National Bank of the Republic of North Macedonia

INFORMATION SECURITY POLICY

June 2021

Pursuant to Article 47 paragraph 1 item 9 of the Law on the National Bank of the Republic of North Macedonia (Official Gazette of the Republic of Macedonia No. 158/10, 123/12, 43/14, 153/15, 6/16 and 83/18 and Official Gazette of the Republic of North Macedonia No. 110/21 and 74/24), the National Bank of the Republic of North Macedonia Council has adopted the following

INFORMATION SECURITY POLICY
(unofficial revised text)[1]

I. GENERAL PROVISIONS

1. The Information Security Policy (hereinafter: ISP) sets forth the manner of ensuring security of information and information assets by implementation of preventive controls for mitigating any adverse effects caused by the occurrence of events that may jeopardize the security of the information system of the National Bank of the Republic of North Macedonia (hereinafter: the National Bank).

2. The ISP shall aim to ensure:
   - **confidentiality** - information and information assets shall be protected from any unauthorized access and shall be accessible only to persons with access authorization;
   - **integrity** – information and information assets shall be accurate, complete and up-to-date; and
   - **accessibility** - information and information assets shall be readily accessible and available to authorized users whenever there is a business need.

3. An information security incident is an occurrence that actually or imminently jeopardizes confidentiality, integrity and availability of information and information assets.

4. Information and information assets shall be a vital segment in the National Bank operations and used only for business purposes. Employees, appointees and other engaged persons in the National Bank undertake to protect information and information assets, as required by this Policy and internal acts.

5. The ISP shall be designed and harmonized with international information security management standards.

II. ENSURING INFORMATION SECURITY OF THE NATIONAL BANK

6. The National Bank Council shall be informed annually on the implementation of security standards and information system security.

7. The National Bank Governor shall integrate information security controls into the National Bank internal control system by:
   - supporting the information security process;

[1] This is an unofficial revised text of the Information Security Policy. It is comprised of the Information Security Policy P. No. 02-15/IX-1/2021 of 30 June 2021 and the Policy on Amending the Information Security Policy No. 02-27277/6 of 25 July 2024.

- establishing centralized oversight and coordination;
- defining roles and responsibilities;
- monitoring the National Bank compliance with ISP.

8. The National Bank Governor shall establish an Information Security Steering Committee of the National Bank for monitoring activities for ISP implementation, as well as monitoring other technological changes and upgrading the National Bank information system.

9. The Information Security Steering Committee shall report to the National Bank Governor on its operations. The work of the Information Security Steering Committee shall be regulated by rules of procedure.

10. The chief and deputy information security, personal data protection and classified information officers of the Strategy and Prevention Office shall be *Information Security Officers* (hereinafter: *ISO).* ISO shall have full autonomy and independence in their work and shall report to the National Bank Governor.

11. ISO shall propose and monitor the implementation of ISP and all other internal acts deriving from the ISP. ISO shall control the adherence to ISP and propose updates upon occurrence of information security incidents, changes to the National Bank organizational structure and technological platform.

12. ISO shall also:
    - coordinate all security activities related to the National Bank's information system;
    - analyze and assess information security risks;
    - give suggestions for ISP implementation and development;
    - propose internal acts for improving information security to the Governor;
    - cooperate with the Internal Audit Department about the subject of the annual information security audit;
    - coordinate and investigate incidents that jeopardized information security, and cooperate with external institutions, whenever applicable;
    - cooperate with the organizational unit responsible for physical security, protection and rescue of employees and property;
    - cooperate with the Legal Department about the development of internal information security regulations and clauses in third party contracts on personal data protection, confidential data, and any other sensitive information to which third parties may have access during the contract implementation;
    - organize training courses for employees regarding the ISP implementation;
    - have access to all control logs of the National Bank's information system;
    - provide consulting services to individuals who have access to the National Bank's information system for proper implementation of ISP and related internal acts.

13. The National Bank Council shall, on proposal of the National Bank Governor, assign, by authorization, a Personal Data Protection Officer (hereinafter: PDPO) for a 4-year term. PDPO shall enjoy full operational autonomy and independence.

14. The PDPO shall directly report to the National Bank Council which in turn ensures that PDPO:
    - is properly and timely involved in all personal data protection matters,
    - has all the necessary resources to perform tasks,
    - has access to personal data and processing operations,
    - constantly acquires professional knowledge,

- does not receive any instruction from senior management for his/her tasks and cannot be replaced or sanctioned for the performance of tasks,
- does not perform any other tasks and duties that may lead to conflict of interest.

