DRAFT
APPROVED BY
Resolution ____ of ____2019

of the Board of Directors

ARARATBANK OJSC

A. Suvaryan _____

Chairman of the Board of Directors

INFORMATION SECURITY POLICY

Effective since_____2019

SECTION I: PURPOSE, SCOPE OF APPLICABILITY, RELATED DOCUMENTS AND DEFINITIONS

CHAPTER 1: PURPOSE

1. ARARATBANK OJSC is a commercial bank operating in the territory of the Republic of Armenia, which provides financial services to individuals and legal entities. The above mentioned activity is related to information management, which is one of the most important assets of ARARATBANK OJSC and is dependent on providing information security, which is a set of other activities aimed at ensuring the privacy, integrity and accessibility of information assets, continuous development and improvement of information security management.

CHAPTER 2: SCOPE OF APPLICABILITY

2. The Information Security Policy shall apply to all employees of ARARATBANK OJSC and all interested third parties.

CHAPTER 3: RELATED DOCUMENTS

3. The Information Security Policy pertains to the following main documents below:

    1) Procedure on Defining Minimum Requirements for Ensuring Information Security, approved by Resolution of the Board of the Central Bank of the Republic of Armenia No 173-N, dated July 09, 2013.
    2) Charter of ARARATBANK OJSC, approved by the Resolution of General Meeting of Shareholders of ARARATBANK OJSC No 04/01 dated 29.12.2008 (with amendments).
    3) Risk Management Policy, approved by the Board Decision of ARARATBANK OJSC No 15/03L-H from November 10, 2015.
    4) The Board Decision of ARARATBANK OJSC No 11/09L from September 14, 2017 “On Approving the Administrative-Organizational Structure of ARARATBANK OJSC”.
    5) The Board Decision of ARARATBANK OJSC No 01/01L from January 8, 2013 “On Approving a New Staff List of ARARATBANK OJSC”.
    6) The Board Decision of ARARATBANK OJSC No 23/01L from June 22, 2017 “On Approving a Staff List of the Head Office of ARARATBANK OJSC”.
    7) Procedure on “Working out and Approving Draft Legal Procedures”, approved by the Board Resolution N11/01L from November 04, 2014.
    8) Procedure on “Classification and Identification of the Bank’s Information Assets”, approved by Board Resolution No 11/02L from November 04, 2014.
    9) ISO/IEC 27001 “Information technology - Security techniques - Information security management systems – Requirements”.

CHAPTER 4: DEFINITIONS AND ABBERVIATIONS

4. Below are the main concepts used in the Information Security Policy:

1) **Bank** stands for ARARATBANK OJSC.
2) **Policy** stands for the Information Security Policy.
3) **ISRE** stands for the information security responsible employee in the Security Department.
4) **ISMS** stands for the information security management system.

CHAPTER 5: AMENDMENTS AND SUPPLEMENTS

5. Edition 03, amendments have been introduced into sub-clauses 3, 4 and 6 of clause 3, and clause 9 of the Policy.

CHAPTER 6: ANNEXES

6. The Policy has no Annexes.

SECTION II: DESCRIPTION

CHAPTER 1: GENERAL PROVISIONS

7. The Policy shall define the goals, issues and approaches in the field of information security which the Bank is guided by during its operation.
8. The parties interested in the incorporation and improvement of ISMS are listed below:
   1) The Board of Directors of the Bank;
   2) The Executive Board of the Bank;
   3) The management of the Bank;
   4) The customers of the Bank;
   5) The partners of the Bank.
9. Actions taken within the framework of ISMS shall apply to all structural and territorial subdivisions of the Bank. The list of structural subdivisions has been approved by the Board Decision of ARARATBANK OJSC No 11/09L from September 14, 2017 "On Approving the Administrative-Organizational Structure of ARARATBANK OJSC" and has been placed in the website of the Bank at https://www.araratbank.am/տեղեկություններ-մեր-մասին/. The list of branches has been placed in the website of the Bank at https://www.araratbank.am/hy/branches. The staff list of the Head Office has been approved by the Board Decision of ARARATBANK OJSC No 23/01L from June 22, 2017 "On Approving a Staff List of the Head Office of ARARATBANK OJSC". The staff list of the Head Office has been approved by the Board Decision of ARARATBANK OJSC No 01/01L from January 8, 2013 "On Approving a New Staff List of ARARATBANK OJSC".
10. The policy shall pursue the following goals and approaches:
    1) to ensure continuity of the main business processes in the Bank;

2) Possibly mitigate potential losses and damages arising from violations in the field of information security;
3) Prevent violations in the field of information security;
4) Exercise control over the encryption of information;
5) Manage encryption keys;
6) Control information accessibility;
7) Clean desk approach;
8) Clean screen approach;
9) Destruction approach to electronic data carriers;
10) Security approach to portable devices;
11) Security approach to computer networks;
12) Approach to password management;
13) Information classification;
14) Physical security;
15) Acceptable use of assets;
16) Information transmission;
17) Software installation and usage restrictions;
18) Backup;
19) Protection against malware;
20) Vulnerability management;
21) Privacy and protection of personal information,
22) Approach to the relationships with the institutions providing services to the Bank.

