Pursuant to Article 64 paragraph 1 item 22 of the Law on the National Bank of the Republic of Macedonia ("Official Gazette of the Republic of Macedonia" No. 3/2002, 51/2003, 85/2003, 40/2004, 61/2005 and 129/2006), and Article 68 paragraph 1 item 4 of the Banking Law ("Official Gazette of the Republic of Macedonia" No. 67/2007), the National Bank of the Republic of Macedonia Council adopted the following

D E C I S I O N
on the bank's information system security
("Official Gazette of the Republic of Macedonia" No. 31/2008)

I. GENERAL PROVISIONS

1. This Decision shall set forth the methodology for security of the bank's information system which establishes standards for the information system security, through defining criteria for establishing process for managing the information system security, ensuring business continuity, as well as security standards for the e-banking systems and the bank's outsourcing companies.

The bank shall be required to establish a system for identification, measurement, monitoring and control of the information systems incompatibility risk.

The information systems risk, according to this Decision, shall be the risk of loss for the bank arising from losing, unauthorized utilization, or unavailability of the information, information assets and/or the services the bank provides.

2. The security of the bank's information system, according to this Decision, shall be defined as fulfillment of the following criteria:

a) **Confidentiality**: the information is accessible only to authorized users;
b) **Integrity**: safeguarding of the accuracy and completeness of the information system;
c) **Availability**: unrestricted access to the information system for the authorized users.

II. INFORMATION SYSTEM SECURITY MANAGEMENT PROCESS

3. For the purpose of accomplishing and constant maintenance of the information system security, the bank shall be required to establish information system security management process, encompassing:

- Risk assessment;
- Information system security policy;
- Security testing;
- Monitoring and upgrading; and
- Segregation of duties of the bank bodies from the aspect of information system security management.

The bank shall be required to establish a process of information system security management, which corresponds to the nature, volume and the complexness of the financial activities the performance of which was previously approved by the National Bank.

4. According to this Decision, the risk assessment shall denote establishment of a constant process, encompassing:

- identification of the bank's information system assets;
- classification of the bank's information system assets, i.e. giving value to the assets in accordance with the criteria under item 2 of this Decision;
- analysis of the probability for occurrence of threats to and weaknesses of the information system and identification of possible consequences thereof;
- giving priority to the risks depending on the volume of the potential loss they can provoke for the bank.

The bank shall be required to prepare a report on the conducted risk assessment once a year, at a minimum.

5. The bank shall be obliged to adopt and implement Information System Security Policy, defining the foundations for the process of managing the information system security risks.

6. The policy under item 5 of this Decision should contain at least the following elements:

- manner of classifying both information and information assets according to the security criteria defined under item 2 of this Decision;
- protection of personal data, in conformity with the enforced regulations in the Republic of Macedonia;
- methodology for applying risk analysis related to information system security, which defines the risk acceptability levels;
- application of the bank's strategy for managing the identified risks through establishing both action plan and budget for ensuring information system security;
- annual plan for training of the bank's employees and clients, for proper utilization of services available through the bank's information system;
- management of security incidents and establishment of suitable mechanism for their identification, reporting and efficient elimination of the possible threats to the information system security;
- defining of the security incidents levels and appropriate activities ought to be undertaken whenever the bank identifies incident;
- defining of the role of the bank's IT organizational unit, which should have suitable personnel capacity and internal working procedures, in line with the adopted acts from the information system security area;
- defining of proper audit trail for the critical parts of the information system at several levels, such as operating system, data bases, telecommunication equipment, in order to verify the identity of the activities they performed on the information system;
- defining of both internal and external audit role from the aspect of ensuring information system security;
- defining of the manner of managing the security upgrades, upgrades of new versions, application parameters and codes modification, preparation and commissioning of the applications;
- defining of the method of establishing the bank's Business Continuity Plan in executing the bank's business activities;
- manner of establishing anti-virus protection;
- defining of the manner of telecommunication connection and ensuring protection to the data that are to be transferred;
- defining of security zones in the bank, thus restricting the physical access to the bank's information and the information assets; and
- defining of the manner of establishing additional security mechanisms, such as fire prevention, flood prevention, monitoring, sensors and alarms.

For the purpose of efficient application of the policy under item 5 of this Decision, i.e. the policy elements defined in paragraph 1 of this item, the bank shall be required to establish appropriate procedures.

7. The policy under item 5 of this Decision should contain description of the administrative, technical and physical security controls and the manner of their application in the bank.

