

‘Approved’  
Central Bank of  
the Republic of Azerbaijan  
Decision № 20/1  
14 July 2021

## **Regulations on information security management in banks**

### **1. General provisions**

1.1. These Regulations have been developed in accordance with Article 38.3 of the Law of the Republic of Azerbaijan on Banks and determine minimum requirements on information security in banks and local branches of foreign banks operating in the Republic of Azerbaijan (hereinafter – banks) in light of the requirements of the International Organization for Standardization ISO/IEC 2700X.

1.2. The requirements determined with these Regulations target banks’ entire business processes and information systems, as well as cover activities of all structural units responsible for management of those business processes and information systems.

1.3. Requirements on protection of private data are regulated with the Law of the Republic of Azerbaijan on Private Data along with these Regulations.

### **2. Definitions**

2.1. The definitions used for the purposes of these Regulations bear the following meanings:

2.1.1. assets – main (business processes and information) and supporting (network and technical infrastructure, software, staff, premises, organizational structure) assets valuable for banks;

2.1.2. asset holder – a bank employee responsible for effective management and protection of the asset throughout its life;

2.1.3. audit – a systematic, independent and documented process for obtaining audit evidence and objectively assessing it to determine the level of compliance with audit criteria;

2.1.4. authentication – the procedure that allows to verify the identity of the service user and reliability of the use of personalized security information;

2.1.5. brute-force attack – a method to ensure access by testing possible combinations of letters or symbols-numbers;

2.1.6. operations administrator – a bank employee who clearly knows business processes for the information system management and their manifestation in the system;

2.1.7. operating environment – real information system environment open to users;

2.1.8. personal information – any information that allows to directly or indirectly identify the person;

- 2.1.9. information – facts, opinions, news or other information created or obtained as a result of any activity, regardless of the date of creation, form of presentation and classification;
- 2.1.10. information asset – information available physically (paper, CD or other media) or electronically (stored in databases, files, PCs), valuable for and at the disposal of banks;
- 2.1.11. information accessibility – ease of obtaining and using information if required;
- 2.1.12. data confidentiality – information not accessible and not open for unauthorized access;
- 2.1.13. information process – creation, collection, handling, storage, search and dissemination of information;
- 2.1.14. information system – an organizational and technical set of information technologies (IT) and documents, including the use of computer technology;
- 2.1.15. data integrity – accuracy and completeness of information;
- 2.1.16. information security – protection of confidentiality, integrity and accessibility of information;
- 2.1.17. information security management system (hereinafter – ISMS) – a set of activities and procedures aimed at creating, implementing, supporting and continuously developing bank's information security to achieve its objectives;
- 2.1.18. information technologies (IT) – a system of methods and tools used during information processes, including application of computing and communication techniques;
- 2.1.19. information security event – occurrence of a system, service or network situation that indicates a possible breach of information security policy or management failure, or a previously unknown situation that may be related to security;
- 2.1.20. information security incident – one or more undesirable or unforeseen information security incidents likely to disrupt business processes and pose a threat to information security;
- 2.1.21. development environment – the environment where software of information systems is developed;
- 2.1.22. user – bank employees, counterparties and customers authorized to work in the information system;
- 2.1.23. cryptographic means – methods used to ensure information security with cryptographic transformation of information (hardware, application software, etc.);
- 2.1.24. critical information system – information systems, including operating, accounting and automated management systems and information-telecommunication networks, which have a high level of impact on risk assessment in accordance with the rules of risk management in banks and are used in the implementation of banking activities;
- 2.1.25. mobile device – portable electronic device for personal use (laptops, tablets, smartphones, etc.);
- 2.1.26. test environment - the environment for the information system to be tested prior to actual commissioning;
- 2.1.27. system administrator – a bank employee eligible to make changes in the bank's information system, create back-up copies of systems, and monitor system's operations and ensure business continuity and other functions of information systems based on allocation of responsibilities.

### **3. Information security management system**

3.1. The ISMS is formed in accordance with by-laws that regulate risk management in banks, these Regulations and the risk management strategy and policy of the bank approved by the Supervisory Board.

