'Approved'
Central Bank of
the Republic of Azerbaijan
Decision № 14/2
28 March 2024

Information security requirements for supervised entities in financial markets

1. General provisions

1.1. These Requirements have been developed in accordance with Article 48.3.4 of the Law of the Republic of Azerbaijan 'on the Central Bank of the Republic of Azerbaijan', as well as Article 34-1.4 of the Law of the Republic of Azerbaijan 'on Compulsory Insurance' and determine minimum information security requirements for banks, non-bank credit institutions, except for credit unions, insurers, securities market licensees, joint-stock investment funds and investment fund managers, the national postal operator, payment institutions, electronic money institutions, payment system operators, credit bureaus, and the central depository.

1.2. These Requirements also apply to the compulsory insurance information system and related assets of the Compulsory Insurance Bureau.

1.3. The persons specified in Items 1.1 and 1.2 of these Requirements jointly are called supervised entities in these Requirements.

1.4. Items 4.12-4.16 and 6.5 of these Requirements do not apply to Category II supervised entities specified in sub-item 2.1.35 of these Requirements.

1.5. Items 4.4, 4.5, 4.12- 4.16, 6.5, 6.9, 6.10, 6.12, 7.17, 7.19, 7.21-7.23 of these Requirements do not apply to Category III supervised entities specified in sub-item 2.1.36 of these Requirements.

1.6. The requirements for the protection of personal data in supervised entities are regulated by the Law of the Republic of Azerbaijan 'on Personal Data' along with these Requirements.

2. Definitions

2.1. The definitions used in these Requirements bear the following meanings:

2.1.1. **asset** – primary (business processes and information) and supporting assets (network, hardware and software, personnel, premises, organizational structure) valuable for supervised entities.

2.1.2. **asset holder** – the person responsible for the management and protection of the asset throughout its life cycle.

2.1.3. **audit** – a systematic, independent, and documented process for obtaining and objectively evaluating audit evidence to determine the extent to which it meets audit criteria.

2.1.4. **authentication** – a supervisory measure that allows to verify the identity of the service user and the validity of the use of personalized security information.

2.1.5. **defense in depth** – multiple layers of security controls for protection of assets.

2.1.6. **emulator** – software that simulates an operating system and runs programs running in that operating system.

2.1.7. **labeling** – labeling of information and related assets in various ways (e.g., physical label, header and footer, metadata, watermark, stamp) according to the information classification.

2.1.8. **operating environment** – real information system environment open to users.

2.1.9. **sensitive information** – information that must be protected from unauthorized processing, including access, alteration, or disclosure due to its potential negative effects on individuals and legal entities, as well as national security (e.g., sensitive payment data, personal information, state secrets, commercial secrets, banking secrecy, insurance secret and other confidential information).

2.1.10. **information** – facts, opinions, news, or other information created or obtained as consequence of any activity, regardless of the date of creation, form of presentation and classification.

2.1.11. **information accessibility** – ease of obtaining and using information if required.

2.1.12. **data confidentiality** – non-accessibility and non-openness of information 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 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 supervised entity's information security to achieve its objectives.

2.1.18. **information technologies** – programs, systems or equipment used for automated execution of information processes.

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** – personnel and customers authorized to access 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 that execute information processes involving sensitive information, are used during the implementation of core activities of supervised entities and/or have a high level of impact based on risk assessment in supervised entities.

2.1.25. **mobile device** – portable electronic device for personal use (laptops, tablets, smartphones, etc.).

2.1.26. **personnel** – specialists operating in the supervised entity, including individuals and interns working under labor and other agreements.

2.1.27. **personalization** – uploading information about the payment card user to the electronic carrier (chip) and/or magnetic tape during the preparation of payment cards and printing identification information on the payment card.

2.1.28. **zero trust** – a security model that initially includes the requirement that all users, devices, and networks be untrusted and verified before access is granted.

2.1.29. **test environment** – the environment for the information system to be tested prior to actual commissioning.

2.1.30. **system administrator** – a supervised entity employee eligible to make changes to the 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.

2.1.31. **end user device** – ICT equipment connected to network (e.g., PCs, mobile devices, Internet of things etc.).

2.1.32. **provider** – a person who provides goods (works, services) to the supervised entity on a contractual basis.

2.1.33. **senior management body** – internal control body of the supervised entity (supervisory board (board of directors), board of trustees or other authorized management body).

2.1.34**. Category I supervised entities** – banks, insurers, the central depository, the Compulsory Insurance Bureau, credit bureaus, electronic money institutions and payment system operators.

2.1.35. **Category II supervised entities** – securities market licensees, the national postal operator, payment institutions, joint-stock investment funds and investment fund managers

2.1.36. **Category III supervised entities** – non-bank credit institutions except for credit unions.

3. The information security management system

3.1. The ISMS is established as an integral part of business processes and overall management system of the supervised entity operating under the general guidance of the senior management body, taking into consideration these Requirements and the requirements of other regulations of the Central Bank of the Republic of Azerbaijan (hereinafter – the Central Bank), to ensure and continually enhance its activities.

3.2. An information security policy aligned with the supervised entity's overarching strategy for ISMS formation is drafted and approved by the senior management body.

3.3. A person responsible for information security is designated by the supervised entity to directly monitor the ISMS. The information security officer:

3.3.1. develops and submits to the management the information security policy, related rules.

3.3.2. organizes the ISMS and issues proposals for its improvement.

3.3.3. coordinates activities of supervised entity's structural units on the ISMS.

3.3.4. submits a report to the management on the information security situation and information security risks in the supervised entity quarterly.

3.3.5. promptly notifies management, providing reasons for the deviation when deviations from information security requirements occur.

3.3.6. organizes the dissemination of information to personnel, including employees of the structural units involved in ensuring information security, engaging them in training sessions, and educating customers.

3.4. The information security policy is prepared in a clear and comprehensible format, addressing relevant information risks and control areas in a comprehensive and reasonable manner, approved, and communicated to the staff.

3.5. The information security policy covers at least the measures defined in parts 4-7 of these Requirements and defines the commitment to continuous improvement of ISMS.