15. PDPO shall:
    - prepare internal personal data protection acts and monitor their compliance with personal data protection law and bylaws;
    - inform, propose trainings, give opinions, advice and recommendations, seek to raise awareness and organize training for management and employees who process personal data about their obligations arising from the Law on Personal Data Protection (hereinafter: LPDP);
    - monitor the compliance with the LPDP and related laws, the compliance of the National Bank personal data protection regulations, including segregation of duties;
    - conduct personal data protection audits/controls and submit to the National Bank Council, an annual report on the National Bank compliance with personal data protection regulations;
    - when necessary, give advice regarding the personal data protection impact assessment and monitor the assessment implementation under the LPDP;
    - cooperate with the Personal Data Protection Agency and act as a contact point regarding issues related to personal data processing, including prior consultation with the Agency before processing, if the personal data protection impact assessment shows that unless measures are taken to mitigate risks personal processing data will pose risk to the rights and freedoms of individuals;
    - act as a point of contact with personal data subjects on issues related to personal data processing and exercising their rights under the LPDP;
    - analyze reports from the supervision conducted by the Personal Data Protection Agency and submit proposals to the Governor for the measures to eliminate any identified shortcomings;
    - check the recorded events in the audit trail management system and
    - may perform other tasks and duties if they do not lead to a conflict of interest.

16. In addition to the obligations under items 12 and 15, ISO and PDPO shall respect confidentiality of documents, data and information that they access during their operations.

17. Tactical managers shall:
    - prepare and update internal operating procedures in accordance with ISP;
    - analyze and assess risks to information security within the organizational units they manage and,
    - assess the impact of personal data protection, if they are managers of an organizational unit that processes personal data.

18. The National Bank employees shall comply with the ISP and the internal information security regulations.

19. The National Bank employees shall inform the tactical managers and the ISO/PDPO when they:
    - determine that an event has occurred that compromise information security;
    - identify obstacles in the information system operations, and
    - suspect that an event may occur that threatens information security.

20. The National Bank security shall apply appropriate measures when third parties have access to segments of the National Bank information system, in accordance with the ISP and the relevant internal acts.

21. The Internal Audit Department (hereinafter: IAD) shall conduct an audit of the adequacy and effectiveness of the system of internal controls for the information system security in the National Bank and shall check whether the procedures and instructions contained in the documentation for the technical and organizational measures for personal data security, are applied and whether they are in accordance with data protection regulations.

21-a. IAD shall plan the audits on the basis of an analysis of the risk and IAD's available resources, taking into account the operations, the volume and the manner of processing personal data, and in accordance with the Annual Work Program of the IAD adopted by the National Bank Council.

21-b. IAD shall prepare audit reports referred to in item 21 in accordance with the Internal Audit Policy. IAD shall prepare an annual report regarding the area which refers to personal data security and shall submit it to the Governor and to the Personal Data Protection Officer.

Personal data processing principles

22. The National Bank applies relevant technical and organizational measures to make sure that personal data is processed in accordance with the law, observing the following principles:

- Lawfulness, fairness and transparency - the processing is performed in accordance with the law, sufficiently and transparently in relation to the data subject;
- Purpose limitation - data is collected for specific, clear and legitimate purposes and is not processed in a manner that is inconsistent with those purposes;
- Data minimization - data processed are appropriate, relevant and limited to what is necessary to achieve the processing purposes;
- Data accuracy - the data are accurate and where necessary updated. Where appropriate, measures are taken to timely erase or rectify data that is inaccurate or incomplete, having in mind the purposes for which they were processed;
- Storage limitation - the data are stored in a form that enables identification of data subjects, for as long as it is necessary for achieving the purposes for which they are processed; and
- Integrity and confidentiality - data is processed in a manner that ensures an appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

III. CLOSING PROVISIONS

23. The National Bank Governor shall adopt internal acts for the ISP implementation.

24. Once this Policy enters into force, it shall supersede the Information Security Policy of the National Bank P. No. 02-15/IX-5/2011 of 15.09.2011, P. No. 02-15/I-2/2015 of 29 January 2015 and P. No. 02-15/III-2/2016 of 24 March 2016.

25. This Information Security Policy shall enter into force on the date of adoption.

Anita Angelovska Bezhoska

Governor and Chairperson
of the National Bank of
the Republic of North Macedonia Council

Skopje