Information security policy (hereafter referred to as the Policy) is part of the information security management system (ISMS) of GNC-ALFA CJSC (hereafter referred to as the Company).

The Policy defines high-level goals, content and main areas of activities to ensure the Company's information security. The Policy provisions are fundamental and are detailed in relation to one or more areas of information security, types and technologies of the Company's activities and in other regulatory documents on information security.

The Policy applies to all information assets of the Company, regardless of where they are installed and used. The Policy requirements are mandatory for compliance by all personnel of the Company, as well as personnel of third-party organizations with access to the Company's information assets.

The Policy has been developed in accordance with the provisions of international standards and recommendations on information security, applicable norms of international law, legislation of the countries where the Company operates, including the country of residence of the Company, and the internal regulatory framework of the Company, including:

- The concept of information security and risk management of the Company;
- Policy for processing personal data in the Company;
- ISO/IEC 27001:2022; Information Security, Cybersecurity and Personal Data Protection; Information Security Management System; Requirements
- PCI DSS 4.0 standard requirements

This Policy is a first-level corporate information security document.

Documents detailing the provisions of the corporate Policy in relation to one or more areas of information security, types and technologies of the Company's activities are the Personal Data Processing Policy, the ISMS Policy and Guidelines, as well as regulations, which are documents on information security of the second level, are drawn up as separate internal regulatory documents of the Company, developed, agreed upon and approved in accordance with the procedure established by the Company.

1. GENERAL PROVISIONS

The Policy was developed to define the basic principles and areas in the field of information security, cybersecurity and covers all business processes, information systems and documents, the owner and user of which is the Company.

The purpose of information security and cybersecurity management activities in the Company is to protect subjects of information relations from the possible infliction of tangible material, physical, moral or other damage to them through accidental or intentional unauthorized interference in the functioning of the information system or unauthorized access to information circulating in the Company (in its systems) and its illegal use.

The main objects of protection of the information security system in the Company are:

- information resources containing trade secrets, confidential information, including personal data of individuals, information of limited distribution, as well as publicly disseminated information necessary for the work of the Company, regardless of the form and type of its presentation;
- The Company's employees who are users of the Company's information assets and systems;
- special controlled areas, which include the following groups of resources: main information servers and computer facilities on which limited distribution information is processed and stored; network equipment and servers that support the operation of critical systems; file servers on which data is stored, including backup data; systems and communication equipment critical for the Company's activities that provide external communications; information security systems and means, facilities and premises in which such systems are located;
- information assets of Customers and Partners entrusted to the Company;
- personal data entrusted to the Company.

The objectives of information security management activities in the Company are:

- categorizing information assets by dividing them into critical and non-critical based on the maximum level of criticality of the information stored and processed within them;

- timely identification of potential threats to information security and vulnerabilities in the Company's information assets;
- eliminating or minimizing identified threats;
- preventing information security incidents or minimizing their consequences.

The main measures to protect the confidentiality, integrity and availability of the Company's information assets are:

- network security management;
- management of vulnerabilities and security policies;
- end device security management;
- identity and access management;
- information security incident management;
- management of cryptographic security measures;
- management of anti-virus protection tools;
- ensuring the physical security of information assets;
- ensuring security when interacting with counterparties;
- training and raising personnel awareness on information security issues;
- ensuring the security of Internet resources.

The set main goals of protection and the solution of the above tasks are achieved:

