**R E P U B L I C  O F  A L B A N I A**

**B A N K  O F  A L B A N I A**

**SUPERVISORY COUNCIL**

# D E C I S I O N

**No. 28, dated 30.03.2005**

The Supervisory Council of the Bank of Albania, having regard to the proposal from Supervision Department, in accordance with the Law No. 8269, dated 23.12.1997 “On the Bank of Albania”, Article 12, letter ”a” and Article 43, letter “c”,

## D E C I D E D:

1. To approve the Regulation “On Supervision of electronic banking transactions”, as provided in the texture therein.

2. The Supervision Department of the Bank of Albania is charged with the implementation of this decision.

3. The Public Relations Department is charged with the publication of this Decision in the Official Bulletin of the Bank of Albania and in the Official Journal of the Republic of Albania.

This Regulation shall enter into force immediately

**SECRETARY** **CHAIRMAN**

**Ylli Memisha** **Ardian Fullani**

**BANK OF ALBANIA**
**SUPERVISORY COUNCIL**

# REGULATION

# "ON SUPERVISION OF ELECTRONIC BANKING TRANSACTIONS "

(Adopted by the Decision No.28, dated 30.03.2005 and amended by the Decision No.80, dated 18.12.2019 of Supervisory Council of the Bank of Albania)

## Article 1
## Legal basis

This Regulation is issued pursuant to the Law No. 8269, dated 23.12.1997 "On Bank of Albania" and the Law No. 8365, dated 02.07.1998 "On Banking Law in the Republic of Albania".

## Article 2
## Purpose

The purpose of this Regulation is to establish:

a) organizational conditions, conditions on the personnel as well as technical conditions for conducting electronic banking transactions (e-banking);
b) requirements related to the verifications conducted by the Bank of Albania on e-banking service;
c) principles on e-banking risk management.

## Article 3
## Subject

Subject to this Regulation shall be all banks and branches of foreign banks (hereinafter, banks) that conduct banking business in the Republic of Albania and intend to perform electronic banking transactions.

## Article 4
## Definition

E-banking is a distance service, through electronic channels of distribution and communication, of traditional and new banking products and services, within the framework of the allowed activities for commercial banks.

## [1]Article 5
## Prohibitions

## Article 6
## The right of performing e-banking transactions

Banks can perform e-banking services only once they make the verifications on the requirements provided by the Bank of Albania. After the preparations, the bank shall notify the Bank of Albania on the verifications conducted. The notification shall be accompanied by:

a) decision of the board of directors on the use of e-banking when performing bank transactions;

b) curriculum vitae of the immediate responsible and technical personnel that will support the bank in conducting e-banking activity, which must include their qualifications and working experience;

c) data that show the necessary technical requirements for the conduct and control of e-banking activity;

d) assessment of the effects of e-banking use on the bank outcome through financial statements for the next three years;

e) procedures of e-banking operation and internal auditing program for this purpose;

f) the agreement signed upon with the company on information technology support to the bank, if there is any or if signed after receipt of the authorization;

g) the list of banking transactions they will perform along with the communication channels they will use.

## Article 7
## The right of performing the service and suspension of the service

a) After notifying Bank of Albania according to article 6, and after the verifications by the Bank of Albania inspectors are conducted on the assessment of technical conditions, the bank is entitled to perform e-banking service.
b) Bank of Albania may order the bank to suspend partially or completely the e-banking service, if during the supervision process conducted by the Bank of Albania it results that the bank has not meet the requirements of this regulation.

c) In case of partial suspension, the bank interrupts within 60 days the suspended e-banking service and notifies the Bank of Albania on this matter. The bank cannot resume this

[1] Repealed upon the Supervisory Council decision no. 80, dated 18.12.2019.

service before a period of six months from suspension is passed. The conditions of resumption are the same as in article 6.

d) In case of complete suspension, the bank interrupts within 60 days the e-banking service and notifies the Bank of Albania on this matter. The Bank cannot resume this service before a period of 18 months from suspension is passed. The conditions of resumption are the same as in article 6.

**Article 8**
**The request after the opening of the service**

a) The bank shall notify in advance Bank of Albania on all the additions to the list of channels of communication and to the electronic banking transactions that are performed after the opening of e-banking service.

b) Bank of Albania has the right to request that the documents prescribed in article 6 are properly filled in for all the changes and to conduct verifications on the technical conditions when it deems appropriate.