The security controls under paragraph 1 of this item should be compatible with the size and the complexness of the bank, as well as with the type of the financial activities previously approved by the National Bank.

As stated by this Decision, administrative security controls shall denote introduction of policies, standards, instructions and procedures by the bank bodies through which framework for managing the information system security is established.

As said by this Decision, the technical security controls shall mean undertaking of security measures incorporated in the computer equipment, system software, communication equipment and application program solutions.

In light of this Decision, physical security controls shall denote undertaking proper measures for limiting and control of the physical access to the information and information assets, in order to protect the bank from espionage, sabotage, fire, flood, vandalism, natural disasters and other type of damage or destruction of the entire, or part of the information system.

8. The bank shall be required to establish a process of professional, independent and objective testing of the efficiency and suitability of the implemented security controls in the information system security policy.

9. The bank shall be obliged to establish a process through which it shall constantly collect and analyze information on the losses arising from the security incidents in the operations.

The bank should establish an ongoing process through which it will constantly collect and analyze the information on the new weaknesses and threats to the information system security, and on the basis of the performed analyses, it should measure the potential losses arising thereof, that can occur if no appropriate security controls are undertaken in time.

10. The bank should establish proper organizational structure for information system security management, meaning clearly defined competencies and responsibilities of the bank bodies in the information system security management process.

With regard to paragraph 1 of this item, the bank's Supervisory Board shall be responsible for:

- approving the information system security policy and monitoring its implementation;
- assessment of the suitability of the adopted policy, at least once a year, from the aspect of the changes in the organizational structure and the changes in the bank's information system; and
- monitoring of the efficiency of the established process for information system security management, by analyzing the test results from the established information system security controls by an independent and suitably trained team, especially in cases when modifications to the information system of higher importance, or in the information system security management process occurred.

According to paragraph 1 of this item, the Risk Management Committee shall be responsible for:

- monitoring of the information system security policy and identification of the cases when its revision is necessary;
- assessment of the established information system security management process;
- analyzing the report on the conducted risks assessment under item 4 of paragraph 2 of this Decision and monitoring the activities taken with regard to information system security management; and
- determining and regular revision of the defined acceptability risk levels.

According to paragraph 1 of this item the bank's Board of Directors shall be responsible for:

- establishing and implementing the information system security management procedures, in conformity with the information system security policy, approved by the Supervisory Board;
- establishing and maintenance of the efficient system for measuring, monitoring, control and management information system for the information system security risks;
- establishing procedures for assessing the risks to the information system security, arising from the introduction of new products, and services;
- ensuring suitable organizational layout and establishing proper functions and authorizations for efficient and secure IT and information system security management in the bank;
- preparation of operating plan for application of the bank's business strategy regarding IT; and
- appointing a person responsible for information system security.

11. The person responsible for the information system security shall manage the bank's information system security and coordinate the information system policy and processes related to different technological platforms and tasks.

The person under paragraph 1 of this item should be independent from the persons operating in the bank's organizational units facing risks related to the information system security.

The bank's Supervisory Board, at least twice a year, shall be informed about operations related to the information system security.

12. The management information system under item 10 paragraph 3 line 2 should contain the following elements, at minimum:

- information about identified risks and their control;
- information on the agreements with the bank's outsourcing companies;
- results from the completed tests to the information system security, security incidents and appropriate reactions by the bank bodies; and
- identified needs for changes of the bank's information system security policy, from the aspect of its improvement.

III. ENSURING BUSINESS CONTINUITY

13. The bank shall be required to develop and apply its own business continuity plan, which will be based on several scenarios and will enable functionality and minimization of the losses in case of long term business process disruption.

14. Severe business process disruption in light of this Decision, shall represent a situation in which the bank is incapable of meeting the undertaken business obligations due to factors beyond its control, or a situation when the bank is physically damaged or there is damage to the telecommunications, i.e. the information and the information systems on which critical bank operations are performed are not available.

15. The plan under item 13 of this Decision should enable identification of the bank's critical operations, including also those depending on the outsourcing companies, or third parties. For those processes, the bank should:

- set forth the methodology for damage assessment and define the margins of the maximum allowed time for critical operations malfunction;
- identify the alternative mechanisms for business processes continuity in case of interruption of the primary mechanisms;
- identify the possibility of data recovery necessary for the business process continuity;
- identify the secondary location where the data will be protected and which should be at an adequate distance from the primary location, in order to minimize the risk of simultaneous unavailability of both locations.