3.6. The information security policy is reviewed at least once a year separately, as well as when reviewing the supervised entity's risk management system, and relevant changes are made if required. The information security policy is reviewed on an extraordinary basis when changes are made to ensure the continuity, adequacy, and effectiveness of the ISMS.

3.7. To evaluate compliance with these requirements, the ISMS of the supervised entity is examined by an external auditor internationally accredited in information security verification with a minimum of three years of experience in information security verification within financial markets under the following periodicity:

3.7.1. Category I supervised entities – not less than once a year.

3.7.2. Category II and III supervised entities – not less than once in 2 (two) years.

3.8. Payment system operators and banks involved in the collection, processing, and transmission of payment card transaction information, as well as providing technical services for card issuance and acquisition are subject to additional examination by an internationally accredited external auditor in compliance with information security standards at least once a year.

4. Organizational control measures

4.1. An independent structural unit responsible for information security is established within the supervised entity, duties, and responsibilities of this unit, along with those of other personnel involved in information security, are clearly defined, as are their respective authorities. To avoid conflicts of interest, the unit responsible for information security is established separately from the unit responsible for information technologies and is overseen by different curators.

4.2. To prevent unauthorized or inadvertent modification or misuse of information and related assets, the supervised entity ensures the separation of conflicting duties and responsibilities.

4.3. The supervised entity establishes appropriate procedures regarding the initiation of mutual relations with the Central Bank, as well as with authorized public authorities (institutions) and timely exchange of information on mutual activities, and information security incidents to safeguard information security.

4.4. The supervised entity collects and analyzes relevant information to timely identify information security threats.

4.5. Regardless of the type of project, information security is ensured and continuously monitored by the supervised entity at all stages of project management.

4.6. The supervised entity implements the following measures to safeguard information and other related assets:

4.6.1. information and other related assets are identified and inventoried to ensure relevance.

4.6.2. asset holders responsible for their proper management during the entire useful life of the inventoried assets are designated.

4.6.3. rules for acceptable use of information and other related assets are defined and documented with approval.

4.6.4. asset protection is ensured when labor and service agreements change, when they expire, and relevant assets used by personnel are returned to the supervised entity.

4.6.5. information is classified considering its integrity, confidentiality, accessibility, value, importance, sensitivity to unauthorized disclosure or change, requirements of interested parties, as well as requirements of the legislation.

4.6.6. rules for labeling information and related assets according to the adopted information classification are defined and documented with approval.

4.6.7. for all types of internal and external information transmission methods, information transmission requirements are determined considering the following, as well as those requirements are considered in relevant regulations and agreements:

4.6.7.1. control measures for cases involving interception, unauthorized access, copying, modification, misdirection, destruction of transmitted information, including cryptographic methods tailored to protect sensitive information in alignment with the classification of transmitted information.

4.6.7.2. control measures to ensure the traceability and non-repudiation of information while maintaining its reliability during transmission.

4.6.7.3. ensure reliability and availability of information transmission facilities.

4.6.7.4. define procedures for storage, processing, use, archiving and deletion of information.

4.6.7.5. use a labeling system agreed with the counterparty to ensure appropriate protection of information.

4.7. Rules on access to information and other related assets are developed and approved, based on business and information security requirements, considering at least:

4.7.1. registration and regular monitoring of access rights to information and other related assets throughout their life cycle.

4.7.2. classification of accounts with access rights as user, privileged and service accounts and ensuring their relevance.

4.7.3. blocking of login accounts not used during the period established by the supervised entity, as well as those that have lost their relevance.

4.7.4. providing access rights to relevant information and other related assets only to the extent necessary for the performance of assigned duties.

4.7.5. in the event of termination or change of contractual relationships with personnel and suppliers, immediately cancel or adjust their access rights to information and other related assets accordingly.

4.7.6. restrict access rights to system and software source codes.

4.8. Rules for the management of authentication data in the supervised entity are developed and approved, considering at least the following requirements:

4.8.1. change pre-defined (by default) authentication information immediately after installation of systems or software.

4.8.2. passwords defined as authentication information should at least meet the following requirements:

4.8.2.1. passwords should not contain information easily guessed by third parties or related to the password holder (e.g., names, phone numbers and dates of birth, etc.).

4.8.2.2. require the personnel to update the password in the information system during the first login to the system or after the password has been updated by the system administrator and not to allow the request to be rejected.

4.8.2.3. determine minimum length, alphanumeric and special character requirements when setting a password.

4.8.2.4. set a password validity period.

4.8.2.5. restrict reuse of previously used passwords.

4.8.3. require and monitor the staff to comply with the rules set by the supervised entity to hold them accountable for protecting their authentication information.

4.9. In relations with providers, information security requirements defined by these regulations are met, including the implementation of the specified measures below.

4.9.1. agree and document information security requirements between the parties to minimize risks in relation to providers with the right to access supervised entity’s assets.

4.9.2. develop a register of providers and regularly monitor the services by providers by the supervised entity.

4.9.3. make changes in the services provided by providers in accordance with existing policies and regulations on information security, considering the criticality of information, information systems and processes, and perform risk assessment.

4.9.4. designate the information security liaison(s) in agreements with providers with access to supervised entity's assets.

4.9.5. when the supervised entity outsources services, limit access to sensitive information and establish appropriate professional requirements for the provider's direct service personnel based on the risk assessment conducted in relation to the providers providing such services and the services provided by them, as well as the requirements of the legislation.

4.10. The following measures are taken by the supervised entity regarding the acquisition, use, management, and access to the ‘Cloud’ services:

4.10.1. rules are developed and approved considering at least the following:

4.10.1.1. information security requirements on the use of ‘cloud’ services.

4.10.1.2. ‘cloud’ service selection criteria (ISO/IEC, PCI DSS, Uptime Tier and/or compliance with other international standards) and the coverage of the cloud service use.

4.10.1.3. duties and responsibilities on the ‘cloud’ service use and management.

4.10.1.4. measures of control applied by the 'cloud' service provider and the supervised entity separately.