**Article 9**
**Accounting**

Banks shall conduct accounting records on the transactions performed even for e-banking, pursuant to the law “On Accounting and Financial Statements” and “Banking Accounting Manual”.

## PRINCIPLES ON E-BANKING RISK MANAGEMENT

**Article 10**
**Effective supervision**

**The Leading Council and the senior executive administrators should establish an effective supervision of e-banking risk management on the e-banking operations, including the establishment of specific responsibilities, politics and controls on the management of these risks.** For this purpose they should in a documented way:

a) clearly define the bank risks in terms of e-banking;

b) define the authorities, their competencies and the reporting mechanisms, including the necessary procedures of acting according to the degrees of responsibility in case of violation of the security (such as penetration through the net, violation of security requirements from the employed persons, any serious misuse of computers, etc.) that have an important impact on the service security, on the situation and reputation of the bank;

c) evaluate the unique risk factors for guaranteeing the security, the integrity and availability of ebanking products and services and apply the request that the thirds, with whom the bank shares/uses the main systems or applications, take similar measures;

d) ensure that due diligence and risk analysis are carried out before cross-border operations are performed;

e) define the resources that are required to supervise the e-banking services in proportion with the operational functioning and system riskiness, network deficiencies and nature of the information transmitted.

**Article 11**
**Quality control infrastructure**

**The Leading Council and senior executive administrators should review and adopt the main orientations of security control process of the bank.**

a) The Leading Council and senior executive administrators should supervise the ongoing development and maintenance of quality control infrastructure, that protects on an adequate basis the systems and e-banking data from the external and internal threats. This process includes the granting of authorized rights, of rights on logical and physical controls and the definition of the adequate infrastructure security to maintain the required limits and restrictions in the internal and external activities.

The Leading Council and senior executive administrators should:

b) define the explicit responsibilities of the personnel for the application and control on the application of the bank's security policies;

c) enable adequate physical controls for protection from the unauthorized physical inflows in the computerized environment;

d) enable adequate logical controls and monitoring processes for protection from the unauthorized external and internal inflows in the applications and e-banking database;

e) enable regular reviewing and testing of measures and security controls, including the ongoing follow-up of the current developments of security industry and the setting-up of an advanced software, of service packets and other measures.

**Article 12**
**External resources supervision**

**The Leading Council and senior executive administrators should establish a supervision process and demonstrate full and continuous diligence for the administering of the bank's relations with other external parties that support e-banking and for the use of other external resources in this field.**

The Leading Council and senior executive administrators must ensure that:

a) the bank understands to a full extent the risks that are associated with involvements in a partnership agreement or external resource (for example, with an independent company that offers Internet service, etc.) for the systems and e-banking applications;

b) a careful and adequate reviewing of professional skills and financial condition of the service provider as a third party, before the contract on e-banking services is signed, is conducted;

c) the contractual responsibility of all the parties in a partnership relation, including an external party is defined. Particularly, the responsibilities on providing and receiving information to and from the service provider, responsibilities on the backups keeping and copies of transactions performed through e-banking, should clearly be defined;

d) all the e-banking systems and operations provided by external resources are subject of risk management, of security policies and the keeping of confidentiality that are in line with the standards of the bank itself;

e) periodical internal/and or external controls on external resources operations are conducted, at least to the same extent as required when they are conducted by internal resources;

f) there are plans for reserve resources in case of incidents for e-banking activities from external resources.

## Article 13
## Identity and authorization of clients

**Banks should take the necessary measures to verify the identity and authorization of clients with whom they conduct business through Internet.**

a) Banks should employ safe methods for the verification of identity and authorization of new clients as well as the verification of the existing clients that seek to undertake electronic transactions.

b) Banks may employ various methods, separate or combined ones, to proceed on the identification, including PIN-s, passwords, smart cards, biometrics and digital certificates.

   Banks should monitor and adopt sound practices of industry in this field to ensure that:

   i. Verification database that ensures the access to the e-banking account of clients or the access to the sensitive systems, is protected from the manipulations and corruptions. These manipulations must be detected and investigation controls must be in place to document such attempts.

   ii. Additions, deletions or changes on individuals, agents or on the system based on the verification data are authorized only from a verified source.

iii. Necessary measures to control the e-banking system links are established in order that third parties are not able to move or replace the identified clients.

iv. The verified e-banking sessions should remain safe during all the session process, or in the event of a security error the system requires a new verification.

