Pursuant to Article 5, Paragraph 1, Item b, Article 20, Paragraph 2, Item b and Article 37 of the Law on Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska", No.: 59/13 and 4/17), and Article 6, Paragraph 1, Item b and Article 19, Paragraph 1, Item b of the Statute of Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska", No.: 63/17), the Management Board of the Banking Agency of Republika Srpska, on its 44th session held on 11 December, 2017 issued the

DECISION
ON INFORMATION SYSTEM MANAGEMENT IN BANKS

1. General provisions

Article 1

This Decision shall determine requirements and criteria the bank is obliged to ensure and implement, and which relate to the information system management in banks and information system risks.

Article 2

Certain terms used in this Decision shall have the following meaning:

1) Information system is an overall set of technological infrastructure, organization, human resources, and procedure for collecting, storing, processing, maintaining, using, distributing and disposal of information.
2) Information system resources include software components, hardware components and information property.
3) Software components include all types of systemic and applicative software, software development tools, as well as other software.
4) Hardware components include computer equipment, communication equipment, media for data storage, as well as technical equipment which serves as a support to the information system functioning.
5) Information property includes data in files and databases, program code, configuration of hardware components, expert knowledge, key personnel, technical and user documentation, internal acts, and similar.
6) Information system users are all persons who are authorized to use information system (bank employees, service provider employees, e-banking users and other).
7) Information system risk is the risk stemming from the use of information technology, i.e. information system.
8) Information technology includes all technology which is used for collecting, processing, storing, distributing and protecting information. It is related to software and hardware components.
9) Information system safety implies preserving confidentiality, integrity, disposal, authenticity, provability, irrefutability and reliability in the information system.
10) Confidentiality is a feature which implies that data and information are not available or disclosed to unauthorized persons or processes.
11) Integrity is a feature which implies that data, information and processes are not changed in an unauthorized and unforeseen manner.
12) Availability is a feature which ensures that data, information and processes are always available and usable upon the request of authorized person.

13) Authenticity is a feature which ensures that the person's identity is indeed the one it is claimed to be.
14) Provability is a feature which ensures that each activity in the information system can be unambiguously traced to its source.
15) Irrefutability is a feature which ensures impossibility of denial of the activity performed in the information system or information receipt.
16) Reliability implies that the information system consistently and expectedly performs foreseen functions and provides accurate information.
17) Sensitive data/information are those data/information whereby the violation of features of confidentiality, integrity and availability would case negative consequences to the bank business operations.
18) Controls encompass policies, procedures, practices, technologies and organizational structures relating to the information system determined in order to ensure reasonable belief that the business objectives shall be achieved and that undesired events shall be prevented or identified, and according to the application manner they are divided into managerial, logical and physical.
19) Managerial controls include issuing internal acts relating to the information system and setting up of appropriate organizational structure, and they ensure application of these acts in order to secure functionality and safety of the information system.
20) Logical controls are controls implemented on software level of information system components.
21) Physical controls are controls by means of which information system resources are protected from unauthorized physical access, theft, physical damage or destruction.
22) Identification is a process of presenting the information system user when logging in and in the course of performing activities in that system.
23) Authenticity is a process of verification and confirmation of user's identity by the application of one of the following elements or their combination:
    1. something known only to the user (e.g. password, cryptographic key and similar),
    2. something possessed only by the user (e.g. smart card, token, cryptographic key and similar) and
    3. something that only the user is (biometric features such as fingerprint, eyeball, voice, handwriting and similar).
24) Authorization is a process of division of access rights to the information system users.
25) Supervision of user access rights is a process which includes monitoring, change and revision of information system user rights.
26) Privileged access is an access to information system resources which enables authorized users (network administrators, system software, database and other) to circumvent installed logical controls.
27) Remote access is an access to the information system resources from a remote location by means of telecommunication infrastructure over which the bank has no full control.
28) User request is a request of the information system user for access to certain information system resources or IT services, request for information or advice, and other standard request (e.g. password reset, request for equipment and other).

29) Operation and system records encompass chronological records on activities of the information system resources (operation system records, applicative software, database, network devices and similar).