4.10.1.5. measures of information security incident management regarding the use of 'cloud' services.

4.10.1.6. measures regarding the monitoring and assessment of 'cloud' services used for information security risk management.

4.10.1.7. measures regarding business continuity in emergencies during the use of 'cloud' services.

4.10.1.8. the procedure for refusing cloud services or changing (stopping) the service, including the exit strategy.

4.10.2. cloud service agreements should meet the requirements of the information security policy of the supervised entity. To protect the availability of the information and services owned by the supervised entity, the following conditions should be met in cloud service agreements:

4.10.2.1. cloud service solutions rest upon the relevant international architecture and infrastructure standards.

4.10.2.2. cloud service access control mechanisms are compliant with supervised entity's requirements.

4.10.2.3. introduction of malware protection and monitoring solutions.

4.10.2.4. processing of supervised entity-owned sensitive information should adhere to the requirement outlined in sub-item 4.10.2.5 of these Requirements by ensuring full encryption of data transmission channels (end-to-end encryption).

4.10.2.5. supervised entity-owned sensitive information should be stored solely within the Republic of Azerbaijan.

4.10.2.6. ensuring that the information belonging to the supervised entity is not utilized by the 'cloud' service provider for other purposes and maintaining its segregation from the data of other organizations utilizing the service.

4.10.2.7. provision of appropriate support by the cloud service provider in the event of an information security incident within the cloud service.

4.10.2.8. prohibition of subcontracting of cloud services by a cloud service provider through a third party.

4.10.2.9. provide support to the supervised entity in collecting digital evidence.

4.10.2.10. provide appropriate support and availability of services within the time frame agreed between the parties in case the supervised entity refuses the cloud service.

4.10.2.11. creation and ensuring security of backup copies of the information required by the supervised entity by the cloud service provider.

4.10.2.12. provision of configuration files, backup copies, source code and other sensitive information belonging to the supervised entity during the provision of or refusal to use the service, return and irrevocable deletion of information from the cloud service provider.

4.10.2.13. notifying the supervised entity in advance about the changes implemented by the cloud service provider (e.g., making changes to information systems and infrastructure components, processing or storing information in another country or region, using the services of other cloud service providers within the framework of a subcontract).

4.10.2.14. business continuity measures applied by the cloud service provider in emergencies are in compliance with the business continuity rules of the supervised entity

4.11. For flexible, continuous, and effective management of information security incidents, including the communication of information security events, the supervised entity develops and approves information security incident management rules, considering at least the following:

4.11.1. define information security incident management processes, relevant roles, and responsibilities, contact person(s) and necessary communication channels.

4.11.2. assess information security events and decide on whether the event is an information security incident.

4.11.3. In response to information security incidents, covering all assets affected by the incident, obtaining necessary evidence, communicating according to the needs of stakeholders, and applying documented procedures based on root-cause analysis.

4.11.4. immediate notification of information security events and incidents through appropriate communication channels.

4.11.5. establishing a process for notifying the contact person(s) of information security incidents discovered or suspected by personnel and providers and recording the information obtained.

4.11.6. taking measures covering at least the following information security incidents:

4.11.6.1. collection of evidence from the moment of the incident.

4.11.6.2. registration and communication of the incident.

4.11.6.3. risk-based assessment of the incident, prioritization, and categorization according to at least the following criteria:

4.11.6.3.1. low – as consequence of the incident, the supervised entity continues to perform its activities on one business process ineffectively.

4.11.6.3.2. medium – as consequence of the incident, the supervised entity fails to perform its activities on some business processes.

4.11.6.3.3. high – as consequence of the incident, the supervised entity fails to perform its activities on any critical business process.

4.11.6.4. form a list of measures to be taken to eliminate the incident and monitor its implementation.

4.11.6.5. conduct incident closure and reporting once the incident has been resolved.

4.11.6.6. determine the means of notifying about incidents (e-mail, special purpose information system, phone call, etc.).

4.11.7. formulate and use a knowledge base to reduce the probability and impact of incidents in the future as consequence of incident analysis and resolution.

4.11.8. increase necessary knowledge and skills of employees involved in incident management.

4.12. In cases where information systems and information technologies in the supervised entity are damaged, malfunctioning or exposed to risks, information security and business continuity are ensured. At least the following measures are taken to ensure the continuity of the critical information system:

4.12.1. business impact analysis is conducted, business processes are classified according to their criticality level, and critical information systems and related assets are identified.

4.12.2. processes are defined, documented, applied, and updated to ensure the necessary level of information security and business continuity in the event of an emergency on an identified critical information system.

4.12.3. necessary planning is conducted by ensuring availability of staff with crucial knowledge and skills to provide an adequate response to the risks affecting business continuity.

4.12.4. for business continuity, it is ensured that the supervised entity has two information processing centers (main and backup centers) located in non-adjacent economic regions of the Republic of Azerbaijan.

4.12.5. An emergency business continuity and recovery plan(s) is/are developed and documented that includes at least the following:

4.12.5.1. classification of emergencies by the level of impact on business processes.

4.12.5.2. a list and powers of persons responsible for restoration of operations in case of emergency.

4.12.5.3. a list of critical information systems and technologies used in facilitating information sharing in emergency situations, logical and physical topological diagrams depicting the connection between them.

4.12.5.4. an acceptable time indicator of irrecoverable data loss in the information system as consequence of an emergency case.

4.12.5.5. the time required to restore the information system that serves the business process after the occurrence of an emergency case.

4.12.5.6. measures to prevent risks that may exist during emergency shutdowns under possible scenarios.

4.12.5.7. communication in emergencies.

4.12.5.8. measures to ensure business continuity in case of using the services of third-party service providers for the maintenance of information systems and (or) resources.

4.13. The supervised entity ensures reliable, safe, and continuous operation of critical information systems and related assets from a backup center to ensure business continuity in emergencies.

4.14. In case of emergencies, business continuity and recovery plans are tested at least 2 (twice) a year under different scenarios over the backup center, results are documented, and if the test result is unsuccessful, the supervised entity conducts a test check again through the backup center within the next 2 (two) months and documents the result.

