INFORMATION SECURITY POLICY

CONTENT

SECTION 1. PROVISIONS RELATED TO THE DOCUMENT

CHAPTER 1. PURPOSE OF THE DOCUMENT

1. The purpose of this Policy is to define the main concepts of information security within " QUALITY TESTING LAB " LLC.

CHAPTER 2. SUPPORTING DOCUMENTS

2. This Policy is supported by the following documents:
    1) ISO/IEC 27001:2013 "Information technology — Security techniques — Information security management systems — Requirements" standard.
    2) " QUALITY TESTING LAB " LLC Charter.

CHAPTER 3. DEFINITIONS AND ABBREVIATIONS

3. The following key concepts and abbreviations are used in this Policy:
    1) ***Organization*** - " QUALITY TESTING LAB " LLC;
    2) ***Policy*** – *Policy on Information Security*
    3) ***IS*** – *Information Security*
    4) ***CISO*** – *Chief Information Security Officer*
    5) ***ISMS*** – *Information Security Management System*

CHAPTER 4. AMENDMENTS, ADDITIONS AND REVIEWS

4. Version 01, with no amendments.
5. This Policy shall be reviewed as required, at least once every three years.

CHAPTER 5. APPENDICES

6. There are no appendences available in the Policy.

CHAPTER 6. SCOPE OF DOCUMENT

7. This Policy applies to staff of the Organization.

CHAPTER 7. RESPONSIBILITY

8. CISO is responsible for maintaining the compliance of requirements, reviews and updates of the Policy and the Director is responsible for the overall control.

CHAPTER 8. OBLIGATIONS OF MANAGEMENT AND STAFF OF THE ORGANIZATION

9. The implementation of the requirements provided by the Policy is mandatory for all the employees of the Organization.
10. The control over the requirements provided by this Policy is carried out by CISO and the supervision by the Director of the Organization.

SECTION 2. PROVISIONS RELATED TO THE POLICY

CHAPTER 9. PROVISIONS RELATED TO THE POLICY

11. The Policy defines the IS goals, objectives, and approaches.
12. The Policy is designed
    1) to ensure the continuity of the Organization's core business processes
    2) for the maximum reduction of losses and damages as a result of IS violations
    3) for prevention of IS violations
    4) to monitor information encryption
    5) to manage encryption keys
    6) to ensure information availability
    7) to ensure the use of clear desk and screen principles
    8) to ensure the use of media disposal principles
    9) to maintain the security approaches for mobile devices
    10) to maintain the security approaches to computer networks
    11) to maintain password management approaches
    12) to maintain information classification approaches
    13) to ensure physical security
    14) to maintain acceptable approaches to the asset management
    15) to maintain the information transfer approaches
    16) to maintain thee approaches to software installation and usage restrictions
    17) to maintain back-up approaches
    18) for the protection against malicious programs
    19) for the vulnerability management
    20) for the protection of the personally identifiable information
    21) to reduce IS risk in relationships with Organization's partners.

CHAPTER 10. PROVISIONS ON THE ORGANIZATION'S INFORMATION SECURITY MANAGEMENT SYSTEM

13. For the implementation of the purposes provided for in point 12 of this Policy, the Organization shall implement ISMS, which shall comply with:
    1) with ISO/IEC 27001:2013 "Information technology — Security techniques — Information security management systems — Requirements" standard.

2) with the legislation of the Republic of Armenia
3) with the internal requirements set in the Organization's internal legal acts as well as the contractual agreements.

14. The interested parties for the ISMS implementation are:
    1) Organization's investors
    2) Organization's shareholders
    3) Organization's management
    4) Organization's employees
    5) Organization's partners
    6) Organization's clients.
15. Organization's ISMS scope includes all offices, structural subdivisions of the Organization (if any), processes related to the Organization's activities, staff, information processing and storage systems.
16. All information assets of the Organization, asset owners, holders, custodians, and users, including equipment, software, information on paper or electronic media, are subject to accounting and classification according to their level of criticality and availability.
17. The annual assessment of information security risks is carried out in accordance with the Organization's "Information Security Risk Management Procedure".
18. As a result of information security risk assessment, a risk management plan is developed, information protection management measures are selected, applied, including organizational, physical, technical, and software means of ensuring the security of the ISMS.
19. Security zones are established for the physical protection of the Organization's information assets within the scope of the ISMS measures are taken to prevent unauthorized access.
20. The Organization records and resolves IS incidents in accordance with the Organization's "Information Security Incident Management Policy".
21. The Organization establishes procedures for ensuring the continuity of critical business processes in the event of significant failures of information systems, emergency situations, and control over the efficiency of the ISMS.
22. Organization employees receive access to the information necessary for the performance of their job responsibilities.
23. The Organization regularly informs, trains and upgrades employees in the field of IS.

CHAPTER 11. INFORMATION ENCRYPTION

24. The Organization shall perform information encryption.
25. The minimum applicable length for the encryption keys is 128 bit.
26. The length of encryption keys is periodically reviewed as part of security upgrades.

CHAPTER 12. MANAGEMENT OF ENCRYPTION KEYS

27. The management of Organization's encryption keys and certificates is carried out in the following stages:
    1) generating keys for encryption systems
    2) issuance and receipt of open key certificates
    3) distribution of keys
    4) key storage
    5) key replacement or upgrade
    6) management of compromised keys

7) cancellation of keys
8) recovery of damaged or lost keys
9) key duplication and archiving
10) destruction of keys
11) logging of essential key events.