30) Malicious code is any form of program code created with the intent to gain unauthorized access to the information system resources, collect or destroy information, cause unexpected behavior or interruption in the functioning of this system, or otherwise violate the confidentiality, integrity or availability of these resources (e.g. computer viruses, worms, Trojan horses, etc.).

31) Incident is any unplanned and undesired event which may undermine safety or functionality of the information system resources which support performance of the bank's business processes.

32) Severe incident is an incident which has or might have a significant impact on the continuity of bank's operations and/or on the safety of sensitive data and/or materially significant impact on a large number of service beneficiaries.

33) Electronic banking is a system which enables bank clients to use services the banks provide (access to financial information, electronic monitoring and similar) from remote location by means of public communication networks or similar.

34) Critical/key business processes are those business processes or functions whose inadequate functioning may significantly jeopardize, i.e. undermine the bank's business operations.

35) Data backup is a backup of original data necessary for re-establishment of the bank's business processes, and other data which the bank assesses as necessary to keep.

36) Recovery time objective – RTO is the longest acceptable time of unavailability of the bank's business process and the information system resources necessary for business process functioning, i.e. time during which it is necessary to re-establish business process.

37) Recovery point objective – RPO is the longest acceptable period from the last data backup up to the occurrence of unavailability of business process, i.e. the longest acceptable period during which the data might be lost.

2. Framework for information system management

Article 3.

(1) The bank shall, in accordance with nature, complexity and scope of operations, as well as with complexity of the information system, establish, monitor, regularly revise and improve the process of information system management in order to mitigate exposure to risks, preserve safety and functionality of this system.

(2) The bank shall establish adequate system that includes identification, measurement, monitoring and control of information system risk management.

Article 4

The bank supervisory board shall be obliged and responsible to at least:

1) based on the bank management proposal, adopt information system strategy which must be in accordance with the bank business strategy,

2) based on the bank management proposal, adopt policies for information system management, particularly information system safety policy, and monitor their implementation,

3) consider adopted policies at least annually, i.e. timely perform their adjustment to economic, market, technological and other conditions (in accordance with changes in environment),
4) establish system for measuring, monitoring, control and management of information system risks, and regularly monitor and asses the efficiency of this system,
5) establish appropriate organizational structure, with clearly defined division of tasks, employee's responsibilities, as well as their expert skills and required competences, in order to ensure adequate information system management,
6) ensure selection and appointment of qualified and competent member of the bank management, who will be responsible for establishment and supervision of information system management process,
7) upon the bank management proposal, define content and frequency of reporting to the supervisory board on relevant facts related to the information system management, and at least annually and
8) ensure conditions for establishment of efficient system of internal controls in the segment of information system management and perform supervision over that system.

Article 5

(1) The bank management shall be obliged and responsible to, at least:
1) appoint the board for information system management, comprised of representatives of various business functions, which will hold meetings periodically and report to the bank management on its activities at least quarterly, and whose role should be coordination of initiatives and monitoring of developing activities of the information system related to the compliance with the bank's business objectives and business strategy,
2) propose and implement policies, and adopt and implement procedures related to the information system management,
3) establish processes and procedures for information system risk management which include identification, measurement, limitation and mitigation measures, monitoring, analyzing and controlling of risks,
4) ensure that all responsibilities related to the information system management are clearly defined and allocated, taking into account the adequate segregation of responsibilities,
5) ensure required resources for information system management,
6) adopt plan and program for establishment and raising awareness on information system safety and
7) adopt and apply methodology for project management, by means of which it will define criteria, manner and procedures of project management related to the information system.

(2) The bank management shall timely inform the Banking Agency of Republika Srpska (hereinafter: Agency) on significant and complex changes on the bank information system, and deliver appropriate documentation (detailed description of change, activity plan, project teams, planned budget, project cost effective analysis, risk assessment results and similar).

Article 6

(1) The bank shall develop and supervise implementation of information system strategy which shall at least:
1) cover long term and short term initiatives related to the information system,

2) define connectedness and compliance of information system objectives with the bank business objectives.

(2) The bank shall periodically update information system strategy, particularly when changing the bank's business strategy, in order to ensure compliance between information system objectives and business objectives, plans and activities.