4.15. The supervised entity appoints and instructs employees (main and substitute persons) responsible for responding to requests and information sharing to ensure business continuity in emergencies.

4.16. To ensure business continuity and recovery in emergency situations, trainings are held for relevant staff no less than 2 (twice) a year and results are documented.

4.17. To protect intellectual property rights, the rules of proper use are enforced according to the legislative requirements, information systems and software are operated in compliance with licensing conditions and unauthorized distribution of copies is restricted.

4.18. Measures of control covering the storage, archiving and destruction of data are determined according to the legislative requirements related to data storage, archiving, prevention of loss, destruction, as well as unauthorized modification to and the classification of information.

4.19. In case of unplanned interruptions and/or significant changes in the critical information system of the supervised entity, as well as in the event of a high-category incident, an internal or external audit is conducted on the respective system, and results are documented.

4.20. To ensure proper and secure operation of IT, operating procedures covering at least the following are documented and made available to relevant staff:

4.20.1. loading and installation of software.

4.20.2. mutual integration links with other software.

4.20.3. error management.

4.20.4. communication plans with software support liaisons.

4.20.5. software recovery in emergencies.

4.20.6. recording audit traces and logs.

4.20.7. monitoring procedures.

5. Control measures regarding human resources

5.1. To ensure that the staff and suppliers with access to assets meet their information security responsibilities before commencing operations the supervised entity:

5.1.1. adequately determines the suitability of candidates for business requirements, the classification of the information accessed and predicted risks.

5.1.2. determines their and the supervised entity's information security obligations with the concluded agreements and internal documents of the supervised entity.

5.2. To ensure that suppliers with access to the staff and assets, as well as customers, know, fulfill, and educate about their information security obligations the supervised entity:

5.2.1. requires the staff and providers to comply with information security requirements in accordance with the information security policy and relevant regulations.

5.2.2. engages the staff in training sessions on information security policy and rules relevant to their functions at least 2 (twice) a year and promptly educates them about any changes in relevant documents, as well as provides information security education at least four times a year.

5.2.3. informs suppliers about information security requirements at least 2 (twice) a year, as well as promptly in case of changes.

5.2.4. educates customers on information security at least quarterly.

5.2.5. training programs for staff on information security are approved by the head of the executive body of the supervised entity and their implementation is monitored.

5.2.6. defines liability measures in its internal rules in accordance with the legislation against the staff who violate information security requirements.

5.3. Information security obligations are defined for the period following the termination or change of contractual relations with providers with access to staff and assets.

5.4. When staff and providers are granted access to information and other related assets, agreement forms covering the following are drawn up and signed between the parties to protect information and prevent unauthorized disclosure to third parties:

5.4.1. coverage of sensitive information.

5.4.2. the validity of the agreement.

5.4.3. responsibilities of the parties for unauthorized disclosure of information.

5.4.4. ownership rights over information and other related assets.

5.4.5. monitoring the use of information and other related assets and actions to be taken in case of non-compliance.

5.4.6. procedure for returning or destroying submitted information and other associated assets.

5.5. To ensure the security of the information accessed, processed, and stored outside the location of the supervised entity during remote work of the staff, rules which include at least the following are prepared, approved, and communicated with the staff:

5.5.1. physical security requirements during remote work.

5.5.2. requirements for secure arrangement of information sharing.

5.5.3. requirements for the safe use of technologies that enable remote work.

5.5.4. requirements related to the use of home and other public Internet networks.

5.5.5. requirements for applying latest updates to the operating system and software.

5.5.6. requirements for organizing protection against malicious software.

5.6. To ensure timely internal reporting of information security incidents detected or suspected by staff, a mechanism is established that includes at least the following:

5.6.1. staff obligation to report information security incidents as soon as possible.

5.6.2. designate the contact person(s) to whom information about information security incidents is provided.

5.6.3. availability of a procedure for reporting information security events.

5.7. Considerations for reporting an information security incident include:

5.7.1. cases of violation of confidentiality, integrity, and availability of information.

5.7.2. ineffective security measures.

5.7.3. human errors.

5.7.4. cases of incompliance with the information security policy and relevant rules.

5.7.5. hardware and software malfunctions or other inconsistencies and deficiencies.

5.7.6. access violations.

5.7.7. vulnerabilities and suspected malware infections.

6. Control measures regarding physical security

6.1. To prevent unauthorized physical access, damage and intrusion to information and other related assets in the supervised entity, the protection of the places where they are stored is ensured, considering at least the following requirements:

6.1.1. security perimeters, as well as the location and resistance requirements of each perimeter, are determined in accordance with the information security requirements relevant to the covered assets.

6.1.2. appropriate procedures to work on security perimeters are established.

6.1.3. a list of authorized persons with access right is developed and updated.

6.1.4. appropriate access control mechanisms are implemented to ensure that only authorized individuals can access the security perimeters.

6.1.5. access points (loading and unloading areas) and other similar points where unauthorized persons may enter are monitored and isolated from information technologies to prevent unauthorized access if possible.

6.2. To prevent unauthorized access, damage and penetration to information and other related assets in the supervised entity, rules are prepared and approved for the protection of offices, rooms, and equipment.

6.3. To detect and prevent unauthorized physical access, areas and buildings are monitored continuously through surveillance cameras.

6.4. Risk assessment concerning natural disasters and other physical threats is conducted and protective measures are determined taking into account geographical features of the area and factors that endanger human life.

6.5. The information processing center (server room) should meet at least the following requirements in addition to the requirements of Items 6.1-6.4 of these Requirements:

6.5.1. images captured by surveillance cameras are stored within the building where they were recorded for a minimum of 6 (six) months and backup copies of these images are kept outside the building where they were recorded.

6.5.2. it should be windowless, if not possible, the window is equipped with armored glass and iron bars.

6.5.3. it should be hermetic.

6.5.4. doors should be impact and fire resistant.

6.5.5. **it should be equipped with** thermometer, ventilation, and cooling systems for temperature regulation.

6.5.6. security and fire alarm systems.

6.5.7. automated fire extinguishing systems.