3.2. The ISMS consists of policies, procedures, relevant resources and activities jointly managed by the bank to protect information assets.

3.3. The Supervisory Board approves the information security policy developed in accordance with objectives of the bank and measures taken to achieve these goals within the framework of the risk management strategy and policy.

3.4. The information security policy covers relevant information risks and areas of control in a comprehensive and thorough manner, is prepared in a clear and understandable manner, and relevant staff is informed on the approved version.

3.5. The information security policy covers at least control goals and mechanisms defined in parts 4-15 herein and defines obligation of the bank to continuously improve ISMS.

3.6. The information security policy is reviewed at least once a year separately, and when reviewing the bank's risk management strategy and policy, and appropriate changes are made as required. Information security policy is reviewed on an extraordinary basis when changes are made to ensure continuity, adequacy and effectiveness of the ISMS.

### **4. Organization of information security**

4.1. The Supervisory Board maintains overall management of the ISMS and the following is provided to organize information security:

4.1.1. determine and coordinate information security related objectives and obligations and authorities on these objectives;

4.1.2. separate conflicting positions and areas of responsibility for unauthorized or involuntary change of bank's assets or restriction of abuse;

4.1.3. establish relations with authorities to ensure information security and formulate relevant procedures for transmission, reception and presentation of information on interaction, as well as information sharing on identified discovered security incidents;

4.1.4. conclude an information exchange agreement containing requirements for protection of confidential information in connection with banks membership in non-profit associations, as well as ensure information security when establishing relevant relations with card organizations;

4.1.5. take into account the requirements for ensuring and monitoring information security in project management for all projects, regardless of the type of project.

4.2. The following measures are taken to ensure security when working remotely and using mobile devices:

4.2.1. a policy to manage risks and information security incidents that may occur during the use of mobile devices should be developed and implemented;

4.2.2. the mobile device policy should take into account the risks associated with the use of mobile devices in unprotected environments and take into account the following:

4.2.2.1. registration of mobile devices;

4.2.2.2. requirements on physical security of mobile devices;

- 4.2.2.3. restrictions related to software downloads;
- 4.2.2.4. requirements on software versions of mobile devices, including patches;
- 4.2.2.5. restrictions related to joining information services;
- 4.2.2.6. access controls;
- 4.2.2.7. cryptographic means;
- 4.2.2.8. malware protection;
- 4.2.2.9. backup copies;
- 4.2.2.10. remote shutdown, deletion or blocking;
- 4.2.2.11. use of web services and web software;
- 4.2.3. if remote work is permitted, policies and supportive security measures should be put in place to ensure secure data handling, and the following should be determined:
  - 4.2.3.1. physical security requirements;
  - 4.2.3.2. security requirements for home network and wireless networks;
  - 4.2.3.3. policies and procedures for applications created on personal mobile devices to prevent disputes over intellectual property rights;
  - 4.2.3.4. requirements on malware protection.

## **5. Human resources security**

5.1. To ensure that employees and counterparties comply with their information security responsibilities prior to starting operations the bank takes the following measures:

5.1.1. suitability of applicants for employment in accordance with business requirements, classification of accessed information and projected risks should be identified;

5.1.2. agreements concluded with the staff and counterparties should determine their information security related obligations.

5.2. To ensure that employees, counterparties, as well as customers are aware of and fulfill their obligations related to information security the Bank should:

5.2.1. request all employees and counterparties to apply information security in accordance with the policies and procedures determined by the bank;

5.2.2. involve all employees and, where appropriate, counterparties, in bank's policies and procedures related to their functions, relevant information trainings related to their innovations, and set requirements such as their completion of a relevant training program and confirmation of mastery of the program;

5.2.3. educate all employees and counterparties, as well as customers on information security requirements at least twice a year;

5.2.4. bank's information security training programs on its organizational structure (including the Management Board) should be approved and controlled in terms of their implementation by the Supervisory Board;

5.2.5. the bank should have internal disciplinary rules for taking measures prescribed by law in relation to employees who have violated information security.