(3) The bank management shall annually adopt operational plan of activities related to the information system, which is stemming from the information system strategy.

(4) The plan referred to in Paragraph 3 of this Article shall contain the following as a minimum: description of activities and project of information system, financial and human resources, timeframes and data on persons responsible.

(5) The bank control functions shall, in accordance with their competences, ensure that the risks connected to the implementation of information system strategy are adequately identified, assessed and mitigated, as well as that an efficient information system management has been established.

Article 7

(1) The bank shall adopt and apply internal enactments related to the information system and ensure implementation of such enactments.

(2) Internal enactments must be at least:
1) aligned with regulation, standards and professional rules,
2) regularly revised and updated and
3) complete, detailed and applicable.

(3) The bank shall ensure that all information system users are familiar with the content of internal enactments related to the information system, in accordance with their competences, responsibilities and needs.

(4) Contracts, audit findings, instructions and other documents must be drafted, i.e. translated into one of the official languages in Republika Srpska.

Article 8

(1) The bank management shall appoint person responsible for the function of information system safety, and define his/her competences, responsibilities, and scope of work. This function should be independent from the function of organizational unit for information system management. Person responsible for the function of information system safety should be a competent person with appropriate expert skills, specialist knowledge and experience.

(2) Person responsible for the function of information system safety should at least supervise and coordinate activities related to the information system safety, and regularly, at least quarterly, report to the bank management on the condition and activities related to the information system safety.

3. Management of risk stemming from contractual relations

Article 9

The bank shall continuously assess risks and adequately manage those risks stemming from contractual relations with legal persons and individuals whose activities are related to the bank's information system.

4. Information system risk management

Article 10

(1) The bank shall establish a process of information system risk management, which should be an integral part of the bank risk management, in accordance with the Decision on bank risk management.

(2) The bank management shall adopt methodology which shall define criteria, manner and procedures of information system risk management, and determine responsibilities of risk management and acceptable risk levels.

(3) Within the information system risk management, the bank shall:
1) assess risk including the following elements: information system resources, threats and vulnerabilities, applied protection and control measures,
2) recommend measures for acting in connection with assessed risks, adopt plan of measure application and continuously monitor realization of such plan and
3) regularly, at least annually, report to the bank management and supervisory board on risk assessment findings.

(4) Information system risk management shall cover all information system resources which support significant business processes, and pay special attention to the importance of parts of the information system and services that:
1) support key business operations and distribution channels,
2) support key management processes and corporate functions, including risk management,
3) are subjected to specific legal or regulatory requirements, which impose higher requirements for availability, recovery, confidentiality and safety,
4) perform processing or storing of sensitive data, whereby unauthorized access to such data may significantly influence reputation, financial result, or the bank's business continuity, and
5) ensure basic functionalities which are crucial for adequate bank functioning (e.g. telecommunication services).

(5) The bank shall, for the requirement of assessment of risk of materially significant outsourced activities, ensure reports on risk assessment of information system of service providers.

(6) The bank shall ensure that internal and external audit regularly assess the efficiency of system for information system risk management, and that the information system risks are adequately identified, assessed and mitigated.

5. Internal audit

Article 11

(1) The bank shall perform internal audit of information system in accordance with the Agency's regulation governing the area of internal audit in banks, and based on defined internal audit activity program.

(2) The bank shall plan and implement information system internal audit in accordance with the assessment of risks of certain areas of information system, whereby it must define time interval in which all areas of the bank information system shall be reviewed (covered).

(3) The bank shall ensure that the information system internal audit is being implemented continuously in the course of whole year.

(4) Persons performing the information system internal audit must possess expert knowledge and skills about information system.

(5) In case information system internal audit is outsourced, the bank should ensure that the information system internal audit service provider at the same time (in that year) does not provide service of information system external audit in the bank, and should ensure that there is no conflict of interest. Persons who operatively perform audit must possess internationally recognized certificates for information system audit.

6. External audit

Article 12

(1) The Agency shall issue prior approval for the appointment of audit firm to perform information system audit (hereinafter: IS external auditor).

(2) The bank shall submit to the Agency a request for issuing approval for the appointment of IS external auditor in order to perform information system audit.