6.5.8. humidity measuring devices and regulating equipment.

6.5.9. motion detectors.

6.5.10. power supply and generator providing uninterruptible power supply.

6.6. Work areas (rooms) designated for payment card personalization, storage (vault), delivery, and printing of PIN envelopes adhere to the requirements outlined in Items 6.1-6.5 of these Requirements and personalization rooms are exclusively used for personalization activities in payment systems operators and banks that provide technical services for the collection, processing, and transmission of information about payment card transactions, as well as card issuance and acquisition.

6.7. ATMs and their locations should meet the following requirements at a minimum:

6.7.1. at least one surveillance camera is installed in the ATM, enabling clear capture of the user's facial image, and recorded images are stored in the appropriate supervised entity for a minimum of 6 (six) months.

6.7.2. an easily readable and clearly visible warning notice about video surveillance by the ATM is placed where the user can see it.

6.7.3. special equipment is installed in the ATM's reader device to prevent external interference.

6.7.4. internal software should meet the requirements specified in Part 7 herein.

6.7.5. equipped with global remote positioning (GPS) and security alarm system.

6.7.6. the area in front of (or around) the ATM installed in open areas is illuminated with clear lighting during nighttime, ensuring a minimum distance of 2 (two) meters.

6.8. For paper and other information carriers, a clean desk and clean screen policy is adopted and communicated with staff, taking into account at least the following:

6.8.1. sensitive information and related IT are stored in protected areas.

6.8.2. when the use of computer equipment is completed, access to the equipment is restricted and an appropriate password, token and other user authentication method is applied for reuse.

6.9. Appropriate security measures are implemented to address potential risks associated with the use of information and other related assets outside the territory of the supervised entity.

6.10. The continuity of electricity and telecommunication lines is maintained by routing them through different channels, junctions of electrical and telecommunication lines are protected, access to the rooms housing these lines is controlled, and measures are taken to safeguard against external intrusion and damage.

6.11. Equipment is safeguarded against interruptions caused by power outages and failures of supporting facilities (uninterruptible power supplies, electricity, ventilation, etc.) by considering at least the following:

6.11.1. supporting equipment is adjusted, used, and maintained according to manufacturer's instructions.

6.11.2. supporting equipment regularly meets the needs of the supervised entity.

6.11.3. supporting equipment is tested at least 2 (two) times a year to verify proper operation and results are documented.

6.11.4. supporting equipment is placed in a separate network segment from the equipment responsible for information processing and is connected to the internet only when required.

6.12. Adequate support service is provided for the reliable and continuous operation of the equipment.

6.13. Information and other related assets are not removed from the territory of supervised entity without agreement.

6.14. Stored sensitive information and licensed software are irretrievably deleted before the equipment containing information is destroyed or reused. A procedure for the physical destruction of equipment is established, employing specialized technologies, and the destruction process is documented

6.15. Staff ensure that the equipment they use is adequately secured while they are left unattended. All personnel are informed about the rules and obligations related to the provision of protection.

7. Technological control measures

7.1. To ensure security of information stored, processed, and accessed through end-user devices, policies are adopted and communicated to personnel for the secure configuration and management of end-user devices, considering at least the following:

7.1.1. the type and level of classification of information that end-user devices can manage, process, store, or support.

7.1.2. registration of end-user devices.

7.1.3. physical security requirements.

7.1.4. restriction in software installation.

7.1.5. requirements for operating systems, software, and latest updates on end-user devices.

7.1.6. access control.

7.1.7. encryption of storage devices of end-user devices and formation of backup copies according to the type and classification level of information.

7.1.8. protection against malware.

7.1.9. procedure for connecting to home and other public Internet networks.

7.2. Access permits to information and other related assets is limited to at least:

7.2.1. anonymous access to sensitive information.

7.2.2. identifying the information to which an individual or groups of individuals have special access (reading, writing, deleting, executing, etc.), assigning powers.

7.2.3. isolating sensitive information.

7.3. Read and write access rights to source code, development tools, and software libraries are governed by at least the following:

7.3.1. managing access rights to the source code and software libraries of the program in accordance with established rules.

7.3.2. granting read and write access to source code based on business needs, as well as in accordance with established policies to manage risks of modification or misuse.

7.3.3. updating the source code and related elements in accordance with change control rules and granting access to the source code.

7.3.4. maintaining application lists in a secure environment, where read and write access rights are managed and assigned.

7.3.5. logging all access and changes to the source code.

7.4. Based on the rules of access to information, secure authentication technologies and processes are applied, considering at least the following:

7.4.1. not displaying the sensitive information accessed until the authentication process is successfully completed.

7.4.2. displaying a general warning that only authorized persons may enter.

7.4.3. confirming the validity of all data only after entering them for authentication.

7.4.4. application of brute-force attack protection methods of usernames and passwords.

7.4.5. logging successful and failed login attempts.

7.4.6. displaying the following information after successful login:

7.4.6.1. the date and time of the previous successful login.

7.4.6.2. details of failed login attempt since the last successful login.

7.4.7. not displaying the entered password and ensuring it is not transmitted in clear text form over the network.

7.4.8. terminating established connections with the system after a specified period of inactivity.

7.5. Privileged access rights should be granted only to authorized personnel, software components and services subject to at least the following safeguards and the requirements of Item 7.4:

7.5.1. granting privileged access rights only when needed and imposing higher authentication requirements than normal access rights.

7.5.2. designating and registering personnel requiring privileged access rights for each system and process and setting the period of use of privileged access rights.

7.5.3. ensuring that privileged users only use their privileged accounts, as well as the separation of privileged accounts from everyday user accounts.

7.5.4. monitoring and logging the actions of personnel with privileged access.

7.6. Information and information technologies are protected from malicious software in conjunction with staff awareness, and at least the following is considered:

7.6.1. detecting and preventing unauthorized software usage.

7.6.2. identifying and preventing the use of known and suspected malicious websites.

7.6.3. application of anti-malware tools only by obtaining a license.

7.6.4. applying anti-malware tools.

7.6.5. centralized management of anti-malware tools.

