«Approved»

The Central Bank of the

Republic of Azerbaijan

Decision # 26/4

10 December 2014

Regulations
on security of information systems in banks

1. General provisions

These Regulations have been developed in accordance with Clause 44.5 of the Law of the Republic of Azerbaijan on the Central Bank of the Republic of Azerbaijan, Clause 38.3 of the Law of the Republic of Azerbaijan on Banks, and determine minimum requirements for the security of information systems in banks in order to protect banking information.

2. Definitions

2.1. Definitions used herein shall have the following meanings:

2.1.1. authorization - confirmation of banking operations verification in information systems;

2.1.2. workstation – computer with access to information systems of the bank;

2.1.3 online interface — real-time direct online information and communication contact established between two or more information systems;

2.1.4. unauthorized access — an attempt to access information systems by an unauthorized user;

2.15. user — person authorized to access bank's information systems;

2.1.6. system administrator — bank employee eligible to make changes to one or more information systems of the bank, create back-up copies of systems, and monitor system's operations, and other functions of information systems based on allocation of responsibilities;

2.1.7. security administrator — bank employee responsible for protection of the bank's one or more information systems, and for unauthorized interventions to information, who is not subordinate to the structural division responsible for application of the bank's information technologies;

2.1.8. topology diagram - a description of the network connection scheme of information technology equipment.

2.2. The definitions -"information system" and "information technology" – used herein shall bear the meanings specified in the Law of the Republic of Azerbaijan on Information, informatization, and protection of information, and the definition – "data"- the meaning specified in the Law of the Republic of Azerbaijan on Electronic Signature and Electronic Document.

3. Main requirements for information systems and information technologies

3.1. Banks should meet the following requirements in order to ensure the effectiveness and security of information systems:

3.1.1. information systems should operate in a reliable and consistent manner in accordance with the bank's strategic plan;

3.1.2. risks (IT risks) arising from problems that occur in the bank's information systems or information technologies should be managed effectively;

3.1.3. business continuity procedures of information systems should be in place in case of emergency;

3.1.4. responsibilities on the use and management of information systems and information technologies should be allocated among bank employees;

3.1.5. system and security administrator (s) should be appointed in the bank;

3.1.6. topology diagram should be developed to cover the location area of IT equipment, the place of lines used for connecting system elements, supportive services (communication, power supply), back-up facilities, and other elements needed to ensure system security.

4. Access to data in information systems

4.1. Users’ access to information systems should be based upon the allocation of responsibilities in the bank.

4.2. The bank should have procedures that identify rules on creation, modification and cancellation of records of users and system administrators in the system, and their access to information systems.

4.3. The system administrator shall create users in information systems, and the security administrator shall define and modify responsibilities, and deactivate users.

4.4. Banks should regularly reconcile system access records against system access authorizations in order to reduce the risks of errors, fraudulent activities, unauthorized access, and unauthorized modification and removal of data.

4.5. Banks should have appropriate physical safeguards and controls for IT hardware to prevent any unauthorized external access to information systems.

5. Emergency handling procedures

5.1. Every bank shall ensure continuity of operations when information systems and information technologies are damaged, destroyed or threatened.

5.2. In order to ensure continuity of operations banks shall ensure the following:

5.2.1. a Back-Up Center should be created away from the bank for storage of back-up copies of information systems and to restore operations;

5.2.2. a continuity plan for bank’s operations in case of emergency should be developed and approved. The continuity plan should determine communication measures in case of emergency, restoration of bank operations, transition to the Back-up Center and the subsequent recovery procedures;

5.2.3. the capacity of information systems to support continuity of operations of the bank in case of emergency should be evaluated at least every 6 months and results documented;

5.2.4. In order to ensure continuity of operations in emergencies, banks shall train relevant personnel not less than once a year on procedures to be followed during crashes in the information systems and IT equipment, and results documented.