(3) The bank shall, along with the request referred to in Paragraph 2 of this Article, submit to the Agency the following documents:

1) decision draft on appointment of IS external auditor,
2) contract draft or letter of intent with IS external auditor,
3) IS external auditor references on performed information system audits,
4) evidence on expert qualifications of persons who will perform the audit and their CVs and
5) statement of non-existence of conflict of interest between IS external auditor (i.e. persons who operatively perform audit) and the bank.

(4) The bank general assembly, with a prior approval of the Agency, shall issue the decision no later than 30th of September of the current year on the IS external auditor appointment, which will perform the information system audit for that year.

(5) The bank shall deliver the decision on IS external auditor appointment within eight days from the day of decision adoption and the contract on performing information system audit in writing within eight days from the date of contract signing.

(6) IS external auditor shall deliver to the Agency the plan of audit performance, from which the areas subject of audit are visible, stated names of persons who will perform the audit and their engagement, and the duration of audit at least 30 days prior to the commence of the bank information system audit.

(7) When performing information system audit, the IS external auditor shall take into account outsourced services and their significance and influence on the information system, and in accordance with that draft audit plan and efficient audit approach.

(8) The IS external auditor shall draft audit report on performed information system audit and provide assessment on the condition of information system and adequacy of its management.

(9) The report on performed information system audit is a separate report which the bank is obliged to deliver to the Agency no later than 31st of May of the current year.

(10) The bank shall perform information system audit annually.

7. Information system safety

Article 13

(1) The bank shall adopt and implement the information system safety policy, which shall represent basis for the bank information system safety management, and which as a minimum should:
   1) contain principles of management of information system safety resources and in doing so adhere to internationally recognized standards and principles to the extent possible,
   2) define competences and responsibilities related to the area of information system safety management,
   3) cover areas of managerial, logical and physical protection of information system resources, in accordance with the size and complexity of information system and
   4) define measures in case of responsibility of information system user for violation of information system safety.

(2) Information system safety policy must be aligned with changes in environment and the bank information system.

(3) The bank shall be obliged to establish the process of information system safety management as a continuous process of identification of needs for this safety and achieving and maintaining adequate level of that safety, based on the risk assessment findings and obligations stemming from regulation, contractual relations and similar.

(4) The bank shall, in order to achieve and maintain adequate level of information system safety, regularly test implemented measures of protection and control of the bank information system, and depending on the findings of this test and risk assessment ensure independent testing (e.g. penetration test), and report to the bank management and supervisory board on the results of such testing.

Article 14

(1) The bank shall establish adequate system of management of access to information system resources, which at least shall include:
   1) defining adequate managerial, logical and physical controls,
   2) defining password policies in accordance with good practices, but also with internal risk assessment and importance of resources to which it is accessed,
   3) management of user access rights, which includes the process of recording, identification, authentication and authorization, and supervision over user access rights,
   4) management of privileged and remote access,
   5) management of generic and service accounts and
   6) regular testing of adequacy of approved rights to access information system resources, at least annually.

(2) The bank shall ensure that the authorization of information system user is based on the principle of dedication of the least possible access rights to the resources of that system, which facilitates efficient operation performance.

Article 15

The bank shall establish adequate information system protection measures for misuse or unauthorized access from outside, at least including:

1) management and supervision over protection mechanisms (e.g. firewall, web traffic filtering, antivirus solutions, systems for detecting and preventing unauthorized access and similar),
2) computer network segmentation, regular monitoring of network traffic and record analysis,
3) software integrity verification,
4) periodical testing of vulnerability and penetration testing,
5) system strengthening (by means of application of safety recommendations),
6) communication channel protection and
7) adequate training of information system users, especially in terms of attack recognition.

Article 16

(1) The bank shall, in accordance with risk assessment, ensure generating, regular monitoring and storing of operational and systemic recordings for the purpose of timely detection of unauthorized access and actions in the information system, problem identification, event reconstruction and responsibility determination.

(2) The bank shall determine the list of information system resources from which the recordings are being collected, recordings type, structure and storing period, manner of monitoring and analyzing, and reporting on analysis results.