7.6.6. installing, debugging, testing, supporting, and monitoring anti-malware by authorized persons.

7.6.7. automatically providing the latest updates to anti-malware databases.

7.6.8. implementing at least the following checks by anti-malware tools:

7.6.8.1. pre-use verification of information received via network or any storage devices.

7.6.8.2. checking attachments in e-mails and instant messaging software before they are used.

7.6.8.3. verifying websites.

7.6.9. registering all cases of malware infections, as well as maintaining accountability by indicating their types and sources of infection.

7.7. In the process of deleting sensitive information, the selection of appropriate deletion methods (e.g., electronic overwriting, cryptographic erasure, etc.) and preserving deletion results as evidence are ensured, as well as the appropriateness of deletion methods when using third-party providers, including 'cloud' service providers is verified, and evidence of deletion is requested from the provider.

7.8. To prevent the loss of information, the rules for creating backup copies of critical information systems, as well as testing the recovery process, covering at least the following are adopted and applied:

7.8.1. determining objectives and responsibilities and powers to create and restore backup copies.

7.8.2. centralized management of means of creating back-up copies.

7.8.3. ensuring encrypted storage of backup copies of sensitive information.

7.8.4. determining the scope of backup copies (e.g., partial, differential and/or full backup copy) and the frequency of creation, considering business needs of the supervised entity, information security requirements and the criticality of information systems.

7.8.5. keeping backup copies for the period and in the manner determined by the legislation regarding archiving and ensuring their deletion after the storage period expires.

7.8.6. implementing test restoration of backups no less than 2 (two) times a year and documenting the results.

7.8.7. registering logs on creation of backup copies.

7.9. Rules are adopted to ensure the creation, maintenance, protection, and analysis of logs of activities, exceptions, errors, and other events. When logging events for critical information systems and other related assets, at least the following is considered:

7.9.1. event logs are registered and monitored regularly by keeping them for at least 1 (one) year. Logs recorded include at least the following:

7.9.1.1. alert logs – logs that contain unusual activity and possible failures.

7.9.1.2. error logs – logs that show hangs or crashes.

7.9.1.3. critical logs – logs that contain critical events that require intervention to prevent system failure.

7.9.2. each event log stores at least the following information:

7.9.2.1. user identifier.

7.9.2.2. the date, time, and details of the event (entry, exit, etc.).

7.9.2.3. event status and/or error code.

7.9.2.4. successful and failed login attempts.

7.9.2.5. system configuration changes.

7.9.2.6. logged files and login type.

7.9.2.7. network addresses and protocols.

7.9.2.8. activation and deactivation of security systems.

7.9.2.9. operations performed in the software.

7.9.3. log recording tools and log data are protected against modification and unauthorized access.

7.9.4. users, including those with privileged access, are prohibited from deleting or disabling logs of their activities.

7.10. information systems and other related assets are synchronized with a single time source and a standard reference time is established for coordination.

7.11. to protect information in networks and network equipment, at least the following requirements are considered:

7.11.1. defining network infrastructure management responsibilities.

7.11.2. ensuring the protection of confidentiality and integrity of information transmitted over wireless, third-party, or global networks.

7.11.3. preparing network diagrams for the network infrastructure, ensuring its relevance, as well as ensuring the storage of equipment configuration files.

7.11.4. defining and incorporating into network service agreements security mechanisms, service levels and management requirements for all network services.

7.11.5. providing segmentation of users and information systems in the network, as well as network management channels.

7.11.6. detection, limitation, and authentication of equipment connected to network.

7.12. for security mechanisms, service levels and management requirements of network services are established and enforced, providing at least the following:

7.12.1. the range of networks and network services to which access is permitted.

7.12.2. authentication requirements for access to various network services.

7.12.3. network management and technological control measures (e.g., authentication, encryption, etc.) and procedures to protect access to the network.

7.12.4. the means used to access the network and network services (e.g., using a virtual private network (VPN) or wireless network).

7.12.5. time, location, and other attributes of the user at the time of login.

7.13. Restrictions on access to unwanted Internet resources are applied, as well as rules for safe and correct use of these resources are formed, considering at least the following:

7.13.1. determining the types of Internet resources to which personnel have the right to access or are prohibited.

7.13.2. blocking access to the following Internet resources:

7.13.2.1. Internet resources with the function of uploading information to the Internet, except those permitted for necessary business needs.

7.13.2.2. known or suspected malicious Internet resources (e.g., Internet resources that distribute malware and phishing content).

7.13.2.3. Internet resources that distribute illegal content.

7.13.3. ensuring the security of social media accounts of the supervised entity, considering at least the following:

7.13.3.1. set a password for each social media account in accordance with the authentication data management rules.

7.13.3.2. apply two-factor authentication.

7.13.3.3. periodically update passwords.

7.13.3.4. view and update individual security settings on a social media account.

7.13.3.5. monitor sensitive information sharing on social media accounts.

7.13.3.6. regularly monitor social media account activity.

7.13.3.7. restrict the use of shared or common-use end-user devices.

7.13.3.8. provide social media software and the end-user devices on which they are installed with the latest updates.

7.13.3.9. secure an email account associated with a social media account.

7.13.3.10. list and periodically review end-use devices connected to a social media account.

7.14. The principles of secure systems engineering are formulated with at least the following in mind and are applied to any information system development activity:

7.14.1. applying the principle of defense in depth.

7.14.2. application of the 'zero trust' principle, which includes at least the following:

7.14.2.1. not rely only on network perimeter security to ensure information security.

7.14.2.2. use a 'never trust and always verify' approach to access information systems.

7.14.2.3. provide end-to-end encryption of data transmission channels.

7.15. The anonymized use of sensitive information is not permitted during test inspections; the focus is on ensuring the security of the test environment.

7.16. During an audit involving critical information systems and related assets, audit tests are carefully planned and coordinated with the management of the supervised entity to minimize negative impacts on business processes of the supervised entity.

7.17. To ensure that information technologies, human resources, and other resources meet the necessary volume, their usage is monitored and adjusted to current and anticipated needs of the supervised entity, considering at least the following:

7.17.1. recruitment of new personnel.