5.3. To protect interests of the bank in case of termination or change of labor and counterparty relations, information security obligations and responsibilities after termination or change of labor relations with employees and counterparties should be defined and communicated to them.

## **6. Asset management**

6.1. The following measures are taken in banks to determine assets and relevant obligations related to their protection in banks:

6.1.1. information, as well as assets related to the means of data handling should be identified, inventoried and updated;

6.1.2. owners of assets responsible for their proper management over the entire life of the inventory should be identified;

6.1.3. rules of acceptable use of information, as well as other information-related assets and means of data handling should be established, documented and applied;

6.1.4. Upon expiry of employment and service agreements, employees and counterparties should return all assets in use to the bank.

6.2. The following measures are taken to ensure the necessary level of protection in terms of importance of the information for the bank:

6.2.1. Information should be classified into at least the following classes in terms of legal requirements, value, significance and sensitivity to unauthorized disclosure or change:

6.2.1.1. open - information that can be disclosed to the public;

6.2.1.2. secret – information that constitutes state secret;

6.2.1.3. confidential – commercial, banking secrecy, confidential private information and other information considered confidential under the legislation of the Republic of Azerbaijan;

6.2.2. the bank should develop and apply appropriate procedures for marking information in accordance with the classification of accepted information;

6.2.3. information carriers should be marked by identifying them as ‘Secret information’, ‘Confidential information’ and other labels, depending on the class of information;

6.2.4. The requirements for labeling information carriers are as follows:

6.2.4.1. It should be clearly visible and distinct;

6.2.4.2. It should not be easily erased (torn off) to prevent the label from decomposing;

6.2.4.3. if the format allows marking, files should be marked by inserting a clear and distinctive mark when opening the file;

6.2.5. The bank should develop and apply asset management related procedures in accordance with the classification of received information.

6.3. The following measures are taken to prevent unauthorized disclosure, change, destruction or damage of the information stored in data carriers:

6.3.1. The bank should determine and apply procedures related to removable data carriers in accordance with the classification of the information received;

6.3.2. data carriers should be destroyed in accordance with the procedures established by the bank in case of no need for use;

6.3.3. relevant measures should be taken to prevent unauthorized intrusion during transportation of data carriers.

## **7. Access control**

7.1. The following measures are taken to restrict access to information and data

handling media:

7.1.1. The access control policy should be shaped, documented and updated in light of business and information security requirements;

7.1.2. Users should have access to network and network services they are privately authorized to use.

7.2. To allow authorized user access to information systems the following measures are taken:

7.2.1. the user registration and deregistration process should be formalized and enforced to ensure that access rights are determined;

7.2.2. processes for assigning or revoking access rights to all systems and services should be determined, formalized and applied in accordance with the user authority;

7.2.3. allocation and use of preferential access rights should be restricted and managed;

7.2.4. The process of transferring confidential authentication information (password, multi-factor identification information, electronic signature, biometric information, etc.) should be defined, formalized and applied.

7.2.5. Asset holders should constantly review users' access rights;

7.2.6. Where labor agreements with employees and counterparty agreements are terminated or changed, their access rights to information and data handling media should be immediately revoked or adjusted to the change.

7.3. To make users responsible to protect their confidential authentication information they should be required to follow the rules established by the bank and controlled.

7.4. The following measures are taken to prevent unauthorized access to the information system and application software:

7.4.1. access to information systems and application software should be restricted in accordance with the access control policy;

7.4.2. access to the information system and application software should be managed with at least the following secure access procedure under the access control policy:

7.4.2.1. brute-force attack prevention methods should be applied;

7.4.2.2. unsuccessful and successful attempts should be logged;

7.4.2.3. after the successful access is completed, the following information should be displayed:

7.4.2.3.1. the date and hour of the previous successful attempt;

7.4.2.3.2. details of failed attempts after the last successful attempt.

