APPROVED
By the decision of
the Management Board of
SEC Almaty JSC
Minutes No._____
dated _____ 2023

INFORMATION SECURITY POLICY
SEC Almaty JSC

Owner	**Security Service**
Developer	**Security Service**
Responsible for storing the copy	**Department of Strategy and Corporate Development**
The place of storage of the original on paper and electronic media	**IRD database**
Responsible for monitoring and updating	**Security Service** **Department of Information Technologies**
Information about the IRD that becomes invalid due to the adoption of a new document	**No**
Protocol of Disagreements	**No**
Number of appendices and pages	**No appendices, 20 page Policy**

Almaty city
2023

TABLE OF CONTENT:

Chapter 1. General provisions

1.1. This document - Information Security Policy of SEC Almaty JSC (the Policy) is a document defining the priorities and principles of ensuring information security in the presence of threats characteristic and significant for the systems and information assets of SEC Almaty JSC (the Company).

1.2. This Policy has been developed in accordance with the legislation of the Republic of Kazakhstan in the field of information security, a series of international information security standards ISO/IEC 27000, COBIT, ITIL, the current state and immediate prospects for development of the information infrastructure of the Company, as well as the possibilities of modern organizational and technical methods of information protection.

1.3. The Policy defines a system of views on information security and is a systematic statement of the goals and objectives of protection, rules, procedures, practices and guidelines in the field of information security, as well as the basic principles of construction, organizational, technological and procedural aspects of information security in the Company.

1.4. The Policy takes into account the current state and immediate prospects for development of information technologies in the Company, the goals, objectives and legal bases of their operation, modes of operation, and contains an analysis of security threats to objects and subjects of information relations of the Company.

1.5. The Policy covers all information systems and documents owned and used by the Company. Ensuring information security is a necessary condition for successful implementation of the Company's activities. Information is one of the most important assets of the Company.

1.6. The Policy is the methodological basis for:

- formation and implementation of a unified policy in the field of information security in the Company;
- making managerial decisions and developing practical measures to implement the information security policy and developing a set of coordinated measures aimed at identifying, reflecting and eliminating the consequences of various types of information security threats;
- coordination of activities of the Company's structural divisions in carrying out work on creation, development and operation of information technologies in compliance with information security requirements;
- development of proposals to improve the legal, regulatory, technical and organizational provision of information security in the Company.

1.7. The use of this Policy as a basis for building a comprehensive information security system of the Company will optimize the costs of its construction.

1.8. When developing the Policy, the basic principles of creating integrated information security systems, characteristics and capabilities of organizational and technical methods and modern hardware and software tools for protecting and countering threats to information security were taken into account.

1.9. The main provisions of the Policy are based on a qualitative understanding of information security issues and do not address issues of economic (quantitative) risk analysis and justification of the necessary costs for information protection.
1.10. The provisions of the Policy are binding on all employees of the Company. The requirements of the Policy also apply to other organizations and institutions interaction of which is related to the issues of information resources of the Company.

Chapter 2. Principles of building an information security system of Company

The construction of the information security system of the Company and its functioning should be carried out in accordance with the following basic principles:
2.1. Legality.

It involves the implementation of protective measures and development of the Company's information security system in accordance with the current legislation in the field of information, informatization and information protection, as well as other regulatory acts on information security approved by state authorities and management bodies within their competence, using all permitted methods of detecting and suppressing offenses when working with information.

All users of the Company's information system should have an idea of responsibility for information offenses.

The implementation of this principle is necessary to protect the name and reputation of the Company.
2.2. Systematic approach.

Systematic approach to building an information security system in Company involves taking into account all interrelated, interacting and time-varying elements, conditions and factors that are important for understanding and solving the problem of ensuring information security of Company.

When creating a security system, all the weak and most vulnerable points of the information system of Company should be taken into account, as well as the nature, possible objects and directions of attacks on it by violators (especially highly skilled attackers), ways of penetration into distributed systems and unauthorized access to information. The security system should be built taking into account not only all known channels of penetration and unauthorized access to information, but also taking into account the possibility of fundamentally new ways of security threats.
2.3. Comprehensiveness

The comprehensive use of methods and means of protection of computer systems involves the coordinated use of heterogeneous means in the construction of an integral protection system that covers all significant channels of threat implementation and does not contain weaknesses at the junctions of its individual components. Protection should be built in layers. External protection should be provided by physical means, organizational and legal measures.
2.4. Continuity.