7.17.2. acquisition of new facilities, including more powerful systems and components (central processor, RAM, other memory devices, etc.).

7.17.3. archiving and/or deleting obsolete data.

7.17.4. decommissioning of useless and unnecessary software, database management systems, technical infrastructures.

7.17.5. optimization of software codes and database queries.

7.18. To identify technical vulnerabilities in the critical information system and other related assets and prevent their abuse, the following measures are taken at minimum:

7.18.1. monitoring of technical vulnerabilities, risk assessment of vulnerabilities, management of application additions and updates, and defining duties and responsibilities for these duties.

7.18.2. implementing internal and external intrusion tests, and documenting results by engaging external specialists specialized in penetration tests at least once a year to analyze and eliminate technical vulnerabilities.

7.18.3. switching a critical information system to an operational environment after intrusion testing and elimination of identified vulnerabilities.

7.18.4. testing the changes planned to be applied to the critical information system in the test environment and applying them in the operational environment after eliminating detected vulnerabilities.

7.18.5. determining the associated risks and actions to be taken after a technical vulnerability is discovered.

7.19. Configurations, including security configurations, are defined, documented, implemented, and monitored to ensure that the technical infrastructure and software work properly with the required security adjustments and that their configurations are protected from unauthorized or incorrect changes.

7.20. To prevent illegal disclosure, considering the requirements of the legislation and the terms of the agreement, sensitive information is anonymized in relation to persons without access permission, and access rights are determined and protected under the information classification.

7.21. To mitigate information leakage in information systems, networks, and other infrastructure elements, considering the classification of information, it is ensured that channels susceptible to potential information leakage are monitored and appropriate tools such as control mechanisms, software, and systems are employed to prevent such leaks.

7.22. Sufficient information technologies are ensured by defining at least the following for critical information systems to meet accessibility requirements:

7.22.1. concluding an agreement with at least 2 (two) network service providers and/or internet service providers.

7.22.2. applying load balancing and clustering technologies for business continuity in information systems.

7.22.3. information technology and communication equipment having duplicate components (central processor, RAM, other memory devices, etc.).

7.23. To assess potential information security incidents, a mechanism for continuous monitoring of unusual behaviors that may occur in the network, system and software is established, considering at least the following:

7.23.1. incoming and outgoing network, system, and software traffic.

7.23.2. access to systems, information processing centers, monitoring system, network equipment and network configuration files, including privileged access.

7.23.3. logs of security tools (antivirus, network security equipment, etc.).

7.23.4. availability of resources (central processor, RAM, other memory devices, etc.).

7.24. To safely install software in operating systems, at least the following requirements are considered:

7.24.1. formation of the list of permitted software.

7.24.2. installation of software by authorized persons only.

7.24.3. installing and updating software only after successful trial testing.

7.24.4. defining a rollback plan before the changes are implemented.

7.24.5. limiting the use of utility software that exceeds the control over operating system and software and applying control over its use.

7.25. To ensure correct selection and effective use of cryptography to protect information confidentiality and integrity, the following measures are implemented:

7.25.1. the information requiring cryptographic protection is identified.

7.25.2. the level of complexity of the encryption algorithm of the cryptographic tools used for information encryption is determined based on the risk assessment.

7.25.3. duties for using cryptographic means and responsibilities and powers for these duties are determined.

7.25.4. a cryptographic key management system is established that defines at least the following:

7.25.4.1. generating cryptographic keys.

7.25.4.2. distribution of cryptographic keys.

7.25.4.3. changing cryptographic keys.

7.25.4.4. recalling cryptographic keys.

7.25.4.5. revoking and recovering cryptographic keys.

7.25.4.6. creating and maintaining a backup copy of cryptographic keys.

7.25.4.7. destroying cryptographic keys.

7.25.4.8. logging of cryptographic key management.

7.26. The safe development of software and information systems throughout their entire operational period is ensured by considering at least the following:

7.26.1. separation of development, test, and operational environments.

7.26.2. formulation of secure development methodology and secure coding guidelines.

7.26.3. application of safety requirements at design and projecting stages.

7.26.4. regularly inspecting source codes, conducting penetration tests, and eliminating security holes found in source codes.

7.26.5. secure storage and configuration of source codes.

7.26.6. providing source code version controls.

7.26.7. adopting an outsourcing arrangement that includes at least the following:

7.26.7.1. consideration of license agreements, code ownership and intellectual property rights related to outsourced service.

7.26.7.2. defining supervised entity' information security requirements in agreements.

7.26.7.3. defining security requirements for the development environment.

7.26.7.4. implementing service acceptance tests.

7.26.7.5. adhering to legislative requirements (e.g., on the protection of personal data).

7.27. When developing or acquiring software, information security requirements are determined considering at least the following:

7.27.1. the type and classification level of information processed by the software.

7.27.2. access rights to data and functions in the software.

7.27.3. resilience against malicious attacks and inadvertent disruptions.

7.27.4. requirements for the protection of sensitive information.

7.27.5. requirements for protection during information processing, transmitting, and storage.

7.27.6. encryption of data sharing between all related parties.

7.28. Rules encompassing at least the following for the management of changes affecting information security in business processes, information processing tools and software are developed and approved:

7.28.1. identifying and registering changes.

7.28.2. planning and testing changes.

7.28.3. risk assessment of potential impacts of changes, including impacts on information security.

7.28.4. verification of compliance with information security requirements.

7.28.5. communicating details of changes to all relevant stakeholders.

7.28.6. defining procedures and responsibilities for canceling or reverting failed changes or contingencies during the implementation of changes.

7.28.7. identifying processes for urgent changes necessary to resolve incidents.

7.28.8. keeping records of changes that include those specified in sub-items 7.28.1-7.28.7 of these Requirements.

7.29. To ensure information security in mobile applications, at least the following measures are implemented by the supervised entity:

7.29.1. appropriate control measures are applied to prevent illegal interception of sensitive information entered through the user interface (anti-keylogging).