7.4.2.4. inserted passwords should not be displayed;

7.4.2.5. passwords should not be transmitted over the network as a plain text;

7.4.2.6. in case of no activity over the specified timeframe all relations with the system should be completed;

7.4.3. complexity of passwords in the password management system should be ensured as follows:

7.4.3.1. minimum length of user passwords should be 8 (eight) characters;

7.4.3.2. minimum length of preferential user passwords should be 12 (twelve) characters;

7.4.3.3. the password should be a combination of at least three of the following:

7.4.3.3.1. at least one lowercase letter (a-z);

- 7.4.3.3.2. at least one capital letter (A-Z);
- 7.4.3.3.3. at least one number (0-9);
- 7.4.3.3.4. at least one special symbol (e.g., @ # \$% ^ & \* () \_ + | ~ - = \ `} []:;'<> /).
- 7.4.3.4. user identifiers may not be used in passwords;
- 7.4.3.5. more than two identical characters in a row may not be used in passwords;
- 7.4.3.6. during the first login or after the password is updated by the system administrator, the information system should request the user to update the password and not allow the request to be denied;
- 7.4.3.7. access to the system should be restricted after a maximum of 6 (six) attempts to type the password incorrectly;
- 7.4.3.8. passwords should be valid for a maximum of 90 (ninety) days. The user should be notified on password expiry;
- 7.4.3.9. reuse of last 12 (twelve) passwords used in the system should be prevented;
- 7.4.3.10. passwords for standard (by default) user accounts should be changed at least once a year;
- 7.4.3.11. user passwords should not be open for system administrators;
- 7.4.3.12. All user accounts not used for more than 90 (ninety) days should be blocked;
- 7.4.4. access to system and application software source codes should be restricted.

## 8. Cryptography

8.1. The following measures are taken to ensure correct selection and effective use of cryptography to protect confidentiality, authenticity and / or integrity of information:

8.1.1. A policy on the use of cryptographic means for protection of information should be formulated and implemented. The policy should cover at least the following requirements:

8.1.1.1. information to be secured by cryptographic means should be identified;

8.1.1.2. the level of complexity of cryptographic means of encryption algorithm of information should be determined based on risk assessment;

8.1.1.3. duties for the use of cryptographic means and responsibilities and authorities for these duties should be defined;

8.1.2. a policy for managing cryptographic keys should be formulated and implemented throughout the life of keys and should cover at least the following requirements:

8.1.2.1. cryptographic key generation;

8.1.2.2. cryptographic key distribution;

8.1.2.3. cryptographic key change;

8.1.2.4. cryptographic key recall;

8.1.2.5. suspension and restoration of cryptographic keys;

8.1.2.6. creating and maintaining a backup of cryptographic keys;

8.1.2.7. cryptographic key destruction;

8.1.2.8. registration of logs on cryptographic key management.

## 9. Physical security and security on the perimeter

9.1. The following measures are taken to prevent unauthorized physical access, damage and exposure to information and information processing facilities:

9.1.1. security perimeters should be set and used to ensure protection of information and information processing facilities in the bank;

9.1.2. appropriate procedures to work on security perimeters should be established and applied;

9.1.3. security perimeters should be protected by an appropriate access control (card reader, biometric data reader and (or) PIN pad) to ensure only access by authorized persons;

9.1.4. a list of authorized persons with access to security perimeters should be compiled and updated;

9.1.5. security perimeters should be equipped with motion detectors;

9.1.6. access points (loading and unloading areas) and other similar points where unauthorized persons may enter should be monitored and isolated from information processing facilities to prevent unauthorized access.

9.2. To prevent loss, damage, illegal seizure or deterioration of assets and disruption of bank's activities, the following measures are taken:

9.2.1. equipment should be located and protected in designated areas to reduce the risk of unauthorized access, environmental threats and disasters;

9.2.2. physical protection of workplaces, rooms and equipment should be maintained to prevent natural disasters, unauthorized intrusion and accidents;

9.2.3. the information processing center (server room) should also be equipped with:

9.2.3.1. 7/24 video surveillance; video surveillance footage should be stored for at least 6 (six) months;

9.2.3.2. ventilation (air conditioning) equipment and a thermometer to regulate the temperature;

9.2.3.3. security and fire alarm systems;

9.2.3.4. automated fire extinguishing systems;

9.2.3.5. humidity measuring devices and regulating equipment;

9.2.3.6. the floor should be covered with antistatic coating;

9.2.3.7. power supply and generator providing uninterruptible power supply;

9.2.3.8. The continuity of power and telecommunication lines should be ensured, as well as the following should be taken into account to protect them from external intrusion and damage:

9.2.3.8.1. power and telecommunication lines should be routed via different channels;

9.2.3.8.2. joints of power and telecommunication lines should be protected and access to the rooms controlled.