Ensuring information security is a process carried out by the Company's Management, information protection units and employees at all levels. This is a process that should be constantly going on at all levels within the Company, and every employee

of the Company should take part in this process. Information security activities are an integral part of the Company's daily activities. And its effectiveness depends on the participation of all employees of the Company in ensuring information security.

In addition, most physical and technical means of protection for the effective performance of their functions require constant organizational (administrative) support (timely change and ensuring the correct storage and use of names, passwords, encryption keys, redefinition of authority, etc.). Interruptions in the operation of security tools can be used by attackers to analyze the methods and means of protection used, to introduce special software and hardware "bugs" and other means of overcoming protection.

2.5. Timeliness.

means the proactive nature of information security measures, that is, the formulation of tasks for the comprehensive protection of information and the implementation of information security measures at the early stages of the development of information systems in general and their information security systems in particular.

The development of security system should be carried out in parallel with the development of the most protected information system. This will allow taking into account security requirements when designing and, ultimately, to create more efficient (both in terms of resource costs and durability) systems with a sufficient level of security.

2.6. Continuity of improvement.

means continuous improvement of measures and means of information protection based on the continuity of organizational and technical solutions, personnel, analysis of the functioning of the Company's information system and its protection system, taking into account changes in methods and means of information interception, regulatory requirements for protection, domestic and foreign experience in this area.

2.7. Reasonable sufficiency (economic feasibility).

means compliance with the level of costs for ensuring the security of information resources and the amount of possible damage from their disclosure, loss, leakage, destruction and distortion.

2.8. Personal responsibility.

means assignment of responsibility for ensuring information security and the system of its processing to each employee within his/her authority. In accordance with this principle, the distribution of the rights and duties of employees is structured in such a way that in the event of any violation, the circle of perpetrators is clearly known or minimized.

2.9. Minimization of authority.

Means providing users with minimal access rights in accordance with official necessity. Access to information should be provided only in the case and to the extent that it is necessary for the employee to perform his/her official duties.

2.10. Avoidance of conflicts of interest.

Effective information security system means a clear division of responsibilities of employees and avoidance of situations where the scope of responsibility of employees allows for a conflict of interests. Areas of potential conflicts should be identified, minimized, and under strict independent control. The implementation of this principle assumes that no employee should have the authority to carry out critical operations alone.

Giving employees powers that give rise to a conflict of interest gives them the opportunity to falsify information for deceptive purposes or in order to hide problems or losses incurred. In order to reduce the risk of information manipulation and the risk of theft, such powers should be divided as much as possible between different employees or divisions of the Company.

2.11. Interaction and cooperation.

means creation of favorable environment in the structural divisions of the Company. In such an environment, employees must consciously comply with the established rules and assist the activities of information protection units.

An important element of an effective information security system in Company is a high culture of working with information. The Company's management is responsible for strict compliance with ethical norms and standards of professional activity, for creating a corporate culture that emphasizes and demonstrates to staff at all levels the importance of ensuring information security of the Company. All employees of the Company should understand their role in the process of ensuring information security and take part in this process.

2.12. Flexibility of the protection system.

The information security system should be able to respond to changes in the external environment and conditions of the Company's activities. These changes include:

- changes in legislation regulating relations in the field of information security;
- changes in the organizational and staff structure of the Company;
- corporate restructuring, expansions, mergers and acquisitions;
- modification of existing or introduction of fundamentally new information systems;
- new technical means;
- new activities, new services, products.

The property of flexibility eliminates in such situations the need to take drastic measures to completely replace the means and methods of protection with new ones, which ensures the economic efficiency of the information security system.

2.13. Specialization and professionalism.

The implementation of administrative measures and operation of protective equipment should be carried out by professionally trained specialists of the Company (an employee of the Company with a special profile education in the field of information protection). It is allowed to involve specialized organizations or specialists who are most prepared for a specific type of activity to ensure the security of information resources and have practical experience in the development of means and implementation of information protection measures.