- strict accounting of all information assets subject to protection
- regulation of the processes of processing information subject to protection, using automation tools and the actions of employees of the Company's structural divisions, using, as well as the actions of personnel performing maintenance and modification of the Company's software and hardware, on the basis of organizational and administrative documents approved by the CEO of the Company on issues of ensuring information security;
- completeness, real feasibility and consistency of the requirements of the Company's organizational and administrative documents on issues of ensuring information security;
- appointment and training of officials (employees) responsible for organizing and implementing practical measures to ensure information security and its processing processes;
- providing each user of the Company's information asset with the minimum access powers necessary to perform their functional responsibilities;
- clear knowledge and strict compliance by all employees using and maintaining the Company's hardware and software with the requirements of organizational and administrative documents on information security issues;
- personal responsibility for their actions of each employee participating, within the framework of their functional duties, in information processing processes and having access to the Company's information assets;
- implementation of technological processes for information processing using complexes of organizational and technical measures to protect software, hardware and data;
- taking effective measures to ensure the physical integrity of technical means and continuously maintaining the required level of security of the Company's information assets;
- the use of physical and technical (hardware and software) means of protecting the Company's assets;
- delimitation of information flows of different levels of confidentiality, as well as prohibition of the transfer of information of limited distribution over unsecured communication channels;
- effective control of compliance with information and security requirements by employees of the Company's divisions;
- legal protection of the Company's interests 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;
- carrying out continuous analysis of the effectiveness and sufficiency of the measures taken and the

information protection means used, development and implementation of proposals to improve the system for protecting the Company's information assets.

2. PRINCIPLES AND REQUIREMENTS FOR PROVIDING INFORMATION SECURITY

Legality. The Company's information security measures must comply with the applicable norms of international law, the legislation of the countries where the Company operates, including the country of residence of the Company, and the internal legal framework of the Company.

Business orientation. Information security is considered as a process of supporting business processes in the Company. Any measures to ensure information security should not entail serious obstacles to the Company's activities;

Comprehensiveness and coordination. Governing bodies, structural divisions and personnel of the Company should take part in ensuring information security. To ensure information security, it is necessary to coordinate the use of all available legal, organizational and technical measures, which together cover all significant channels for the implementation of information security threats. Responsibility for organizing and coordinating information security activities should be assigned to a specially authorized person.

Competence and specialization. Decisions affecting the level of information security support, including the choice of information security and information security tools, distribution of personnel responsibilities, information interaction with business partners, etc., must be agreed upon with the authorized information security person.

Continuity. Ensuring information security should be a continuous process, carried out at all stages of processes and all stages of the life cycle of an information system. The information security process should include the stages of planning, implementation, control and analysis, support and improvement of the system.

Awareness. The Company's personnel, as well as employees of external organizations – the Company's clients and counterparties – must be aware of the information security requirements to the extent required to perform their official duties. Regulatory documents on information security must fully explain the subject, obligations and measures of responsibility, both on the part of the Company and on the part of the informed person or organization. The level of personnel awareness in the field of information security is subject to regular monitoring by authorized information security officials.

Knowing your clients, employees and contractors. The Company must have the information necessary to provide information security about its clients, employees and counterparties. This information must be kept up to date and used when making information security decisions.

Echeloning. To increase the level of security, the protection system must be built in echelons. Detection and counteraction to information security threats should be ensured by independent levels (echelons) of protection so that compromise of one level does not lead to compromise of the entire system of protective measures. Along with protecting the Company's perimeter from external threats, the organization and protection of internal perimeters in the locations of critical information assets must be ensured. The information security system must include independent echelons of protection at the levels of: physical access to data storage media, servers, backup systems, and other equipment; access to interconnections and the Company's local computer network; access to operating systems; access to applications and data.

Special measures must be taken to protect information security management, monitoring, accounting and audit systems.

Priority of prevention measures. The Company's information security process should be focused on prevention and timely identification of prerequisites for the emergence and implementation of information security threats.

Minimization of privileges, separation of powers. Each user should be provided with the minimum rights to access information assets necessary to perform their job duties. The rights of one user should not provide the opportunity to violate information security.

Minimum total protection resource. In all possible cases, personalized means of identification and authentication of information system users should be used.

Complete control. The information security system must ensure the implementation of an explicitly defined security policy with each access to each protected information asset.

