APPROVED
Director of Spacegate Services – FZCO
Islam Otegulov

Signature
January 12, 2026

INFORMATION SECURITY POLICY
SPACEGATE SERVICES – FZCO
2026

1. INTRODUCTION

1.1. The Information Security Policy of Spacegate Services – FZCO (hereinafter – the Company) defines the fundamental principles that guide the Company in matters of information security within its information systems.

1.2. The purpose of this Policy is to establish requirements for Company personnel aimed at enhancing the level of information security and minimizing potential losses caused by malicious actors, emergency failures, and human error.

2. POLICY OBJECTIVES

The application of the Information Security Policy achieves the following objectives:

2.1. Detailing the requirements of the Company's Information Security Policy as applicable to the conditions of data access, handling, and processing.

2.2. Minimizing data security threats, characterized by indicators of confidentiality, integrity, and availability, by improving the reliability of organizational and technological solutions and business processes.

2.3. Implementing a systematic approach to data security in the context of processing, reviewing, and interacting with third-party organizations.

2.4. Reducing operational risks associated with data processing technologies.

2.5. Ensuring the Company's compliance with data security requirements established by the legislative acts of the Kyrgyz Republic.

3. KEY ELEMENTS OF THE INFORMATION SECURITY SYSTEM

3.1. Confidentiality, integrity, availability, system security, reliability, and recoverability of data are ensured by the following elements:

Confidentiality implies that only authorized users have access to data and the system, and solely for the purpose of fulfilling their official duties. It is ensured by:

- Access provisioning instructions for information systems;
- The payment system's authorization framework;
- Physical access control at equipment hosting facilities.

Data integrity ensures that data is complete and unaltered during any operation performed on it, whether transmission, storage, or presentation. It is ensured by:

- Event logging;
- Protection against modification and/or substitution;
- Data backup procedures;
- Physical access control at equipment hosting facilities.

Availability means providing information to an authorized user at the required time and in the required format. It is ensured through the authorization system, fault tolerance, and data backup.

Security is maintained through a comprehensive set of measures aimed at ensuring the confidentiality, integrity, and availability of payment system data.

Reliability and recoverability of data are ensured through hardware redundancy, clustering, and backup procedures.

3.2. Information security requirements within the Company are determined by the following components:

- Conducting background checks and establishing information security requirements for Company employees;
- Assigning and distributing roles and registering users in the Company's information resources;
- Establishing an information security risk management process through the designation of responsible personnel and the implementation of necessary measures;
- Ensuring the continuity of information resources, protection against physical threats, and business continuity, including data backup and system recovery;
- Ensuring the physical and informational security of the Company's information resources;
- Logging all activities within the Company's information resources;
- Installing antivirus protection on workstations;
- Governing the use of internet resources.

4. INFORMATION SECURITY MECHANISMS

In order to reduce fraud-related risks, continuous training of Company personnel on fraud prevention and unauthorized access mitigation is required.

4.1. New employees are required to complete training on internal regulations (orders, procedures, rules, instructions, etc.) aimed at preventing and detecting fraud and unauthorized access. Access for employees and management of automated processing complex (APC) systems is permitted only upon completion of such training.

4.2. Existing employees receive periodic training on new methods and technologies for detecting and preventing fraud and unauthorized access.

4.3. Periodic knowledge assessments of existing employees on internal regulations (orders, procedures, rules, instructions, etc.) directed at preventing and detecting fraud and unauthorized access are conducted.

4.4. The Company ensures comprehensive security throughout the lifecycle of its information resources, including the protection of automated systems at all stages of the automated system lifecycle (design, implementation, testing, acceptance, operation, maintenance, modernization, and decommissioning must be documented and approved by

management). Testing is conducted in a test environment identical to the production environment.

4.5. The Company uses only licensed software. Open-source software or internally developed software is permitted provided a complete set of documentation approved by the relevant manager is available (technical specifications, test plans and procedures, test reports and logs, acceptance act for production deployment).