28. Organization's encryption keys are changed at least once every six months.

CHAPTER 13. INFORMATION ACCESS MANAGEMENT

29. To protect unauthorized access to information and information processing systems, the Organization monitors the access to information and information processing systems.
30. Organization employees and if required the third parties are given access to the information or information processing system as prescribed by the Organization's "Access Management Policy", as well as the contracts signed with the third parties.
31. To prevent unauthorized access, the Organization applies a time limit for inactivity, as a result of which the system is automatically blocked.
32. At least annually, the Organization shall establish a commission consisting of the heads of different organization units and performs the reviews of accesses by creating typical access metrics in accordance with the job duties of the employees.

CHAPTER 14. PRINCIPLES ON CLEAR DESK AND SCREEN

33. To protect unauthorized access to information and prevent leakage, the Organization applies the following principles:
    1) Organization's all documents must be kept in accordance with their marking,
    2) in areas where iron or other cabinets are inaccessible, the doors of the rooms shall be closed when leaving the room.
    3) logged in computers and other information processing systems shall not be left out of control
    4) computer screens shall be placed in a position where outsiders can not view the screen
    5) when leaving the computer, it is necessary to lock the computer
    6) at the end of the business day, the employees of the Organization shall log out from all activated systems and turn off the computers.

CHAPTER 15. DESTRUCTION OF INFORMATION MEDIAS

34. Information media are
    1) documents
    2) hard disks
    3) CD and DVD disks
    4) magnetic carriers
    5) flash drives
    6) memory cards
    7) other media.
35. Information media can be destructed:
    1) information deletion/destruction, done in accordance with the DoD 5220.22-M standard
    2) by using physical destruction

3) by using shredders.

CHAPTER 16. SECURITY OF MOBILE DEVICES

36. The security principles of removable (mobile) media are:
    1) physical security control of removable (mobile) devices
    2) protection against malicious programs
    3) exclusion of unauthorized access to the Organization's information via mobile devices

CHAPTER 17. NETWORK SECURITY

37. The Organization's computer network is an integral part of the management system, information processing and transmission, the security of which can be used for virtual local area networks (Wireless LAN), intercom screens, virtual private networks, antivirus protection systems and other security measures.

CHAPTER 18. PASSWORD MANAGEMENT

38. The Organization shall use the following approaches for password protection and management
    1) it is forbidden to store passwords on paper, in a software file or on a mobile device
    2) in case of suspicion of guessing the password by other persons, it is necessary to change the password
    3) the minimum requirements for creating passwords are:
        - should be easy for the creator to remember
        - when creating a password, it is forbidden to rely on a name, phone number or any other data that can be easily guessed by others
        - should not be sensitive to dictionary attacks
        - shall contain numeric and letter symbols
        - shall be replaced upon the first log in to the Organization's information systems
    4) it is prohibited to provide the password to other persons, including other employees of the Organization
    5) it is prohibited to use the "Remember Password" function for automatic access to computer programs
    6) it is forbidden to use the same password for several systems.
39. To ensure information security, the passwords of computer equipment and information processing systems in the Organization are changed in accordance with the procedure of the Organization.

CHAPTER 19. INFORMATION CLASSIFICATION

40. For the purpose of information protection, in accordance with the Organization's "Information Classification Procedure", information classification is done.

CHAPTER 20. PHYSICAL SECURITY

41. For the physical security, special security zones are used as prescribed in the Organization's "Procedure on Physical Security".

CHAPTER 21. ACCEPTABLE USE OF ASSETS

42. To protect information assets, in accordance with the Organization's "Information Systems Acquisition, Development and Maintenance Policy", the rules of acceptable asset operation are applied.

CHAPTER 22. INFORMATION TRANSFER

43. To protect information, the Organization applies the "Information Transfer Policy".

CHAPTER 23. RESTRICTIONS ON INSTALLATION AND USE OF SOFTWARE

44. To avoid the installation and use of malicious software, the Organization, in accordance with the Organization's "Software Installation Procedure", applies restrictions on the installation and use of software.

CHAPTER 24. BACK-UP

45. To exclude loss of information, according to the Organization's "Data Achieving and Backup Procedure", backup of information is used.

CHAPTER 25. PROTECTION FROM MALICIOUS SOFTWARE

46. To protect against malware, the Organization uses a permissible list of software in accordance with the procedures adopted by the Organization.

CHAPTER 26. VULNERABILITY MANAGEMENT

47. To manage vulnerabilities, the Organization uses vulnerability detection systems, based on the data of which the IS risks are assessed; as a result, according to the procedures adopted in the Organization, those risks are managed and reduced.

CHAPTER 27. PRIVACY AND PROTECTION OF PERSONAL INFORMATION

48. Confidentiality of personal information and protection is carried out in accordance with the requirements of the RA legislation, internal legal acts of the Organization and relevant international standards.

CHAPTER 28. RELATHIONSHIPS WITH THIRD PARTIES

49. Non-disclosure or confidentiality agreements should be signed with third parties providing services to the Organization, that have access to information or information processing systems.

SECTION 3. AVAILABILITY OF THE DOCUMENT

CHAPTER 29. AVAILABILITY

50. The Policy is available to all employees of the Organization.
51. Within 5 business days after signing the employment contract with the new employees, CISO provides them with the current version of the Policy, as well as notifies the Organization staff about the amendments and/or additions made to the Policy within 5 business days after the approval.