2.14. Simplicity of primary protection techniques for employees.

The mechanisms and methods of primary protection techniques should be clear and easy to use. The use of primary means and methods of protection should not be associated with knowledge of special languages or with performing actions that require significant additional labor during the normal work of registered users, and also should not require the user to perform routine operations that he/she does not understand.

2.15. Mandatory control.

means the compulsoriness and timeliness of identifying and suppressing attempts to violate the established rules for ensuring information security, based on the systems and means of information protection used.

Control over the activities of any user, each mean of protection and in relation to any object of protection should be carried out on the basis of the use of operational control and registration tools and should cover both unauthorized and authorized user actions. In addition, an effective information security system requires adequate and comprehensive information on the current state of processes related to the movement of information on compliance with established regulatory requirements, as well as additional information relevant to decision-making. The information must be reliable, timely, accessible and properly designed.

Deficiencies in the information security system identified by the Company's employees or security departments should be immediately brought to the attention of managers at the appropriate level and promptly eliminated. Significant deficiencies should be reported to the Company's management. Quarterly reports are sent to the management summarizing all the problems identified by the information security system. The department responsible for information security, quarterly, shall no later than 20 calendar days after the reporting period, send the report to the Company's management summarizing all the problems identified by the information security system.

Chapter 3. Subjects of information relations and objects of protection

3.1. The subjects of information relations in ensuring the information security of the Company are:

- The company as the owner of information resources;
- divisions of the Company participating in the information exchange;
- management and employees of the Company's structural divisions, in accordance with the functions assigned to them;
- The Company's counterparties are legal entities and individuals whose information is accumulated, stored and processed in the Company's information system;
- other legal entities and individuals involved in ensuring that the Company performs its functions (consultants, developers, service personnel, organizations involved in the provision of services, etc.).

3.2. The listed subjects of information relations are interested in providing:

- timely access to the information they need (its availability);
- reliability (completeness, accuracy, adequacy, integrity) of information;
- confidentiality (keeping secret) of a certain part of the information;
- protection against the imposition of false (unreliable, distorted) information on them;
- delineation of responsibility for violations of the established rules for handling information;
- opportunities for continuous monitoring and management of information processing and transmission processes;
- protection of information from its illegal replication (protection of copyright, rights of the owner of information, etc.).

3.3. The Company circulates information of various levels of confidentiality, containing information of limited distribution (official, commercial, personal data), and open information that are objects of protection. All information and information resources of the Company are subject to protection, regardless of its presentation and location in the information environment of the Company:

1) information assets necessary for the Company's work, regardless of the form and type of their presentation;
2) information systems, including information technologies, technical and software tools for the formation, processing, transmission, storage (including archived) and use of information,
3) elements of IT infrastructure, including computer equipment, libraries, archives, databases, servers, including physical and virtual, channels of information exchange and telecommunications, systems and means of information protection, objects and premises in which the protected elements of the Company's IT infrastructure are located;
4) processes, regulations and procedures of information processing in the Company;
5) information constituting a trade secret, access to which is restricted by the owner of the information in accordance with the legislation of the Republic of Kazakhstan;
6) personal data of employees and contractors of the Company;
7) open information necessary to ensure the normal functioning of Company.

3.4. Structure, composition and placement of the main objects of protection

The main features of the information environment of the Company include:

- combining a large number of various technical means of processing and transmitting information into a single system;
- significant expansion of the use of automated information processing systems, a wide variety and ubiquity of information management systems in Company;
- wide variety of solved tasks and types of processed data, complex modes of automated information processing with a wide combination of fulfilling information requests of various users;
- combining information of various purposes, affiliation and levels of confidentiality in single databases;
- presence of a large number of information channels of interaction with the "outside world" (sources and consumers of information);
- the need to ensure the continuity of the Company's information system;
- high intensity of information flows.

In these conditions, the vulnerability of information increases dramatically and the corporate information system becomes one of the most important elements of the information environment of Company, in which significant amounts of information shared by various users are processed and accumulated.