4.6. All Company information resources maintain an event log (logging) of activities performed within the automated system, personal computers, server and network equipment, and databases, as a tool for information security auditing, event reconstruction, and accountability. The event log must capture the actions of all users, including privileged accounts (root, administrator, sysdba, dba).

4.7. The Company ensures the use of only officially procured (licensed) antivirus solutions. Installation and regular updating of antivirus software on workstations and servers must be carried out by designated administrators.

4.8. The Company implements network segmentation and firewall measures within internal computing networks, as well as protection of internal networks when interfacing with the internet.

4.9. The Company ensures that backup copies are created for all processed and completed payments.

4.10. External storage media are used as data carriers: hard drives, magnetic tapes, recordable optical digital discs, and others.

4.11. All backup copies must be labeled with the stored information, a reference number, and the date of creation.

5. SECURITY THREAT CLASSIFICATION

5.1. All types of data security threats are broadly categorized into two types: internal and external threats.

5.2. External threats carry a broad spectrum of destructive impacts and may manifest as follows:

- Natural disasters;
- Armed conflicts;
- Technogenic catastrophes;
- Social conflicts;
- Sabotage acts;
- Disruption of municipal services, including power and water supply.

5.3. Internal threats are localized and targeted in nature, and the damage they may cause can exceed that of external threats. The primary internal threat types include:

- Unintentional errors by personnel;
- Negligent performance of official duties by personnel;
- Deliberate destructive actions by employees;
- Uninformed decision-making by management (management errors).

5.4. When developing protective measures, it is taken into account that some threats may manifest independently or as a consequence of other threats.

5.5. Data security threats are most likely to occur at the following levels of the information and telecommunications infrastructure:

- Physical;
- Hardware;
- Software.

5.6. Threat models developed for data, in order to build effective countermeasures, must account for all specified categories and levels of threat realization.

6. PERSONNEL REQUIREMENTS AND ROLE ASSIGNMENT, DISTRIBUTION, AND REGISTRATION IN THE AUTOMATED SYSTEM

6.1. The Company establishes information security requirements for its employees in accordance with this Policy. All Company employees must be familiarized in writing with the information security requirements.

6.2. The Company's automated system defines roles that ensure a clear delineation of employee authority. When granting employee access to the automated system, the procedures of authorization, identification, authentication, and user approval are performed. Prior to issuing a user identifier, the user's identity must be verified. The system must record the person responsible for issuing the identifier.

6.3. All users of the automated system operate under unique user accounts.

6.4. When granting employees access to the Company's information resources, the procedures of authorization, identification, authentication, and user approval are performed.

6.5. All users of the Company's information resources operate under unique user accounts.

6.6. When distributing access rights for employees and payment system participants to the Company's information resources, the Company adheres to the following principles:

- "Know Your Employee" – a principle reflecting the Company's concern regarding employee conduct and potential issues such as misuse of assets or financial difficulties that may lead to security vulnerabilities;
- "Need to Know" – a security principle that restricts access to information and information processing resources to those who require it to perform specific duties;
- "Least Privilege" – a principle whereby a user is granted only the minimum privileges necessary to perform a given operation.

6.7. Access to information resources (IR) for Company employees (including privileged administrator accounts) is provided by the Chief Technology Officer (CTO) on the basis of a formal request.

6.8. The Company maintains a documented Registry of Information Resources (automated systems and their types) along with the access rights of employees and participants to those assets.

6.9. The CTO reviews and executes the user registration procedure and organizes access to information resources, recording the completion in the relevant request. The following method is used to generate usernames in information systems: first letter of the first name, period, last name in Latin transliteration. In cases of duplicate usernames, the second letter of the first name or patronymic is added to one of them.

6.10. All events related to user registration and access rights modifications are recorded in system and automated system logs.