Availability of services. Information assets must be available to legal users within the time specified by regulatory documents. For critical information assets, plans must be developed to ensure business continuity and recovery from interruptions

Centralization of management. Organizational and technical measures to ensure the Company's information security must be centralized as much as possible and ensure the functioning of the security system according to uniform legal, organizational, functional and methodological principles. Centralization of information security management should ensure maximum personnel awareness, validity, efficiency and minimal costs for coordinating decisions.

Flexibility of control and application. The information security system must be rebuilt with minimal time and resources when business processes and security requirements change, and also provide protection not only from known information security threats, but also from threats that may appear in the future.

Validity and economic feasibility. The capabilities and means of protection used must be implemented at the appropriate level of development of science and technology, justified from the point of view of a given level of security and must comply with the requirements and standards; the relationship between the cost of their implementation and the possible damage from the implementation of threats must be taken into account.

3. ORGANIZATION OF ACTIVITIES TO ENSURE INFORMATION SECURITY

The Company ensures the creation and operation of an information security management system, which is part of the Company’s overall management system designed to manage the process of ensuring information security.

The Company develops internal procedures for the creation, collection, storage and processing of information in the Company’s information systems. The Company monitors the processes of creation, storage and processing of information and access to it using information system mechanisms and technical security means. Access to information created, stored and processed in the Company’s information systems is provided to employees in accordance with their functional responsibilities in accordance with the principle of least privilege.

Participants in the Company's information security management system are:

1) Management;
2) Information Security Committee;
3) information security division;
4) information technology division;
5) security division;
6) HR division;
7) legal support division of the Company;
8) internal audit division;

Management approves a list of protected information, including information on data constituting an official, commercial or other secret protected by law (hereinafter referred to as protected information), and the procedure for working with protected information. It also approves internal documents regulating the information security management process, the procedure and frequency of revision.

The Company creates the Information Security Committee, which includes representatives of the information security division, the information technology division, and, if necessary, representatives of other divisions of the Company. The CEO or the first deputy of the CEO is appointed as a head of the Information Security Committee, who oversees the activities of the information security division.

The Information Security Committee periodically monitors information security activities and activities to identify and analyse threats, counter attacks and investigate information security incidents at least once a year. The process of monitoring information security activities, activities to identify and analyse threats, as well as countering attacks should include a report on identifying, analysing threats and countering attacks based on data

provided by the information security division on the number of threats identified, measures taken and information security incidents that occurred. Monitoring activities to investigate information security incidents includes assessing the consequences of incidents, indicating the causes and action plans to prevent or reduce the impact of information security incidents.

The CEO carries out strategic planning and coordination of the activities of all divisions of the Company to organize and maintain an appropriate level of information security.

The head of the information security division ensures the development, implementation and improvement of documented standards and procedures in the field of information security and information security risk management.

The information security division ensures timely analysis of information about information security incidents, which should include disclosure of the circumstances of the event in which the implementation of an information security incident became possible, and, if necessary, generates recommendations for the implementation of protective measures. The division is responsible for categorizing information assets by dividing them into critical and non-critical based on the maximum level of criticality of the information stored and processed within them.

The information technology division ensures compliance with established requirements for the continuity of operation of the information infrastructure, confidentiality, integrity and availability of data from the Company's information systems (including redundancy and (or) archiving and backup of information) in accordance with the Company's internal regulatory documents, and also ensures compliance with information technology requirements security in the selection, implementation, development and testing of information systems.

The security division implements physical and technical security measures, including organizing access control and internal security policy, and also carries out preventive measures aimed at minimizing the risks of information security threats when hiring and dismissing the Company's employees.

The HR division ensures that the Company's employees, as well as persons involved in work under a service agreement, trainees, and interns sign obligations on non-disclosure of confidential information and consent to the processing of personal data, and also participates in organizing the process of raising awareness of the Company's employees in the field information security.

The legal division carries out legal examination of internal regulations and internal documents of the Company on issues of ensuring information security.

The internal audit division assesses the state of the Company's information security management system when conducting audits.

Business owners of information systems or subsystems are responsible for compliance with information security requirements when creating, implementing, modifying, providing products and services to customers, and also forming and maintaining the relevance of access matrices to information systems.