9.2.4. equipment should be protected from breaks due to power outages and failures in supporting facilities (uninterruptible power supplies, power supply, ventilation, etc.);

9.2.5. equipment should be adequately maintained to ensure their reliable and uninterrupted operation;

9.2.6. equipment, information or application software should not be taken beyond the bank without coordination;

9.2.7. risks associated with external use of assets should be considered and appropriate security measures taken;

9.2.8. confidential information stored and licensed software should be deleted without recovery prior to destruction or reuse. Physical destruction of equipment should be formalized, as well as documented upon being destroyed with special tools and technologies;

9.2.9. users should ensure that their equipment is adequately secured while they are left unattended. All users should be informed on the requirements and procedures, as well as their obligations to ensure safety of unattended equipment, as well as the bank should conduct awareness-raising activities at least twice a year. The following should be communicated to users:

9.2.9.1. all active sessions should be stopped when the activity ends;

9.2.9.2. password access blocking or automatic screen saver function should be activated;

9.2.9.3. application software or network services should be shut down when not needed;

9.2.10. A clean desk policy for paper documents and information carriers, including a clean screen policy for information processing facilities, should be adopted and at least the following should be considered:

9.2.10.1. critical information and information processing facilities should be stored in a protected area;

9.2.10.2. when use of computer equipment ends, access with appropriate password, token and other user authentication mechanisms should be blocked;

9.2.10.3. critical information should be cleaned up immediately from printers, copiers and other similar equipment and protected.

## **10. Safety of operation**

10.1. The following measures are taken to ensure proper and safe operation of information processing facilities:

10.1.1. operation procedures should be documented and be available for related staff.

The operation procedures should consist of at least the following:

10.1.1.1. downloading and installation of application software;

10.1.1.2. creation of back-up copies;

10.1.1.3. interaction facilities with other application software;

10.1.1.4. error management;

10.1.1.5. communication plans with coordinators on application software support;

10.1.1.6. application software recovery in emergencies;

10.1.1.7. registration of audit trails and logs;

10.1.1.8. monitoring procedures;

10.1.2. Change management procedures should be developed and implemented. Records containing all relevant information should be stored during the change management process. All changes affecting information security in the bank, business processes, information processing tools and application software should be managed and at least the following should be taken into account:

10.1.2.1. identification and registration of considerable changes;

10.1.2.2. change planning and testing;

10.1.2.3. risk-based assessment of potential impact of changes, including impact on information security;

10.1.2.4. verification of compliance with information security requirements;

10.1.2.5. conveying details of changes to all related persons;

10.1.2.6. establishing procedures and responsibilities for canceling or reversing failed changes or contingencies when applying changes;

10.1.2.7. establishing processes on urgent changes necessary for incident solving;

10.1.3. use of resources should be monitored, regulated and forecasted in light of potential operational needs. The resource management should at least ensure:

10.1.3.1. deletion of outdated information;

10.1.3.2. shutdown of useless application-software and database management systems;

10.1.3.3. optimization of application logic and queries to database management systems;

10.1.4. separation of development, testing and operational environments to minimize the risks associated with unauthorized access and changes to the operating environment.