6.11. The CTO conducts a user briefing on security requirements and the consequences of non-compliance.

6.12. Requests to modify user access rights to information resources are formally documented.

6.13. User access rights are regularly reviewed and monitored by the CTO based on Company orders (promotions, demotions, transfers, or terminations).

6.14. Termination or restriction of a user's access rights to information resources is carried out upon a change in the employee's duties or functions, upon dismissal, or upon transfer to another department of the Company.

6.15. Grounds for restricting or revoking access include:

- A management request to restrict access to information resources;
- Orders for dismissal, transfer, or leave, electronic copies of which are sent by HR personnel to the employee responsible for information security.

6.16. Upon employee dismissal, the following actions are performed:

- Revocation of access to information resources;
- Retrieval of personal identifiers (where applicable);
- Removal of the departing employee's public key from the electronic digital signature (EDS) public key database (where EDS or digital certificates are in use);
- Retrieval of identification cards, proximity cards, and key storage devices (where applicable).

6.17. Additionally, upon dismissal of privileged users (administrators) across all categories (local network, application system, database server, information security, etc.):

- A new administrator must be appointed in the prescribed manner no later than five business days prior to the dismissal date;
- After the appointment of a new administrator, a formal handover of responsibilities is conducted, including an audit of all registered system users, access rights to information resources, integrity verification of software installed on systems administered by the departing employee, and confirmation that all required documentation is in order. A handover act is prepared and signed by a specially formed commission, the departing administrator, and the newly appointed administrator;
- Following the signing of the handover act by the IT Officer and the Information Security Officer, the newly appointed administrator must immediately change all passwords in the automated system;
- In the event that integrity violations or misconduct are discovered during the handover process, the newly appointed administrator must promptly inform the IT and information security personnel.

7. INFORMATION SECURITY REQUIREMENTS

7.1. The Company ensures information security in the course of its primary and other activities, and conducts background checks during employee recruitment, including:

- Verification of the authenticity of submitted documents, declared qualifications, and the accuracy and completeness of biographical information using available and publicly accessible data sources;
- Assessment of professional skills and suitability for the position;
- All Company employees must be familiarized in writing with the Company's information security requirements.

7.2. The Chief Technology Officer of the Company serves as the Information Security Officer – the person responsible for ensuring information security. The CTO oversees and bears responsibility for organizing information security within the Company, and must on a systematic basis update awareness of information security threats, promptly inform Company management and staff of such threats, and carry out measures aimed at raising the overall security awareness of personnel.

7.3. The CTO, as Information Security Officer, carries out work to ensure information security, including:

- Monitoring compliance with internal regulations and regulatory legal acts in the field of information security;
- Analyzing the level of information security protection;
- Developing internal regulatory documents on information security.

7.4. Employee access to technological operations involving data processing:

- Is granted solely for the purpose of fulfilling official tasks;
- Is formalized through internal Company orders (directives), or specified in job descriptions with explicit access rights (permissions);
- Is implemented in accordance with job descriptions and Company access rights.

7.5. Data stored on physical media is maintained separately from other categories of information.

7.6. Protection against unauthorized access (UAA) is achieved through the comprehensive application of regulatory and technical-software requirements governing access control procedures.

7.7. Backup copies of disk arrays and business automation systems ensure guaranteed recovery of source objects and technological processes within the calculated time frame.

7.8. Information security requirements are consolidated in a regulatory document covering the stages of approval, design, implementation, and operation.

7.9. Protection of the Company's information assets against malware and network attacks is ensured through a comprehensive set of software and technical solutions combining capabilities for intrusion prevention, spyware defense, and protection against network and computer viruses.

7.10. Access procedures for premises housing technical equipment and data storage media include controls for restricting unauthorized entry and physical barriers against unauthorized access.

7.11. Connections between the payment system and systems of other classes or the internet are established using firewall solutions.

7.12. Development of technical specifications, design, creation, acceptance (trial operation), and commissioning are carried out in coordination with and under the supervision of the CTO, who is responsible for data security within the Company.