Chapter 4. Goals and objectives of information security

4.1. Protection objectives.

The main goal, which the provisions of this Policy are aimed at achieving, is to protect the subjects of the Company's information relations from possible material, moral or other damage through accidental or intentional impact on information, its carriers, processing and transmission processes, as well as minimizing the level of operational and other risks (the risk of damage to the Company's business reputation, legal risk, etc.).

This goal is achieved by providing and continuously maintaining the following properties of information:

- accessibility of information for legal users (stable functioning of the information system of Company, in which users have the opportunity to obtain the necessary information and results of solving problems in a reasonable time);
- integrity and authenticity (confirmation of authorship) of information stored and processed in the information system of the Company and transmitted via communication channels;
- confidentiality - keeping secret a certain part of the information stored, processed and transmitted through communication channels;

The necessary level of accessibility, integrity and confidentiality of information is provided by methods and means corresponding to the level of threats to information security.

4.2. In order to achieve the main goal of protecting and ensuring the specified properties of information, the Company's information security system must ensure the effective solution of the following tasks:

1) timely identification, assessment and forecasting of sources of threats to information security, causes and conditions contributing to damage to interested subjects of information relations, disruption of the normal functioning of the information system of the Company;

2) timely identification and elimination of vulnerabilities of the Company's assets and thereby preventing the possibility of damage and disruption of the normal functioning of business processes;

3) definition and documentation of the basic requirements and procedures for ensuring information security;

4) creation of mechanism for rapid response to information security threats and negative trends;

5) creating conditions for minimizing and localizing the damage caused by illegal actions of individuals and legal entities, weakening the negative impact and eliminating the consequences of information security violations;

6) protection against interference in the functioning of the information system of the Company by unauthorized persons (access to information resources should be available only to users registered in accordance with the established procedure);

7) differentiation of users' access to information, hardware, software and other resources of the Company (the ability to access only those resources and perform only those operations with them that are necessary for specific users to perform their official duties), that is, protection against unauthorized access;

8) ensuring the authentication of users participating in the information exchange (confirmation of the authenticity of the sender and recipient of information);

9) protection against unauthorized modification of software tools used in the Company's corporate information system, as well as protection of the system from the introduction of unauthorized programs, including computer viruses;
10) protection of restricted information from leakage through technical channels during its processing, storage and transmission via communication channels;
11) ensuring the survivability of cryptographic means of information protection;
12) planning and optimization of costs for ensuring information security of the Company.
4.3. The main ways to solve the problems of the protection system.
The set main goals of protection and the solution of the tasks listed above are achieved by:

- strict consideration of all the resources of the Company's information system subject to protection (information, tasks, documents, communication channels, servers, automated workplaces);
- logging the actions of personnel performing maintenance and modification of software and hardware of the corporate information system;
- completeness, real feasibility and consistency of the requirements of the Company's organizational and administrative documents on information security issues;
- training of employees responsible for the organization and implementation of practical measures to ensure the security of information and its processing processes;
- endowing each user with the minimum necessary powers to access the information resources of the Company for performance of their functional duties;
- clear knowledge and strict compliance by all users of the Company's information system with the requirements of organizational and administrative documents on information security issues;
- personal responsibility for the actions of each employee who, within the framework of their functional duties, has access to the information resources of the Company;
- continuous maintenance of the necessary level of security of the elements of the information environment of the Company, elimination of possible damage during the implementation of threats to information security, including reducing the recovery time of business processes after possible interruptions;
- application of physical and technical (software and hardware) means of protection of system resources and continuous administrative support of their use;
- monitoring and processing of information security events and incidents;
- effective control over the compliance of users of the Company's information resources with information security requirements;
- legal protection of the interests of the Company in the interaction of its divisions with external organizations (related to the exchange of information) from illegal actions, both on the part of these organizations, and from unauthorized actions of service personnel and third parties.

Chapter 5. The main threats to the security of the Company's information

5.1. Information security threats and their sources.

The whole set of potential threats to information security by the nature of their occurrence are divided into two classes: natural (objective) and artificial (subjective).

Natural threats are threats caused by impacts on the information system and its components of objective physical processes of a technogenic nature or natural phenomena independent of man;

Artificial threats are threats caused by human activity. They include, based on the motivation of actions:

- unintentional (accidental) threats caused by errors in the design of the information system and its elements, errors in the actions of personnel, etc.;
- deliberate (intentional) threats related to the selfish, ideological or other aspirations of people (intruders).