10.2. The following measures are taken to ensure protection of information and information processing facilities from malware:

10.2.1. to protect against malware, control measures on detection, prevention and recovery should be carried out in conjunction with the relevant user notification;

10.2.2. the bank should ensure only application of licensed malware protection;

10.2.3. malware protection tools should be applied to all information processing facilities;

10.2.4. malware protection tools should be managed in a centralized manner;

10.2.5. installation, adjustment, testing, support and monitoring of malware protection should be carried out by authorized persons;

10.2.6. malware protection databases should be automatically updated;

10.2.7. malware protection tools should be adjusted to automatically remove all detected malware;

10.2.8. if not possible to remove malware, the information processing tool should be disconnected from network;

10.2.9. malware protection devices should provide at least the following checks:

10.2.9.1. pre-use verification of information received via network or any memory device;

10.2.9.2. pre-use check of attachments with e-mails;

10.2.9.3. website checks;

10.2.10. all malware infections should be recorded, as well as reported, indicating their types and sources of infection.

10.3. a list of application-software allowed to be used in banks should be formed and installed only by authorized persons.

10.4. Use of all external storage devices in banks should be prohibited, a list compiled if necessary, and the operation managed by authorized persons. Confidential information should be stored in external storage devices only as encrypted.

10.5. To prevent information loss, procedures are developed and implemented to create backup copies of critical information systems, as well as test the recovery process, covering at least the following requirements:

10.5.1. duties and responsibilities and powers on these duties should be defined to create and restore backups;

10.5.2. back-up copy creation means should be managed in a centralized manner;

10.5.3. back-up copies of confidential information should be stored as encrypted;

10.5.4. daily, weekly, monthly and annual back-up copies should be created;

10.5.5. backups should be tested for recovery at least once a year and results

documented;

10.5.6. logs for backups should be registered, maintained and regularly reviewed;

10.5.7. To protect against natural disasters, malicious intrusion and accidents, backup copies should be kept in a reserve center outside the bank.

10.6. The following measures are taken to record events in the critical information system and form evidence:

10.6.1. Information security events, errors, as well as event logs that record information on users' activities should be registered, stored and regularly reviewed. Event logs should be stored for one year. Registered logs should include:

10.6.1.1. information logs:

10.6.1.1.1. 'debug' logs – logs activated by information systems and equipment (network and security) to conduct research on all processes;

10.6.1.1.2. info logs – logs reflecting information on the normal operation of services by information systems and equipment (network and security).

10.6.1.2. critical logs:

10.6.1.2.1. warn logs – logs reflecting abnormal operation of services and possible malfunctions by information systems and equipment (network and security);

10.6.1.2.2. error logs – logs indicating downtime or failure on important elements of services by information systems and equipment (network and security);

10.6.1.2.3. critical logs – logs including critical events across information systems and equipment (network and security).

10.6.2. Every event log should include at least the following information:

10.6.2.1. user identifier;

10.6.2.2. date, time and details of major events (login, logout, etc.);

10.6.2.3. the event status and/or the error code;

10.6.2.4. successful and failed login attempts;

10.6.2.5. changes to system configurations;

10.6.2.6. logged files and login type;

10.6.2.7. network addresses and protocols;

10.6.2.8. activation and deactivation of protection systems;

10.6.2.9. operations in application-software;

10.6.3. log registration tools and log information should be protected against changes and unauthorized access;

10.6.4. logs on activities of system and operations administrators should be recorded, protected and regularly reviewed in registration journals;

10.6.5. in light of the importance of logs, information systems and information processing tools should be synchronized with a single time source.

10.7. The following measures are taken to identify technical vulnerabilities in the critical information system and prevent their abuse:

10.7.1. duties and responsibilities and powers on these duties should be determined for monitoring of technical vulnerabilities, assessment of risks on vulnerabilities and patch management;

10.7.2. intrusion tests should be conducted at least once a year to analyze and eliminate technical vulnerabilities in each critical information system and results should be formalized;

10.7.3. the critical information system should be transferred to the operating

environment after intrusion tests to analyze and eliminate technical vulnerabilities;

10.7.4. upon detection of technical vulnerabilities related risks and measures to be taken should be identified.

10.8. Audit requirements and activities are carefully planned and agreed with the asset owner to minimize negative impact on bank's business processes during the audit of information systems.

