank should determine the criteria, methods and procedures for classifying information according to the degree of sensitivity and criticality - regarding the possible consequences of violation of confidentiality, their integrity and availability.
4. Security of information and all activities related to it, must be in compliance with all applicable laws relating to the information and operations of the institution.

Article 10
Physical security of information systems

1. Bank should take the necessary protection measures to prevent any unauthorized physical access, interference or damage to information, information processing devices and banking operations based on the ISO 27002 standard.
2. Bank should establish access and work procedures for security areas for all employees and external parties. Security zones must be protected through access controls to ensure that only authorized employees have access.
3. Devices should be maintained in oder to be protected against failures, to ensure continuous availability of integrity and to be supported against interruptions as a result of failures of auxiliary devices, natural disasters, malicious or accidental attacks, etc.
4. Security measures should also be established for devices used and located outside the bank's premises depending on the location and risks should be taken into account when determining the necessary controls.
5. All information-containing devices should be verified to ensure that all licensed data and software are removed before dumping, destruction or reuse, to prevent the retrieval of original information.
6. All users should be aware of security requirements and procedures for the protection of unattended devices.
7. Bank should establish clean desk criteria, methods and procedures in order to protect information.
8. Contractual obligations for employees and external IT service providers should reflect the bank's information security policies. All IT employees and external service providers must understand the responsibilities for the roles considered.
9. Where appropriate for the application, the bank shall establish that employees and external service providers shall retain the information received during the exercise of their activity even for a certain period after the termination of the contractual agreement with the employee or external IT service providers.
10. Bank shall determine the actions and measures to be taken in case of breach of security requirements by employees or external IT service providers.

Article 11
IT asset management

1. Bank should identify all IT assets.
2. Bank must keep inventory of all assets with all the necessary information, including asset type, format, location, backup information (where applicable), information on license and business value.

3. Bank should define and document the ownership and classification of all assets related to information processing.
4. The asset owner shall be responsible to:
   4.1. Ensure that information and assets related to information processing are classified according to sensitivity;
   4.2. Define and regularly review access restrictions and classification.
5. Bank should establish rules on the acceptable use of information and assets related to the information processing.

Article 12
Computer network management

1. Bank computer network should be managed and controlled in order to protect the information of systems and applications. The Bank should implement control to ensure the confidentiality and integrity of information on the network and the protection of services from unauthorized access based on the ISO 27002 standard.
2. For the management of computer networks the bank should define:
   2.1. Procedures for the use and management of network services and devices in order to limit access to network services and applications;
   2.2. Establishment of special controls on the protection of confidentiality and integrity of data passing through public or wireless networks;
   2.3. Technology applied to the network security services like authentication, encryption and network connections controls;
   2.4. Information service groups, users and information systems should be isolated from public networks;
   2.5. Special controls should be dedicated to the access of external service providers in cases of need for interconnection (connections with third parties).

Article 13
User access management

1. Bank shall manage access to information systems through appropriate internal procedures for the management of user access rights. Internal procedures must contain criteria for access, authorization, identification and authentication of users according to ISO27001 standards.
2. Each user must be unique and the system must set the criteria for setting the password according to ISO 27000 standards. Before giving access to information systems, both the bank's internal workers and external service providers must sign the agreement for maintaining confidentiality and non-disclosure of information.

3. Bank shall ensure that the authorization of users' access to information systems is done by the persons responsible for those systems and is based on the principle of the lowest possible access to the system, enabling them to perform their duties. The bank should at least on a 6-month basis review the access rights of users to high-importance systems based on risk assessment and at least on an annual basis all other systems.
4. In managing user access rights, the bank should specifically authorize privileged access and/or remote access to the information system. All access and privileged user activity and remote access shall be monitored.
5. Remote access to information systems should be made possible by two-factor authentication methods. The communication between the device that will remotely access the information system must have *end-to-end* encryption measures for each communication session.
6. Bank should monitor and retain information security events in their infrastructure based on ISO 27001.