CHAPTER 2: INFORMATION SECURIY MANAGEMENT

11. To accomplish the goals set out in clause 10 of the Policy, ISMS shall be incorporated in the Bank, which must comply with:
    1) the requirements of ISO/IEC 27001:2013 “Information technology - Security techniques - Information security management systems – Requirements”.
    2) the requirements of the RA legislation and internal legal acts of the Bank, and contractual obligations.
    3) the Risk Management Policy of the Bank.
12. ISMS shall be regulated by the Policy and other internal legal acts approved within the framework thereof.
13. The Bank’s ISMS shall cover the Bank’s Head Office, regional and structural subdivisions, processes related to the Bank’s activity, the Bank’s staff, information processing and storage systems.
14. All and any information assets of the Bank, asset holders, asset keepers and users, including equipment, software, information resources on paper and electronic media shall be subject to registration and classification according to their degree of importance and availability.
15. Information security risks shall be regularly assessed in compliance with the Bank's Procedure of Information Security Risks Management. During assessment, potential vulnerability and threats of

information security and degree of their impact on the Bank's business processes, financial position and business reputation shall be taken into account.

16. The assessment of information security risks shall result in drafting of the risk management plan, selection and application of information protection management tools, including organizational, physical, technical, software and software-hardware tools to ensure the safety of ISMS.
17. For the physical protection of the Bank's information assets, security zones shall be defined and measures shall be taken within the scope of ISMS to prevent unauthorized access.
18. The Bank shall seek to detect, consider and respond to the incidents having taken place in the information security field in accordance with the established procedures.
19. The Bank has established procedures for ensuring the continuity of critical business processes and controlling ISMS operational capability against significant breakdowns or emergency situations of information systems.
20. Employees of the Bank shall get access to the information necessary to perform their functional duties. The Bank shall regularly inform, train and improve qualification of its employees in the field of information security.

CHAPTER 3: CONTROL OVER THE INFORMATION ENCRYPTION

21. Information in the Bank shall be encrypted.
22. The applicable encryption key length shall be at least 128 bits.
23. The length of encryption keys shall be regularly reviewed within the framework of security and upgrading to the extent allowed by the encryption technology in place.

CHAPTER 4: MANAGEMENT OF ENCRYPTION KEYS

24. Encryption keys and certificates in place in the Bank shall be managed undergoing the following stages:
    1) Key generation for encryption systems;
    2) Issue and receipt of public-keys;
    3) Dissemination of keys;
    4) Storage of keys;
    5) Replacement (rekeying or key updates);
    6) Decision on dealing with endangered keys;
    7) Cancelling keys;
    8) Recovery of damaged or lost keys;
    9) Key backup and archiving;
    10) Key destruction;
    11) Logging of main events of keys.
25. Encryption keys in place in the Bank shall be changed every six months.

CHAPTER 5: CONTROL OVER THE INFORMATION ACCESS

26. In order to protect against unauthorized access to information and information processing systems, the Bank shall organize control over access to information and information processing systems.
27. Bank employees and, where necessary, contractors shall be provided access to information and information processing systems in compliance with respective legal acts incorporated in the Bank.
28. In order to prevent against unauthorized access, the Bank shall apply a time limit of inactivity, as a result of which the system is automatically blocked.
29. At least once a year, a committee comprised of Heads of different subdivisions shall be set in the Bank and the scope of competences shall be reconsidered by making a list of model competencies in compliance with official duties of employees.

CHAPTER 6: CLEAN DESK AND CLEAN SCREEN

30. In order to protect against unauthorized access to information and prevent information leakage, the following approaches shall be applied:
    1) During non-working hours, all and any documents in the Head Office and subdivisions of the Bank must be stored in respective iron or other lockable cabinets.
    2) The doors of the workplaces which lack iron or other cabinets must be locked when leaving the room.
    3) Accessed computers and other data processing systems must not be left uncontrolled.
    4) Computer screens must be positioned in a way to protect against accidental disclosure of screen contents to unauthorized persons.
    5) Computers must be locked when leaving the desk.
    6) By the end of the working day, Bank employees must exit all activated systems and shut down computers.

CHAPTER 7: DESTRUCTION OF DATA CARRIERS

31. A data carrier shall be considered the carrier wherein information is stored. Among the mentioned data carriers are:
    1) documents;
    2) hard disks;
    3) CDs and DVDs;
    4) magnetic disks;
    5) flash drives;
    6) memory cards etc.
32. In accordance with the procedure incorporated in the Bank and in order to exclude an opportunity to recover information, the following destruction approach to data carriers shall be applied:
    1) information removal/erasure in compliance with DoD 5220.22-M standard.
    2) physical destruction of a data carrier in a way which makes impossible to recover information and use the data carrier.