The sources of threats to the information system itself can be both external and internal.

5.2. The most significant threats to the information security of Company (ways of causing damage to the subjects of information relations) are:

- violation of the functionality of the components of the information system of the Company, blocking of information, violation of technological processes, disruption of timely problem solving;
- violation of the integrity (distortion, substitution, destruction) of information, software and other resources of Company, as well as falsification (forgery) of documents;
- violation of confidentiality (disclosure, leakage) of information constituting an official or commercial secret, as well as personal data.

5.3. Ways to implement unintentional artificial (subjective) threats to information security.

The Company's employees registered as legal users of the Company's information system or serving its components are internal sources of accidental impacts, because they have direct access to information processing processes and may make unintentional mistakes and violations of the current rules, instructions and regulations.

The main ways to implement unintentional artificial (subjective) threats to the security of Public information (actions committed by people accidentally, out of ignorance, inattention or negligence, out of curiosity, but without malicious intent):

- unintentional actions leading to partial or complete disruption of the functionality of the components of the information system of Company or the destruction of information or software and technical resources;
- careless actions leading to the disclosure of information of limited distribution or making it publicly available;
- disclosure, transfer or loss of access restriction attributes (passes, identification cards, keys, passwords, encryption keys, etc.);
- ignoring organizational restrictions (established rules) when working with information resources;

- design of systems, data processing technologies, software development with capabilities that pose a danger to the functioning of the information system of Company and information security;
- forwarding data and documents to the wrong address (devices);
- entering erroneous data;
- unintentional damage of media;
- unintentional damage to communication channels;
- illegal disconnection of equipment or change of operating modes of devices or programs;
- infecting computers with viruses;
- unauthorized launch of technological programs capable of causing the loss of operability of Corporate information system components or performing irreversible changes in them (formatting or restructuring of information carriers, data deletion, etc.);
- incompetent use, configuration, or improper disabling of security features.

5.4. Ways to implement deliberate artificial (subjective) threats to information security.

The main possible ways of deliberate disorganization of work, disabling components of the information system of Company, penetration into the system and unauthorized access to information (for selfish purposes, under duress, out of a desire for revenge, etc.):

- intentional actions leading to partial or complete disruption of the functionality of the components of the information system of Company or the destruction of information or software and technical resources;
- actions to disorganize the functioning of the information system of Company, theft of documents and media;
- unauthorized copying of documents and media, intentional distortion of information, entering incorrect data;
- disabling subsystems for ensuring the functioning of information systems (power supply, cooling and ventilation, communication lines and equipment, etc.);
- interception of data transmitted over communication channels;
- theft of industrial waste (printouts of documents, records, media, etc.);
- illegal acquisition of access control attributes (by agent means, using the negligence of users, by forgery, selection, etc.);
- unauthorized access to Corporate Information System resources from workstations of legal users;
- theft or opening of cryptographic protection ciphers of information;
- introduction of hardware and software bugs in order to secretly access information resources or disorganize the functioning of components of the Company's corporate information system;
- illegal use of equipment, software or information resources that violates the rights of third parties;
- the use of eavesdropping devices, remote photo and video shooting for unauthorized removal of information;

- interception of secondary electromagnetic, acoustic and other radiations of devices and communication lines, as well as active radiation leads to technical means not directly involved in information exchange (power supply networks).

5.5. Ways to implement the main natural threats to information security:

- failure of information systems equipment and equipment ensuring its functioning;
- failure or inability to use communication lines;
- fires, floods and other natural disasters.