## Article 14
## Verification of the transactions

**Banks shall employ methods on the verification of transactions, which lead to the real acknowledgement of facts and establish the responsibilities on e-banking transactions.**

Banks shall make reasonable efforts pursuant to the type of e-banking transaction and the proper value this transaction has or might have for the bank, to ensure that:

a) E-banking systems are projected to reduce the possibility that the authorized users get involved in ill-considered transactions and the clients fully understand the risks related to the transactions they perform.

b) All the parties involved in transactions are positively verified and the control on verification channels is made.

c) Financial transactions data are protected from modifications and, if occurred, these modifications must be observed.

## Article 15
## Distribution of tasks

**Banks shall ensure that the appropriate measures for the proper distribution of tasks within the systems, databases and e-banking applications are made.**

Practices on establishing and maintaining the distribution of tasks within the e-banking environment shall include:

a) processes and systems, which ensure that none of employees/service providers from outside might gain access to, authorize and complete a transaction;

b) distribution of tasks among the staff who organizes statistical data (including website contents) and those who are responsible for the verification of their integrity;

c) e-banking system testing, ensuring that the distribution of tasks might be neither avoided nor left out;

d) distribution of tasks among the staff who develops and those who manage the e-banking systems.

## Article 16
## Control and right of access to the system

**Banks shall ensure that controls for the authorizations and privileges on the rights of access to the systems, in e-banking database and applications, are established.**

Banks shall strictly control the privileges of access and authorization in order to preserve the allocation of duties. In e-banking system, authorizations and rights of access may be established in a centralized or allocated way within one bank, and are generally saved in databases. The protection of these databases from external intervention or corruption is fundamental for an authorized and efficient control.

## Article 17
## Integrity protection

**Banks shall ensure that the appropriate measures to protect the integrity of data on transactions, records and e-banking information are established.**

a) Banks shall ensure that the appropriate measures to define the accuracy, completeness and security of transactions, records, and e-banking information that is transmitted via Internet, resident within the internal database of the bank, or that is transmitted/protected from a third service provider on behalf of the bank, are established.

b) Practices on integrity protection of the data within the e-banking environment shall include:

   i. performing e-banking transactions in a way that makes them too resistant against any intervention throughout the process;
   ii. saving, accessing and modifying e-banking records in a way that makes them too resistant against interventions;
   iii. projecting e-banking transactions and processes to keep the records in a way that makes impossible the avoidance of discovering unauthorized modifications;
   iv. establishing adequate policies on modifications control, including the monitoring and testing procedures, that are established to be protected against the e-banking system modifications, and which might wrongly compromise the controls or data security;
   v. discovering interventions in the e-banking transactions or records through transaction processing, monitoring functions and records maintenance.

## Article 18
## E-banking transactions control

**Banks shall ensure that safe controls for all e-banking transactions exist.**

The distribution of financial services via Internet can render more difficult for banks to apply and implement the internal controls and maintain the safe tracing of control, if these measures are not adapted for an e-banking environment. In the process of determining where control tracing should be carried out, the following elements of e-banking transactions are to be taken into consideration:

a) opening, modification or closing of client's account;

b) financial consequences of transaction;

c) an authorization issued to a client who exceeds the allowed limit;

d) a granting, modification or revocation of rights and privileges to have access to the systems.

**Article 19**
**Keeping the information confidentiality**

**Banks shall take the necessary measures to keep the confidentiality of basic e-banking information. The measures on keeping confidentiality must be in proportion with the sensitivity of information being transmitted and/or saved in the database.**

Thus, banks shall ensure that:

a) all the confidential data and records of the bank be accessible only from individuals, agents and from authorized and certified systems;

b) all confidential data of the bank be safely kept and be protected from the viewing or modification during the transmission via public, private or internal networks;

c) bank standards and controls for the use and protection of data be implemented even when the third parties have access to the data through the relationships with external sources;

d) all entries to the limited data be traceable and require the confirmation (be logged-in), even following a certain number of unsuccessful efforts to log-in.