## **11. Information exchange security**

11.1. Networks are managed and monitored to protect the information in networks and supporting information processing tools. To protect information in networks and supporting information processing tools, at least the following should be considered:

11.1.1. rules governing network infrastructure management responsibilities and procedures should be developed and enforced;

11.1.2. adequate control mechanisms should be applied to protect confidentiality and integrity of information transmitted in wireless and global networks with access to application software;

11.1.3. the actions likely to affect information security should be recorded and appropriate logging and monitoring should be applied to ensure detection;

11.1.4. security mechanisms, service levels and management requirements across all network services should be defined and included in network service agreements, whether they are provided internally or externally;

11.1.5. to ensure information security in the network, at least users and information systems should be segmented.

11.2. The following measures are taken to ensure the security of information transmission inside and outside the bank:

11.2.1. exchange policies, procedures and control mechanisms should be developed and applied to ensure security during transmission of information by any means of communication;

11.2.2. requirements for protection of confidentiality and non-disclosure of information should be stipulated in agreements concluded between parties;

11.2.3. information used in electronic correspondence should be protected from unauthorized intrusions.

## **12. Acquisition, application and support of information systems**

12.1. To ensure that information security is an integral part of the critical information system over its entire period of use, the following measures are taken:

12.1.1. information security requirements should be taken into account when introducing new or improving existing information systems;

12.1.2. information transmitted over open networks via application programming interfaces should be protected from external intrusion, unauthorized disclosure and changes;

12.1.3. information security should be ensured to prevent incomplete transmission, incorrect addressing, unauthorized disclosure, change, copying and duplication of information exchanged via application programming interfaces;

12.1.4. appropriate management procedures should be developed and approved to manage changes in information systems;

12.1.5. changes in information systems should be assessed on a risk basis, application prioritized, a reversal strategy should be developed and tested before commissioning;

12.1.6. principles for application of protected information systems should be defined, documented and used in the application of information systems;

12.1.7. security of all environments (development, testing and operation) should be ensured during the creation of information systems;

12.1.8. when information systems application services are obtained from a counterparty, security requirements should be established by the agreement signed between the parties;

12.1.9. when information systems are applied, the information security mechanisms of the systems should be tested and their safe operation ensured;

12.1.10. when new information systems, updates and new versions are applied, acceptance tests for compliance with information security requirements should be carried out, documented, agreed and acceptance of the systems ensured according to them;

12.1.11. confidential information should not be used during tests, safety of the test environment should be taken into account and logging of operations should be ensured.

### **13. Relations with counterparties**

13.1. Information security is ensured in relation to counterparties and the following measures are taken:

13.1.1. to minimize risks in relation to counterparties who have access to bank's assets, information security requirements should be taken into account, agreed with counterparties and documented;

13.1.2. all relevant information security requirements should be formulated and agreed with for each counterparty that has access to, processes, stores, transmits bank information or provides information technology infrastructure components;

13.1.3. agreements with counterparties should include relevant requirements to minimize information security risks.

13.2. To ensure the agreed level of information security and adequate services within the service agreements concluded with counterparties, the following is taken into account:

13.2.1. the bank should regularly monitor and audit the services provided by counterparties;

13.2.2. changes in services provided by counterparties should be made in accordance with existing information security policies, procedures and control mechanisms, taking into account the criticality of information, information systems and processes, and risk assessed;

13.2.3. banks should take appropriate measures to limit access of counterparties to such information to maintain confidentiality, integrity and accessibility of the information they hold when outsourcing information security services, and to minimize the impact on the continuity of banking activities.