7.29.2. appropriate control measures are applied to prevent outsiders from running mobile applications in a debugger environment, emulator, or a virtual machine (anti-debugging and anti-emulation).

7.29.3. mobile applications are designed to operate exclusively on the mobile device upon which they are activated (device-binding).

7.29.4. To use in a form not defined by the manufacturer, penetration with the operating system of the mobile device (jailbreak) is checked, and it is not allowed to run mobile applications on such a mobile device.

8. Accountability/reporting

8.1. The supervised entity provides the information on last, first and middle names, address, and contact details of the person responsible for information security appointed as per Item 3.3 of these Requirements, as well as a copy of the decision on appointment within 5 (five) working days from the date of appointment, as well as from the date of change in the event of a change to this information to the Central Bank in writing.

8.2. The supervised entity submits to the Central Bank within 5 (five) working days the external auditor's opinions obtained as per Items 3.7 and 3.8 of these Requirements, as well as a copy of the document on compliance with the requirements obtained according to Item 3.8 of these Requirements.

8.3. The supervised entity submits the preliminary report specified in Annex No. 1 to these Requirements within four hours of the occurrence or discovery of a high-category incident to the Central Bank through a dedicated information sharing system. If this period falls outside of normal working hours, the information should be submitted to the Central Bank during the first working hour of the following working day.

8.4. Within five working days from the complete elimination of the incident, the supervised entity submits the final report specified in Annex No. 2 to these Requirements to the Central Bank through a dedicated information sharing system.

8.5. Current information about the critical information system and related assets determined as per sub-item 4.12.1 of these Requirements is submitted to the Central Bank within the first 10 (ten) working days of January of the following year for each calendar year as per Annex No. 3 to these Requirements.

8.6. According to Item 4.14 of these Requirements, the supervised entity informs the Central Bank about the test 5 (five) working days before conducting it and within 7 (seven) working days after completing the test, the entity submits the report specified in Annex No. 4 to these Requirements.

8.7. The results of penetration tests carried out according to sub-item 7.18.2 of these Requirements are submitted to the Central Bank no later than 5 (five) working days.

Annex 1
to the 'Information security requirements
for supervised entities in financial markets'

Preliminary high-category incident report

Reporting date (day/month/year, hour/minute)	
Incident number	
Incident time (day/month/year, hour/minute) (if known)	
Incident detection time (day/month/year, hour/minute)	
General information	
Supervised entity name	
Information on the person responsible for incident (last, first, middle names, position, including contact information (e-mail, GSM))	
Incident's brief and overall description	
Incident impact criteria	□ Impact on service users □ Impact on servicer availability □ Economic impact (financial losses) □ Reputation impact □ Impact on operations □ Impact on other supervised entities or relevant financial services infrastructure
Has/will a report been/be submitted to related public authorities (institutions)? (If 'yes', please provide the name of the relevant public authority or institution)	

Annex 2
to the 'Information security requirements
for supervised entities in financial markets'

Final high-category incident report

Reporting date (day/month/year, hour/minute)		
Incident number (referred to the preliminary report)		
1. General information		
Updated information (in addition to the preliminary report)		
Incident information		
Changes to the preliminary report		
Other significant information		
Additional incident information		
Incident date and time (day/month/year, hour/minute)		
How did the incident start?		
How did the incident progress?		
Have service users been informed on the incident? (if 'yes', please provide details)		
Is it connected to previous incidents? (if 'yes', please provide details)		
Were other institutions/third parties exposed to this incident? (if 'yes', please provide details)		
Incident elimination date and time (day/month/year, hour/minute)		
2. Incident classification		
Impact on supervised entity's operations	The number of operations affected	
	Percentage of operations affected (vs the average daily	

	indicator of the previous month)	
	Size of operations affected (in thousand manat)	
	Incident duration	
	Notes	
Impact on supervised entity's users	The number of users affected (in numbers)	
	The number of users affected (in %)	
Economic impact (financial losses)	Size of loss (In thousand manats)	
Impact on other institutions or relevant supervised entity's infrastructure (Yes/No) (if 'yes', please provide details)		
Reputation impact (Yes/No) (if 'yes', please provide details)		
3. Incident description		
Incident cause (If the answer is 'other', please provide details)		□ Harmful activity □ Processing error □ System error □ Human factor □ External factor □ Other
4. Incident impact		

Overall impact		□ Integrity □ Confidentiality □ Accessibility
Service channels affected		□ Branches □ Electronic commerce □ Mobile application □ Website □ ATMs □ Agent network □ Other
The service affected		
5. Incident cause and analysis		
Incident cause (multiple causes may be specified)	Harmful activity	□ Malware □ Unauthorized intrusion □ System overloading □ External damage □ Fraud □ Other
	Processing error	□ Monitoring and control error □ Communication error □ Recovery challenges □ Other
	System error	□ Technical error □ Network error □ Database error □ Software error □ Physical damage □ Other
	Human factor	□ Unexpected error □ Inaction □ Resource shortfall □ Other
	External factor	□ Technical service provider □ Force-majeure case □ Other
	Other (if none of the above)	

Additional information associated with the cause of the incident	
Measures taken (to be taken) to prevent the incident from recurring	
6. Additional information	
Have other institutions been informed on the incident? (If yes, please provide related information)	
Has a legal action been taken against the institution? (If yes, please provide related information)	

Annex 3
to the 'Information security requirements
for supervised entities in financial markets'

Information
on the critical information system and related assets

Critical information system		
Critical information system name		
Critical information system purpose		
Criteria to consider the system critical		
Business impact analysis findings		
Related assets		
Related asset name	Supporting functionality	Operating system
Provider information		
Provider(s) supporting the critical information system	1. 2.	
Provider(s) supporting related assets	1. 2.	

Annex 4
to the 'Information security requirements
for supervised entities in financial markets'

Report on the transition to the back-up center

General information			
Supervised entity name			
Back-up center transition scenario			
Transition date and time			
Transition period			
Covered areas (services)			
Non-covered areas (services)			
Transition result			
Persons responsible on the organization of transition to the back-up center			
Last, first, middle names	Structural unit	Position	Signature