6. Risk management

6.1. IT risks should be managed in accordance with the Regulations on Risk Management in Banks, dated December 9, 2013, approved by Resolution No. 24/3 of the Management Board of the Central Bank of the Republic of Azerbaijan.

6.2. Banks should implement the following arrangements on the automated banking information system (hereinafter - ABIS) in order to minimize IT risks:

6.2.1. maintain daily, weekly, monthly and annual back-up copies of databases;

6.2.2. maintain logs and create back-up copies of any changes in databases;

6.2.3. keep daily back-up copies of the database for no less than 1 week, weekly copies for no less than 1 month, monthly copies no less than 1 year and yearly back-up copies no less than 5 years;

6.2.4. before handing yearly copies over to the bank's archives, run them through a data restoration procedure on the back-up server;

6.2.5. develop and apply document authorization mechanisms in the ABIS;

6.2.6. establish interfaces between the ABIS and bank’s payment system and other information systems, excluding the possibility of modifying transmitted data;

6.2.7. establish online interfaces between the bank's head office and branch offices, divisions and exchange bureaus;

6.2.8. maintain back-up copies of information systems at the Back-Up Center.

7. Information security

7.1. Data processing servers of banks should meet the following requirements:

7.1.1. use licensed software distributed under the terms of a free and open license agreement, to be agreed upon with the security officer and the structural division responsible for the application of IT.

7.1.2. server software should be agreed upon with the information security officer;

7.1.3. information systems should be protected by antivirus software and the software base updated on a daily basis.

7.2. Information system users and system administrators should be equipped with an authentication function, which meets the following requirements;

7.2.1. each user and system administrator should have a password;

7.2.2. the validity period of passwords should be a maximum of 30 days;

7.2.3. the system user password should have at least 8 characters;

7.2.4. the system administrator password should have at least 10 characters;

7.2.5. the password should be changed by the user at the first entry to the system;

7.2.6. after 3 erroneous entries of a password, access to the system should be blocked and only system administrators should be authorized to lift the system access denial;

7.2.7. reuse of the last 12 passwords used in the system should be automatically prevented;

7.2.8. system administrators should not be able to access other users' passwords;

7.2.9. an automatic verification function should be activated to check whether the password have both letters (the password should have at least one capital letter) and numbers;

7.2.10. passwords should not be displayed on the screen;

7.2.11. a password-protected screen saver should be available;

7.2.12. passwords of all system administrators should be kept in a sealed envelope in a safe place.

7.3. The following requirements should be met when implementing cryptographic protection systems:

7.3.1. passwords should be maintained in encrypted form;

7.3.2. password transmission should be encrypted;

7.3.3. data should be encrypted when transmitted to external communication channels;

7.3.4. data should be recorded to external drives in encrypted form;

7.4. Each bank shall have the following arrangements for the protection of server rooms:

7.4.1. server rooms should be equipped with fire-proof furniture;

7.4.2. installation, replacement and repair of equipment in, and removal of equipment from server rooms, and the work of outside specialists shall be carried out under the supervision of the system administrator and (or) security administrator;

7.4.3. rooms should be built using sustainable materials (stone, brick, concrete);

7.4.4. server rooms should be equipped with surveillance cameras allowing to observe the whole area at the same time. Surveillance camera shooting should be kept by the security administrator for at least six (6) months.

7.4.5. server room doors should always be kept closed and only authorized persons should be provided access to rooms;

7.4.6. rooms should be equipped with fire protection systems in good working condition, as well as fire-fighting equipment;

7.4.7. all exterior windows (if any) should be provided with iron bars or bulletproof glass. All exterior windows should be equipped with coating for inside of the room not to be seen from outside;

7.4.8. server rooms should be equipped with a generator and power source providing uninterruptible electrical power;

7.4.9. the floor and ceiling of the room should be provided with anti-static coating;

7.4.10. rooms should be equipped with ventilation (air conditioning) equipment, and thermometers to regulate heat;

7.4.11. rooms should be equipped with humidity measurement devices and humidity regulating equipment.