### **14. Information security incident management**

14.1. The following measures are taken to ensure ongoing and effective management of

information security incidents, including communication of security incidents and vulnerabilities:

14.1.1. continuous monitoring, policies and procedures should be in place to identify actions and unauthorized intrusion likely to affect information security;

14.1.2. a clear division of powers and necessary communication channels should be established to ensure an adequate response to information security incidents;

14.1.3. notification on information security incidents should be provided as soon as possible through appropriate management channels;

14.1.4. employees and counterparties using information systems should be required to register and report vulnerabilities identified or suspected in relevant information systems;

14.1.5. an information security event should be assessed and a decision made on whether it is an information security incident;

14.1.6. Measures related to information security incidents should be carried out in accordance with relevant procedures. The following requirements should be considered when designing these procedures:

14.1.6.1. evidence should be collected from the moment the incident occurs;

14.1.6.2. the incident should be registered and communicated;

14.1.6.3. the incident should be assessed on a risk basis and prioritized;

14.1.6.4. the incidents should be categorized at least as follows to be prioritized:

14.1.6.4.1. low – as a result the bank continues to operate inefficiently on one business process;

14.1.6.4.2. medium – as a result the bank fails to operate on several business processes;

14.1.6.4.3. high – as a result the bank fails to carry out any business activities.

14.1.6.5. a list of measures to be taken to eliminate the incident should be compiled and its implementation should be monitored;

14.1.6.6. once the incident is eliminated, it should be closed and reported;

14.1.6.7. incident notification means (e-mail, special information system, phone calls, etc.) should be assigned, registered and formalized.

14.2. Information on high category incidents on information security should be submitted to the Central Bank via a special information exchange system within 5 (five) working days, confirmed by the Chairman of the Management Board of the bank with a strengthened electronic signature as per Annex 1 herein.

14.3. Experience gained from the analysis and resolution of incidents should be used to reduce the likelihood and impact of future incidents.

## **15. Information security in business continuity management**

15.1. Every bank should ensure continuity of information security in the event of damage to, destruction of or threat to information systems and information technologies.

15.2. The bank takes the following measures to ensure continuity of information security of critical information infrastructure:

15.2.1. processes, procedures and management methods should be defined, documented, applied and updated to ensure the required level of continuity of information security in emergencies;

15.2.2. there should be a back-up center beyond the bank's location with an adequate

operation to maintain backups and restore operations of information systems;

15.2.3. a business continuity plan in emergencies and a recovery plan for information systems should be developed and approved. The business continuity plan should identify communication measures in emergencies, conduct business impact analysis, and identify procedures for resuming bank operations, transitioning to a backup center, and subsequent recovery;

15.2.4. to check reliability and continuity of information systems in emergencies, the operation of information systems should be carried out over the backup center at least twice a year and the results should be documented;

15.2.5. to ensure continuity of information security in emergencies, trainings should be conducted at least twice a year for relevant bank staff on the procedures to be followed in the event of accidents in information systems, information technologies and communication equipment, and the results should be formalized.

### Information on high category incidents

№	Nature of the information security incident	Information security incident
	<b>General information</b>	
1	Incident name	
2	Incident description	
3	When occurred (d.m.y ss:dd:ss)	
4	When detected (d.m.y ss:dd:ss)	
5	Where detected (bank, branch/division, information system)	
6	Source of incident information (user and/or related administrator)	
7	Methods used in occurrence of the incident (social engineering, malware application etc.)	
<b>Content</b>		
8	Incident: <ul style="list-style-type: none"> <li>- exploitation of vulnerabilities in the information system;</li> <li>- unauthorized access to the information system;</li> <li>- service rejection (DoS, DDoS);</li> <li>- creation and spread of malware;</li> <li>- unauthorized transfer of funds;</li> <li>- other information security incidents threatening business continuity in the bank.</li> </ul>	
9	Exposed assets: <ul style="list-style-type: none"> <li>- technical infrastructure of the information system (server, network, security equipment, etc.);</li> <li>- application software, services and operating systems;</li> <li>- bank's business processes.</li> </ul>	
10	Damage (in manat)	
11	Information source on the incident	
<b>Actions taken</b>		
12	Actions taken (identification, blocking, recovery of the vulnerability etc.)	
13	Action(s) to be taken	
14	Start and end time of action(s) (gg.aa.iiii ss:dd:ss)	

15	Responsible person(s) (last, 1st, middle names, position)	
16	Notified person(s) (last, 1st, middle names, position)	
17	Attracted specialist(s) (last, 1st, middle names, position)	

Signature: \_\_\_\_\_

Date: \_\_\_\_\_