(3) The bank shall establish adequate recordings protection, ensure their integrity and confidentiality in accordance with information classification, and separate duties of persons who administrate information system resources from which the recordings are being collected from the persons who administrate recordings.

Article 17

(1) The bank shall adopt and implement procedures defining protection measures and control of access to premises in which information system resources are located (premises with server infrastructure, communication equipment and similar), as well as premises in which systems for support to information system functioning are located, for the purpose of protection from unauthorized physical access, theft, physical damage or destruction of information system resources.

(2) The bank shall define and implement adequate protection measures for static electricity, fire, flooding, earthquake, explosion and other forms of natural disasters or damages caused by human factor, and based on the risk assessment.

(3) The bank shall regularly control properness of implemented protection measures referred to in Paragraph 2 of this Article.

Article 18

The bank shall, by means of application of appropriate controls, protect information system resources from malicious program code, and at least shall include the following:

1) define roles and responsibilities of persons in charge of protection measure implementation,
2) establish prevention and detection controls (prevention of malicious program code execution, continuous updating of software for malicious program code detection, management of vulnerability and testing of information system and similar),
3) define procedures in case of malicious program code detection and

4) raising awareness of information system users on risks from consequences of malicious program code activity by means of regular training program.

Article 19

The bank shall ensure that applicative software has installed controls of functionality, completeness and consistency of data that are input, changed, processed and generated.

8. Information system development and maintenance

Article 20

(1) The bank shall establish a process of information system development in accordance with relevant business changes in the bank and environment, taking into account functional and safety aspects, which at least include:
   1) planning and formal organization of projects in accordance with project management methodology,
   2) establishing and documenting process of program development and delivery, which covers procedures of analysis and projecting, programing, testing, and introduction to production work,
   3) employees' training and
   4) communication and reporting procedures.

(2) The bank shall ensure adequate separation of developing, testing and productive environment.

Article 21

(1) The bank shall establish a process of management of hardware and software components in all phases of their life cycle – from supply or development to withdrawal from use.

(2) The process of management of hardware and software components should include: procedures of identification, maintaining detailed and updated recordings, appointment of one or more bank employees responsible for management and protection of such components, and determining rules of their acceptable usage and safe storage when withdrawing from use.

(3) The bank shall ensure adequate maintenance of hardware and software components of information system according to the manufacturer's recommendations, and store recordings on such maintenance.

(4) The bank shall classify and protect information, and define manner of management of the same according to their importance, legal requirements, sensitivity and criticality for the bank.

Article 22

(1) The bank shall establish a process of management of information system changes, in order to avoid that they cause unexpected and undesired behavior of this system, i.e. undermine its safety or functionality.

(2) The process referred to in Paragraph 1 of this Article shall at least include:
   1) initiating, analysis, risk assessment and approval of request for change, and manner of determining priorities and realization,
   2) testing, approving and documenting prior to the implementation of change in production,
   3) implementation plan which also includes return plan,

4) separation of duties related to the development and implementation of changes,
5) informing users of information system on details of executed changes and
6) emergency change management.

(3) The bank shall determine initial versions of software and hardware components of information system, and record and chronologically document all changes of these components.

(4) The bank shall determine procedures for safety correction management – patch, within which it will define the manner in which information on patch are being monitored, the longest period in which patch must be applied depending on criticality and risk assessment for the bank, and manner of their application.

(5) The bank shall ensure that testing environment reflects, to the largest extent possible, productive environment, whereby the information confidentiality is not jeopardized.

Article 23

The bank shall establish a process of management of user requests, which at least should include procedures for registration, classification, priority determination, processing and reporting on user requests.

Article 24

The bank shall define and implement procedures for management of documentation related to the information system, which at least should ensure:

1) existence of accurate, complete and updated documentation and
2) employees' access to the documentation in accordance with their business needs.

Article 25

(1) The bank shall ensure adequate and continuous training of employees related to the use of information system resources, as well as specialist training of system administrators, persons responsible for information system safety function and internal auditor who performs information system audit.

(2) The bank shall implement programs of raising awareness of information system users about safety of information system, taking into account current trends.

(3) The bank shall implement testing of information system users from the area of information system safety, and analyze and document findings of such testing.