Article 14
Internal audit of the information system

1. The requirements set out in the Regulation on Internal Controls and Internal Audit shall apply to the audit of the information system.
2. The activity of the IT field should be subject to at least a periodic annual review that focuses on risk-based methodology.
3. IT audits must be performed by the competent persons within the internal audit function or by external persons contracted for this purpose.

Article 15
Information backup

1. Information backup should be done according to the internal procedures of the bank.
2. Internal acts according to paragraph 1 of this Article shall include at least the following elements:
   2.1. Determining the required level of information backup;
   2.2. Maintaining accurate and complete data on the information backup, as well as documented procedures for restoring backups;
   2.3. Type (Full, incremental, differential) and frequency of backups according to business complexity.
3. Backup creation schedule should be set by ensuring that all information and software can be recovered in the event of a disaster or device failure.
3. Backups should be stored in a second location, at a sufficient distance not to be endangered by the same threats as the central location.

4. Backups should be given the appropriate level of physical and environmental protection consistent with the standard applied in the central location.
5. Backups should be tested regularly, ensuring that they are reliable and usable when needed.
6. Backups should be protected from unauthorized access through encryption.
7. Duration of information backup should be done according to the legislation in force.

Article 16
Servers room

1. The requirements set out in the Regulation on Minimum Security Requirements apply to the servers room.
2. In addition to the requirements of paragraph 1 of this Regulation, the bank should determine the conditions of access of personnel and third parties authorized to access the server room in case of emergencies.
3. The servers room should be restricted to access only for authorized personnel and monitored by evidencing the entry/exit of staff and outsiders in these spaces.

Article 17
Continuation of operation after the interruption as a result of extraordinary events

1. In order to ensure uninterrupted operation of all IT systems, the bank should establish a process for continuous operation.
2. Bank should approve a business impact analysis (BIA) plan that will analyze interruption of activities, that shall at least contain:
   2.1. Most prioritary processes, as well as the resources needed for these processes;
   2.2. Service Delivery Objective;
   2.3. Recovery Time Objective;
   2.4. Recovery Point Objective.
3. Bank's Board of Directors should, 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 resources of the information system necessary to carry out business critical processes.
4. Business Continuity and Disaster Recovery Plan shall include at least the following requirements:
   4.1. procedures to be followed in the event of system interruption;
   4.2. an updated list of all necessary human and technical resources to restore business continuity;

4.3. information regarding responsible persons and their deputies, who will be 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;

4.4. an alternative location in case of business interruption and recovery in function of business processes in the primary location. This location should have the proper distance from the primary center, in order to avoid the impact of the same risks in both locations.

5. For the implementation of the plans according to paragraph 4 of this Article, the bank shall ensure that all employees are acquainted with their roles and responsibilities in case of emergencies.

6. Bank shall harmonize 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.

7. Bank shall test the plans, at least once a year and after the occurrence of significant changes, and shall document the results of these tests.

8. In managing the continuity of the business, the bank takes into consideration the activities entrusted to third parties and the dependence on the services of these parties.

9. 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 bank shall notify the Central Bank of the Republic of Kosovo, no later than the day after the occurrence of such circumstances. The Central Bank of the Republic of Kosovo may request additional documentation regarding the relevant facts related to these circumstances and set the time line for the submission of this document.

Article 18
Documentation of IT activity

Bank maintains complete and updated documentation of the organization, devices, systems, accesses and other important factors related to IT activity. Such documentation shall prove that compliance with the requirements of this regulation is ongoing.

Article 19
Remedial Measures

Any violation of the provisions of this Regulation shall be subject to corrective and punitive measures, as defined in the Law on the Central Bank and the Law on Banks, Microfinance Institutions and Non-Bank Financial Institutions.

Article 20
Entry into force

This regulation shall enter into force six (6) months after the date of its approval.

Flamur Mrasori

The Chairman of the Board of the Central Bank of the Republic of Kosovo