CHAPTER 8: SECURITY OF PORTABLE DEVICES

33. Portable (mobile) devices are considered one of the vital elements of the Bank's business process. However, because of being portable, such devices become more vulnerable in terms of theft of devices and leakage of information.
34. In order to mitigate and exclude such vulnerabilities and in accordance with the procedure incorporated in the Bank, the following approaches to protection of portable (mobile) devices shall be applied:
    1) Physical security control of portable (mobile) devices;
    2) Antivirus protection against viruses and other malware;
    3) Control over unauthorized access to the information of the Bank through portable (mobile) devices.

CHAPTER 9: SECURITY OF COMPUTER NETWORKS

35. The Bank's computer network is an essential and integral part of the management system, information processing and transmission, and — for the purposes of ensuring security thereof — virtual local area network (VLAN), inter-network displays, virtual private networks, antivirus protection systems and other security measures shall be applied in the Bank in compliance with the existing procedures.

CHAPTER 10: PASSWORD MANAGEMENT

36. In order to protect and manage passwords, the following approaches shall be applied:

    1) Passwords must be never stored on sheet of paper, in a software file or portable device;
    2) If you suspect someone else has learned your password, you then must change it.
    3) Password minimum requirements:
        a. passwords must be easy for the creator to remember;
        b. passwords must not be based on anything somebody else could easily guess (e.g., names, telephone numbers or other data);
        c. Passwords must not be vulnerable to dictionary attacks;
        d. Passwords must contain alphanumeric characters;
        e. Passwords must be replaced once you have registered.
    4) Never provide you password to another employee.
    5) Never remember passwords in computer software to access the system automatically.
    6) Never use the same password for multiple systems.

37. In order to ensure information security, the passwords of computer equipment and information processing systems shall be changed in compliance with the procedure incorporated in the Bank.

CHAPTER 11: INFORMATION CLASSIFICATION

38. In order to protect information, information classification shall be used in compliance with the procedure incorporated in the Bank.

CHAPTER 12: PHYSICAL SECURITY

39. In order to ensure physical security, security zones shall be applied in compliance with the procedure adopted in the Bank.

CHAPTER 13: ACCEPTABLE USE OF ASSETS

40. In order to protect information assets, acceptable operation rules of assets shall be used in compliance with the procedure adopted in the Bank.

CHAPTER 14: INFORMATION TRANSFER

41. In order to protect information, information transfer rules shall be applied in compliance with the procedure adopted in the Bank.

CHAPTER 15: SOFTWARE INSTALLATION AND USAGE RESTRICTIONS

42. In order to avoid the installation and use of malicious software (malware), the Bank shall apply restrictions on the installation and use of software in accordance with the established procedure.

CHAPTER 16: BACKUP

43. In order to exclude information loss, information shall be backed up in compliance with the procedure adopted in the Bank.

CHAPTER 17: PROTECTION AGAINST MALICIOUS SOFTWARE (MALWARE)

44. In order to protect against malicious software (malware), eligible software list shall be applied in the Bank in compliance with the procedure adopted in the Bank.

CHAPTER 18: VULNERABILITY MANAGEMENT

45. Vulnerability detection systems shall be used in the Bank for the purpose of managing vulnerabilities. Information security risks shall be assessed based on the detected data and, hence, managed and mitigated in compliance with the procedure adopted in the Bank.

CHAPTER 19: PERSONAL DATA PRIVACY AND PROTECTION

46. Personal data privacy and protection shall be applied in the Bank in compliance with the requirements of the Armenian legislation.

CHAPTER 20: RELATIONSHIP WITH SERVICE PROVIDERS

47. Non-disclosure and confidentiality agreements must be concluded with the organizations that provide services to the Bank and have access to information or information processing systems.

SECTION III: RESPONSIBILITY FOR THE VIOLATION OF POLICY REQUIREMENTS, FINAL PROVISIONS

CHAPTER 1: RESPONSIBILITY FOR THE VIOLATION OF POLICY REQUIREMENTS

48. Bank employees shall be personally liable for compliance with ISMS requirements and shall be obliged to inform the ISRE about any violation detected in the field of the information security.
49. Employment contracts and official instructions provide for responsibility for the maintenance of official documents and sensitive information that is made known to employees when performing their official responsibilities.
50. The management of the Bank shall overall manage the information security of the Bank and shall ensure necessary conditions for the following:
    1) measures aimed at the assessment of information security risks and information protection;
    2) efficiency of ISMS operation;
    3) regular training and requalification of Bank employees in the field of information security;
    4) allocation of the resources necessary for regular operation of ISMS.

CHAPTER 2: FINAL PROVISIONS

51. The Bank highlights continuous development and improvement of ISMS.
52. The management of the Bank shall be directly responsible for compliance with Policy requirements and for compliance of employees, including contractors and/or service providers with the requirements, who have access to the infrastructures of the Bank and make use thereof when performing their duties.
53. The Policy may be provided to all interested parties and posted on the official web page of the Bank either wholly of partially (in the form of a statement).
54. The Security Department shall overall control and the Internal Audit Department shall supervise compliance with the Policy provisions.