9. Information system recovery plan

Article 26

(1) In order to secure continuous operation of critical (key) business processes, the bank shall adopt business continuity plan and information system recovery plan in accordance with the Decision on bank risk management.

(2) Based on conducted analysis of business impacts, the bank shall define and adopt information system recovery plan, which it will apply in emergency situation, and it will determine recovery priorities in business processes, as well as necessary resources and systems, and in detail describe procedures which are necessary to be adhering to in order to recover critical (key) business processes in required recovery period and in accordance with required functionality.

(3) Within the impact business analysis, it is necessary at least to:

1) determine critical (key) business processes and activities,
2) determine resources and systems necessary for implementation of individual business processes, as well as their interconnectedness and relatedness,

3) assess the risk related to individual business processes,
4) determine acceptable risk level for individual business processes and
5) determine RTO and RPO of individual business processes, taking into account outsourcing and dependence on third parties.

(4) Information system recovery plan must contain:
1) detailed procedures and instructions for recovery of information system resources necessary for performance of critical (key) business processes in emergency,
2) defined recovery priorities of information system resources, as well as the list of all resources necessary for re-establishment of critical (key) business processes,
3) data on teams which will be responsible for information system recovery and their members, with clearly defined duties and responsibilities,
4) data on location for information system recovery and
5) data on key service providers.

(5) The bank shall, for the purpose of efficient implementation of plans referred to in Paragraph 1 of this Article, ensure that all employees are familiar with their roles and responsibilities in case of contingency. The bank management is responsible for implementation and compliance of these plans with business changes.

Article 27

(1) The bank shall, based on the analysis of impact on business operations and risk assessment, ensure back up location for information system recovery, which shall be at appropriate distance from primary location, taking into account that primary and back up location cannot be exposed to the same risk impact simultaneously.

(2) The bank shall plans referred to in Article 26, Paragraph 1 of this Article test periodically and afterwards significant changes, and at least annually, and document results of such testing and ensure that the report on testing results is adopted by the bank management. Testing should be implemented based on various scenarios (e.g. cyber-attack, communication channel interruption, unavailability of primary location, loss of key data, and other).

(3) The bank shall, at least 30 days prior to the testing of information system recovery plan, inform the Agency thereof.

(4) The bank shall in case of occurrence of circumstances which require application of information system recovery plan immediately inform the Agency on all relevant facts and circumstances referring to that.

Article 28

In case the bank outsourced information system, partially or fully, outside the territory of Bosnia and Herzegovina, it shall be obliged to:

1) within the information system recovery plan define critical (key) business processes from the aspect of business continuity and their implementation in the country,
2) ensure information system resources on the territory of Bosnia and Herzegovina which are required for the recovery of business processes defined in Item 1 of this Paragraph, in required recovery timeframe,
3) ensure back up data on an annual level on the territory of Bosnia and Herzegovina in accordance with applicable regulation and
4) implement information system recovery plan testing in the country in accordance with the provisions of Article 27 of this Decision.

Article 29

(1) The bank shall establish a process of back up data management, which includes detailed procedures and responsibilities related to the manner and frequency of production, manner and period of storing, testing properness, as well as data recovery, in order to ensure data availability, and facilitate recovery, i.e. re-establishment of critical (key) business processes in required recovery timeframe in case of unforeseen events and contingency.

(2) Back up data must be updated, periodically tested and adequately protected on one or more secondary locations, out of which at least one must be distant from the one on which original data are stored, and based on conducted risk analysis. Thereby, the bank shall ensure back up data on some of external media.

(3) The bank shall adequately protect back up data when transferring and storing them, and ensure update recordings thereof.

Article 30

(1) The bank shall establish a process of incident management which facilitates timely and efficient response in case of disruption of safety or functionality of the information system resources.

(2) The bank shall, as a minimum, define procedures for registration, classification, processing, recovery and monitoring, as well as analysis and reporting on incidents.

(3) The bank shall, as a minimum, record the following types of incidents: error or disruption in functionality of hardware and software components, reduced service performance, unauthorized access to information system resources, data outflow, identity theft, malicious code, theft, unsuccessful process of back up data production, and data integrity disruption.