**Article 20**
**Informing the clients**

**Banks shall ensure that the adequate information is provided in the website, to allow the clients to get an informed conclusion on the bank's identity and its regulatory status, before they have access to the e-banking transactions.**

The information the bank shall provide in its website-in is as follows:

a) name of the bank and location of its Head Office (and other local offices if applicable);

b) identity of the principal supervisory banking authority responsible for the supervision of the bank's Head Office;

c) the way the clients can contact the client service center regarding the service problems, complaints, suspected misuse of accounts, etc.;

d) how the clients can have access to the information on the applicable compensation, coverage of secured deposits and protection level they afford (or the website links that provide such an information);

e) other information that might be adequate or that are required under particular circumstances.

**Article 21**
**Requirements on the client's confidentiality**

**Banks shall take the necessary measures to ensure the loyalty to the requirements on the client's confidentiality, applicable within the jurisdictions based on which the bank provides the e-banking services and products.**

Banks shall make reasonable efforts to ensure that:

a) policies and standards of the client's confidentiality consider the consistency with all the laws and regulations on confidentiality, within the jurisdiction based on which it provides the ebanking services and products;

b) clients are acquainted with the policies and issues related to confidentiality on the use of ebanking services and products;

c) clients may give up allowing the bank to share with third parties for cross-marketing purposes the information on the requirements, interests, financial position or personal banking business of the client;

d) data on the client are not used for purposes other than those allowed specifically or allowed by the client;

e) bank standards on the use of client's data must be implemented even when the third parties have access to client's data through the relationships with external sources.

**Article 22**
**Ensuring the e-banking operations continuity**

**Banks shall possess effective capacities to ensure business continuity and efficient process of reserves planning, to help ensure the availability of the e-banking systems and services.**

a) To protect banks from business risks, legal and reputation risks, the e-banking services must be performed continuously and respond in due time to clients' expectations.

b) To achieve this goal, the bank must be able to provide e-banking services to the last users, either from the primary sources (such as internal systems and applications of the bank) or from the secondary ones (such as systems and applications of service providers).

To provide the clients the continuity of the e-banking services they seek for, banks shall ensure that:

c) current capacities and future development of e-banking systems are analysed in the context of the development of all the markets on electronic trade and of the expected degree of acceptance of the e-banking services and products from the client;

d) calculations of the e-banking transactions processing capacity are certified, stress tested and reviewed periodically;

e) plans on the regular business continuity for the systems and e-banking critical processing are applicable and duly tested.

**Article 23**
**Contingent events management**

**Banks shall have adequate plans to react to incidents, to manage, maintain and minimize the problems arising from contingent events (including both internal and external shocks), that might make difficult the e-banking systems and services provision.**

To ensure an effective reaction to contingent events, banks shall prepare:

a) reaction plans to contingent events, to address the process of putting again into functioning e-banking systems and services. Scenarios analysis must take into consideration the possibility of exposure to risks and their impact on the bank. E-banking systems provided from external providers must be integral part of these plans;

b) mechanisms to identify an imminent incident or crisis, to assess their material and control reputation risk related to any service interruption;

c) a communication strategy to sufficiently address the concerns of foreign markets and communications means that might emerge in case of failure of e-banking systems;

d) a clear process to notify the supervisory authorities, in case security materials are broken or interruption incidents occur;

e) reaction teams to incidents that must be adequately trained and have the authority to act in emergency cases to analyse the reaction/detection systems of incidents and construe the significance of results;

f) a clear chain of commands, including either the internal operations or those of external sources, to ensure that the immediate actions according to the gravity of incident are taken. Escalation and procedures of the internal communication must be defined and include the notification from the executive board when necessary;

g) a process to ensure that all the relevant external parties, including the bank’s clients, correspondents and communications means, are informed properly and in due time on the e-banking interruptions and the activity resumption developments;

h) a process for the gathering and preservation of legal evidence to ease the necessary reviews following an e-banking incident, as well as to assist in bringing a charge against illegal meddlers.

**Article 24**
**Penalties**

Any infringement of the requirements of this regulation is a violation of the terms on conducting banking business in a sound and safe way, and is treated according to the provisions of article 44, Law No. 8365, dated 02.07.1998 “On Banking Law in the Republic of Albania”.

**Article 25**
**Transitional provisions**

The banks that have started to perform e-banking transactions before this regulation enters into force must meet, within a six-month period from the time this regulation enters into force, the terms and conditions provided in this regulation.

**Article 26**
**Entering into force**

This Regulation shall enter into force fifteenth days following its publication in the Official Gazette of the Republic of Albania.

**CHAIRMAN OF SUPERVISORY COUNCIL**

**Adrian Fullani**