For efficient implementation of the plan under item 13 of this Decision, the bank shall be required to establish procedures through which the elements defined under paragraph 1 of this item shall be properly applied.

16. The bank should periodical test the plan under item 13 of this Decision in order to conform it with the current business operations and its business policy.

IV. E-BANKING

17. E-banking, in light of this Decision, shall denote offer of bank services and products through interactive electronic communication channels, such as access to financial information, information on products and services, processing of bank transactions, etc.

18. Along the criteria stated under item 2 of this Decision, for the e-banking systems which include also processing of transactions, the bank should additionally provide the following security criteria:

a) **identification**: system for unique identification verification and authentication of the information system users identity;
b) **transaction non repudiation:** systems for verification of the information integrity and providing evidence for transfer of certain information or transactions performed by certain user.

19. The bank can make user identity verification, in light of this Decision, by applying the following methods:

- through set of symbols known only by the user, such as password, pin, etc.
- through device owned by the user only, such as electronic card, key (token), etc. and/or
- through some of the unique personal physical features of the user, such as fingerprint, iris, speech recognition, etc.

20. Safe and efficient methods for user identity verification and their authorizations should be applied by the bank in the e-banking systems.

21. User identity verification, with a combination of at least two of the defined methods under item 19, should be incorporated in the e-banking systems which include execution of transactions.

22. For the e-banking systems available through public computer network - Internet, the bank should provide valid verification of its identity through the transmission channel, in order to enable the users to verify the identity of the bank's system.

23. Proper audit trail should be incorporated by the bank in the e-bank systems thus providing non-repudiation of the transactions.

V. OUTSOURCING COMPANY

24. Outsourcing company shall denote a company, which on the basis of a written agreement, provides services to the bank from the information system area for processing bank and financial activities.

25. Before the company under item 24 of this Decision is selected, the bank should undertake the following activities:

- make legal and financial due diligence of the company's operations from legal, financial aspect, as well as from the aspect of the manner it manages the information system security defined in this Decision; and
- make risk assessment in the bank's operations, that can arise from the utilization of services, during processing of bank and financial activities from the information system area.

Selection of the company under item 24 of this Decision shall mean conclusion of new agreement or continuation of the current one for providing outsourcing.

26. The bank should not conclude agreement with the company under item 24 of this Decision, if the agreement, in any way, prevents, restricts or hampers National Bank's access when performing supervision, or oversight, in conformity with the Banking Law.

27. The company under item 24 of this Decision must not use services provided by other outsourcing companies, i.e. subcontractors, for processing of those services agreed in the agreement under item 24 of this Decision, unless not explicitly stated therein.

28. The operations of the company under item 24 of this Decision should be harmonized with the bank policy under item 5 of this Decision.

29. The policy of the bank which adopted a decision on utilization of services provided by the company under item 24 of this Decision, besides the policy elements defined in item 6 paragraph 1 of this Decision, should also envisage the following elements:

- defining the manner of determining the unique principles and rules for company selection;
- defining the protection mechanisms that should be contained in the agreements with the company, such as clause for non-disclosure of information, clause for the services quality level, clause for coordinated management of security incidents, clause for conducting independent audit, etc.

- determining standards the company should meet and which should be harmonized with the bank's business continuity plan;
- defining the manner of monitoring the services and operations quality of the company, its financial situation and its risk profile, through periodical testing of its compliance with the bank's information system security policy.

VI. TRANSITIONAL AND CLOSING PROVISIONS

30. The bank shall be required to notify the National Bank whenever identifies the highest level of security incident in the information system, according to the defined levels of security incidents under item 6 paragraph 1 line 7 of this Decision.

The bank shall be required to submit the notification under paragraph 1 of this item to the National Bank, no longer than three days from the day it is determined that security incident occurred.

31. The bank shall be required to notify the National Bank on the changes in the key parts of the information system management process, especially in case of changes in the policy elements defined in item 6 paragraph 1 of this Decision.

32. This Decision shall enter into force eighth day from its publishing in the "Official Gazette of the Republic of Macedonia", and its implementation shall commence on January 01, 2009.

33. With the implementation of this Decision, the Decision on defining the standards for preparation and implementation of the bank's information system security ("Official Gazette of the Republic of Macedonia" No. 77/2003) shall cease to be effective.

D.No. 02-15/II-7/2008
February 28, 2008
Skopje

Petar Goshev, MSc.
Governor
and President of the National Bank
of the Republic of Macedonia Council