(4) The bank shall, immediately upon the occurrence of severe incident, whether it relates to the part of information system located in the bank or to the outsourced one (key banking application, e-banking system, card payment system, and similar), inform the Agency, and after solving the incident, it shall deliver full documentation related to the incident, which must contain data on the type of incident, incident description, its duration, consequences caused, and undertaken activities.

10. Electronic banking

Article 31

(1) The bank shall, as an integral part of information system risk management, establish a process of management of risks stemming from providing services of electronic banking, within which it is necessary to implement and document detailed assessments of these risks, at least taking into account the following: technological solutions used, outsourced services and client technical environment.

(2) In electronic banking operations, the bank shall at least:

1) establish a process for supervising, solving and monitoring of safety incidents, also including clients' complaints which refer to the safety, and regular reporting on such incidents,
2) apply safety and efficient methods of authentication for verification of identity and persons' authorizations, processes and systems,
3) ensure that authentication of e-banking user includes combination of at least two mutually independent elements required for user identity verification,
4) ensure appropriate verification of its identity on e-banking distribution channel, in order that the e-banking users could check identity and authenticity of the bank,
5) ensure that when exchanging sensitive data, safe encryption of communication channels between parties participating in the session is applied, in order to secure

confidentiality and integrity of data,

6) define maximum number of unsuccessful attempts to register in the system or authentication attempts, the longest duration of session without user's activity, as well time limit of authentication validity and

7) ensure generating, storing and regular analysis of operational and systemic recordings, as well as controls of access to sensitive data on transactions and critical resources, in order to secure indisputability and provability of actions related to electronic banking.

(3) Exempt from the Paragraph 2, Item 3 of this Article, the bank may apply user authentication which is being performed by the usage of one element for user identity confirmation, in case of:

1) payment of a smaller cash value amount, under the condition that the risks related to the total amount of these transactions are managed in appropriate manner,
2) transfer of cash funds between two accounts of the same user at the same bank and
3) payments to reliable recipients, i.e. recipients defined in advanced by the user (so-called recipients' white lists).

(4) The bank shall, for the purpose of authentication application referred to in Paragraph 3 of this Article, document comprehensive and detailed risk analysis and manner of management of risks stemming from providing services defined in the provisions of Paragraph 3, Items 1-3 of this Article.

(5) The bank shall, within the framework of e-banking system, establish transaction monitoring mechanisms in order to prevent, detect and block suspicious payment transactions before final authorization by the bank, whereas suspicious or highly-risk transactions should be subject of separate procedure of checking and assessing.

(6) The bank shall, within the information it provides to the user, related to the e-banking, state the following:

1) requirements related to the user's equipment, software or other required tools (e.g. anti-virus software, firewall, and other),
2) instructions for proper and safe usage of software and hardware resources (e.g. token, smart card, password and other), as well as procedures in case of loss or theft of resources used for registration in the system or transaction implementation,
3) procedures to be followed in case of detected misuse or suspicion of misuse and
4) description of individual responsibilities and obligations of e-banking service provider and user in relation to the use of e-banking service.

11. Transitional and final provisions

Article 32

(1) Instructions for reporting on information system management shall in more detail stipulate reporting, manner and methodology of forms filling, which are an integral part of the stated instructions.

(2) The bank shall align its operations with the provisions of this Decision within 90 days, except Article 29, Paragraphs 2-6, which shall start to be applied 180 days after the day of this Decision coming into force, and Article 10, Paragraph 4, Article 13, Paragraph 4 and Article 15, which shall start to be applied 360 days after the day of this Decision coming into force.

(3) The bank shall deliver to the Agency reports in accordance with the Instructions referred to in Paragraph 1 of this Article, starting from the reporting data as of 31/12/2017.

(4) The Decision on minimum standards of information system management in banks ("Official Gazette of Republika Srpska", No.: 1/14) shall cease to be valid on the day of this Decision coming into force).

Article 33

This Decision shall come into force on the 8th day after its publication in the "Official Gazette of Republika Srpska".

Number: UO-327/17

Date: 11 December 2017

PRESIDENT OF THE MANAGEMENT BOARD
Mira Bjelac