8. HARDWARE SECURITY

In order to reduce risks associated with physical damage to hardware and communication lines, as well as to prevent power supply failures and equipment malfunctions, the following security measures are applied:

8.1. Equipment for the electronic payment system is installed exclusively in dedicated lockable premises with load-bearing walls and parameters that comply with the technical specifications for the operation of such equipment.

8.2. Access for unauthorized persons to premises where equipment related to the electronic payment system is installed is restricted. Only authorized personnel, as defined by their job descriptions, have the right of access.

8.3. Routine monitoring of the system configuration and its configurable parameters is conducted by authorized personnel through visual inspection at least once per month. All changes to equipment configuration and configurable parameters must be approved by the Company Director.

8.4. Magnetic data storage media are stored in specialized containers that exclude the possibility of mechanical and electromagnetic impact.

8.5. The transfer of equipment related to the electronic payment system, as well as corresponding documentation, to third parties, institutions, or organizations is prohibited.

8.6. Operation of equipment related to the electronic payment system without power smoothing filters, uninterruptible power supplies, or autonomous power sources is prohibited.

9. SOFTWARE SECURITY

In order to reduce risks associated with software errors or modifications, the following security measures are applied:

9.1. Access for unauthorized persons to software is restricted. Only authorized personnel, as defined by their job descriptions, have the right of access.

9.2. Backup to magnetic media is performed no less than once per day. All backup and restore operations are recorded in dedicated logs by designated responsible personnel.

9.3. Testing using the latest versions of antivirus software is conducted periodically, no less than twice per month, to protect software from computer virus intrusion.

10. SECURITY OF ELECTRONIC PAYMENT DOCUMENT TRANSMISSION

In order to reduce risks associated with repudiation of authorship or receipt of an electronic payment document, as well as disclosure and distortion of data during transmission via communication channels, the following security measures are applied:

10.1. Access for unauthorized persons to computers equipped with specialized electronic digital signature software is restricted. Only authorized personnel appointed by order have the right of access.

10.2. Transmission of electronic payment documents via communication channels is performed exclusively using firewall solutions and certified cryptographic protection tools that have undergone testing and trial operation.

10.3. Cryptographic protection and firewall tools must be installed at every interface point between local-level network segments and external-level segments.

10.4. Firewall solutions must provide multi-level data filtering with the formation and analysis of network connections.

10.5. Access for unauthorized persons to cryptographic protection and firewall tools is restricted. Only authorized personnel appointed by order have the right of access.

10.6. In the event of a violation or attempted violation of access rights to information resources associated with the electronic payment system, the payment system participant must immediately notify the head of the Security Department of the National Bank and submit a report describing the identified breach.

10.7. Operation of cryptographic protection and firewall tools, and the use of electronic digital signatures, must be carried out in strict accordance with the applicable operation instructions and rules governing cryptographic protection, firewalls, and the use of electronic digital signatures.

11. DEVELOPMENT OF NEW ANTI-FRAUD METHODS

In order to reduce fraud-related risks, the following measures are required:

11.1. Measures to identify and assess the risks of money laundering or terrorist financing that may arise in connection with the development of new products and business practices, including new delivery mechanisms, and the use of new or emerging technologies for both new and existing products. In the case of financial institutions, such a risk assessment must be conducted prior to the launch of new products, business practices, or the use of new or emerging technologies.

11.2. Measures to review existing systems for vulnerabilities and fraud risks arising from technical, technological, software, and other weaknesses within the automated processing complex (APC).

11.3. Measures for the development of new anti-fraud methods, including but not limited to:

- Development of additional methods, systems, and rules for the identification of APC system users;
- Development of monitoring methods and early detection techniques for fraudulent transactions using algorithms and search patterns;
- Development of additional data protection tools for users and system participants;
- Development of new methods for protecting transmitted data using encryption;
- Development of new methods for remote identification of system users.