5.6. The information security system of the Company should be based on assumptions about the following possible types of violators in the system (taking into account the category of persons, motivation, qualifications, availability of special means, etc.):

- incompetent (inattentive) user is an employee of the Company (or a subdivision of another organization that is a legal user of the Company's information system) who may attempt to perform prohibited actions, access protected resources of the information system in excess of his authority, enter incorrect data, violate rules and regulations for working with information, etc., acting by mistake, incompetence or negligence without malicious intent and using only regular (provided) funds at the same time;
- amateur - an employee of the Company (or a subdivision of another organization who is a registered user of the Company's information system) who tries to violate the protection system without selfish goals or malicious intent or for self-affirmation. To overcome the protection system and commit prohibited actions, he/she can use various methods of obtaining additional access rights to resources, shortcomings in the construction of the protection system and the regular means available to him/her (unauthorized actions by exceeding his/her authority to use permitted means). In addition, he/she may try to use additional non-standard instrumental and technological software tools, independently developed programs or standard additional technical tools;
- internal attacker is an employee of the Company (or a subdivision of another department registered as a user of the system) acting purposefully out of selfish interests or revenge for an offense, possibly in collusion with persons who are not employees of the Company. He/she can use the whole set of methods and means of hacking the security system, including agent methods, passive means (technical means of interception), methods and means of active influence (modification of technical means, connection to data transmission channels, introduction of program bugs and the use of special instrumental and technological programs), as well as combinations of influences, both from within and from outside of Company;
- external attacker is an outsider acting purposefully out of self-interest, revenge or out of curiosity, possibly in collusion with other persons. He/she can use the whole set of methods and means of hacking the security system, including agent methods, passive means (technical means of interception), methods and means of active influence (modification of technical means, connection to data transmission channels, the introduction of program bugs and the use of special instrumental and

technological programs), as well as combinations of influences, both from within and from outside of Company.

Chapter 6. Measures, methods and means to ensure the required level of security of information resources

6.1. All measures to ensure the security of the Company's information system are divided into:

6.1.1. Legal (legislative) protection measures.

Legal protection measures include laws, decrees and regulations in force in the country that regulate the rules for handling information, enshrining the rights and obligations of participants in information relations in the process of its processing and use, as well as establishing liability for violations of these rules. Legal protection measures are mainly proactive, preventive in nature and require constant explanatory work with users and service personnel of the Company's information system.

6.1.2. Technological protection measures.

This type of protection measures includes technological solutions and techniques based on the use of certain types of redundancy (structural, functional, informational, temporary, etc.) and aimed at reducing the possibility of employees making mistakes and violations within the rights and powers granted to them. An example of such measures is the use of procedures for double entry of responsible information, initialization of responsible operations only if there is agreement of several persons, procedures for checking the details of outgoing and incoming messages, etc.

6.1.3. Organizational (administrative) protection measures.

Organizational (administrative) protection measures are organizational measures that regulate the processes of functioning of the data processing system, the use of its resources, the activities of service personnel, as well as the procedure for user interaction with the system in such a way as to most complicate or exclude the possibility of implementing security threats or reduce the amount of losses in the event of their implementation.

6.2. Regulation of access of employees to the use of information resources.

Within the framework of the permissive admission system, it is established: who, to whom, what information and what type of access can be provided and under what conditions.

The access of users to work with the information system of the Company and access to its resources should be strictly regulated. Any changes in the composition and powers of users of subsystems must be made in accordance with the established procedure, according to the rules for granting user access.

The main users of information in the Corporate Information System are employees of the Company's structural divisions. The level of authority of each user is determined individually. Each employee enjoys only the rights prescribed to him/her in relation to the information with which he needs to work in accordance with his/her official duties. The extension of access rights and the provision of access to additional information

resources, without fail, must be coordinated with the division of the Company responsible for the information support of this resource.
6.3. Regulation of maintenance processes and modification of hardware and software resources.

The system resources to be protected (documents, tasks, servers, programs) are subject to strict accounting (based on the use of appropriate forms or specialized databases).

In order to maintain the information security regime, the hardware and software configuration of the automated workplaces of the Company's employees, from which access to the resources of the corporate information system is possible, must correspond to the range of functional responsibilities assigned to these users. All information input and output devices that are not used in work at the workplaces of employees working with confidential information should be turned off if possible, software tools that are not necessary for work and data from disks should also be deleted. Additional information exchange devices may be used only in exceptional cases and only as a temporary means. The installation of such devices must be coordinated with the information security units of the Company.

Software tools that have only been received from the Information Technology Department should be installed and used in the components of the corporate information system and at the workplaces of users. The use of software that has not been verified and has not been registered in the Company should be prohibited.

Special software can be used to solve special tasks of assessing the security of the Company's information network and building an information security system in the Company's network.
6.4. Ensuring and monitoring the physical integrity (immutability of configuration) of hardware resources.

The equipment of the corporate information system used for access to confidential information, to which the access of maintenance personnel is not required during operation, after commissioning, repair and other works related to access to its components, must be closed and sealed. Day-to-day control over the integrity and compliance of seals should be carried out by the users of the equipment, periodic control - by the Security Service of the Company.
6.5. Users of the Company's information system, as well as management and service personnel should be familiar with their level of authority, as well as organizational and administrative, regulatory, technical and operational documentation defining the requirements and procedure for processing information in the Company.

Chapter 7. Information security units

7.1. The direct organization of information security work is assigned to the Security Service and the Information Technology Department of the Company.
7.2. The main functions of information security units:

- implementation of the information security policy of the Company;
- organization of events and coordination of work of all divisions of the Company on complex information protection;

- analysis of the current state of information security;
- development of regulatory documents related to information security issues, including documents regulating the activities of users of the Company's information system;
- formation of information security requirements and protection system in the process of creation and further development of existing components of the Company's information system;
- participation in the design of protection systems and programs, their testing and commissioning;
- ensuring the functioning of established information security systems, including the management of cryptographic systems;
- distribution among users of the necessary attributes of access to the resources of the information system of the Company;
- monitoring the functioning of the protection system and its elements;
- checking the reliability of the protection system;
- development of measures to neutralize models of possible attacks;
- training of users and service personnel in the rules of safe information processing;
- providing methodological assistance to the Company's employees in matters of information security;
- control over the actions of database administrators, servers and network devices;
- monitoring of users' compliance with the established rules for handling information;
- monitoring and evaluation of the effectiveness of the measures taken and the means of information protection used;
- taking measures in case of attempts of unauthorized access to information resources and components of the system or in case of violations of the rules of operation of the protection system;
- collection, accumulation, systematization and processing of information on information security issues;
- conducting internal inspections and investigations into violations of information security requirements.

7.3. To solve the tasks assigned to them, information security units have the right to:

- receive information from users of the Company's information system on any aspects of information security;
- stop processing information if there is an immediate threat to it;
- participate in the elaboration of technical solutions for information security issues in the design and development of new information technologies;
- participate in the tests of the developed information technologies on the issues of assessing the quality of the implementation of information security requirements;
- monitor the activities of users of the Company's information system on issues of information security;
- initiate the prosecution of employees who commit violations of information security requirements.

Chapter 8. Responsibility for violations of requirements for information security

The Company's employees are personally responsible for violations of the established information processing procedure, rules for storing, using and transferring protected system resources at their disposal. Each employee, when applying for a job, must sign an obligation to comply with and be responsible for violating the established requirements for the preservation of official and commercial secrets, as well as the rules for working with information in the Company. The measure of responsibility of the Company's employees for actions committed in violation of the established rules and requirements of information security is determined by the damage caused, the presence of malicious intent and other factors at the discretion of the Company's management.

Chapter 9. Organizational and legal regime of ensuring information security

The introduction of the organizational and legal regime of information security in the Company provides for development and approval of the necessary regulatory documents:

- defined by the legislation of the Republic of Kazakhstan regarding information security and mandatory for execution;
- regarding the information constituting the Company's commercial secret (the regulation on commercial secrets, the list of information constituting the Company's commercial and official secrets);
- orders of the Company's management regarding the security regime.

Chapter 10. Final provisions

10.1. Issues not covered by this Policy shall be regulated in accordance with the legislation of the Republic of Kazakhstan.
10.2. If the Policy contradicts the requirements of the legislation of the Republic of Kazakhstan, the Policy is subject to application in the part that does not contradict the legislative and regulatory legal acts of the Republic of Kazakhstan.
10.3. The requirements of the Policy apply to all employees of the Company. Compliance with the requirements of the Policy by employees of departments is ensured by the heads of departments and supervising managers.
10.4. This Policy shall come into force from the date of approval by the Management Board of the Company.
10.5. Amendments and additions to this Policy shall be made by the decision of the Management Board of the Company.