Heads of the Company's structural divisions ensure that employees are familiar with the Company's internal regulatory documents containing information security requirements, and are also responsible for ensuring that subordinate divisions comply with information security requirements and implement protective measures when developing new products, services, business applications, business processes and technologies.

4. INFORMATION SECURITY RISK MANAGEMENT

To ensure and effectively manage information security, the Company provides information security risk management, including:

- analysis of the impact on the Company's information security of technologies used in the Company's activities, as well as events external to the Company;
- identifying information security issues, analysing the causes of their occurrence and forecasting their development;
- identification of information security threat models;
- identification, analysis and assessment of information security threats significant to the Company;
- identification of possible negative consequences for the Company resulting from the manifestation of

information security risk factors, including those associated with a violation of the security properties of the Company's information assets;

- identification and analysis of risk information security events;
- assessing the magnitude of information security risks and identifying among them risks that are unacceptable to the Company;
- processing the results of information security risk assessment based on operational risk management methods;
- optimization of information security risks through the selection and application of protective measures that counteract the manifestations of risk factors and minimize possible negative consequences for the Company in the event of risk events;
- assessment of the impact of protective measures on the goals of the Company's core activities;
- assessment of the costs of implementing protective measures;
- consideration and assessment of various options for solving information security issues;
- developing risk management plans that provide for various protective measures and options for their application, and choosing from them the one whose implementation will have the most positive impact on the goals of the Company's core activities and will be optimal in terms of costs incurred and the expected effect;

5. INFORMATION SECURITY THREATS

The entire set of potential threats to information security is divided into three classes according to the nature of their occurrence: anthropogenic, technogenic and natural.

The emergence of anthropogenic threats is caused by human activity. Among them, one can highlight threats arising as a result of both unintentional (involuntary) actions: threats caused by errors in the design of the information system and its elements, errors in the actions of personnel, etc., and threats arising due to deliberate actions associated with selfish, ideological or other aspirations of people.

The emergence of technogenic threats is caused by the impact on the threat object of objective physical processes of a technogenic nature, the technical state of the environment of the threat object or itself, not directly caused by human activity.

Technogenic threats may include failures, including operational failures, or destruction of systems created by man.

The emergence of natural (environment) threats is caused by the impact on the threat object of objective physical processes of a natural nature, natural phenomena, states of the physical environment that are not directly caused by human activity.

Natural (environment) threats include meteorological, atmospheric, geophysical, geomagnetic, etc., including extreme climatic conditions, meteorological phenomena, and natural disasters.

Sources of threats to the Company's infrastructure can be both external and internal.

6. INFORMAL MODEL OF POSSIBLE INFORMATION SECURITY VIOLATORS

In relation to the Company, violators can be divided into external and internal violators.

Violator is a person who has attempted to perform prohibited operations (actions) by mistake, ignorance or knowingly with malicious intent (for selfish interests) or without it (for the sake of game or pleasure, for the purpose of self-affirmation, etc.) and using various opportunities for this, methods and means.

The system for protecting the Company's information assets is based on assumptions about the following possible types of violators (taking into account the category of persons, motivation, qualifications, availability of special means, etc.):

"Inexperienced (inattentive) employee" is an employee of the Company (or another organization registered as a user in the company's information systems) who may attempt to perform prohibited operations, access protected Company resources in excess of their authority, enter incorrect data, etc. actions due to error, incompetence or negligence without malicious intent and using only standard hardware and software (available to them).

"Amateur" is an employee of the Company (or another organization registered as a user in the company's information systems) trying to overcome the defense system without selfish goals or malicious intent, for self-affirmation or out of "sporting interest." To overcome the security system and commit prohibited actions, he can use various methods of obtaining additional access rights to resources (names, passwords, etc. of other users), deficiencies in the construction of the security system and standard (installed on the workstation) programs (unauthorized actions by exceeding their authority to use authorized means) available to them. In addition, they may try to use additional non-standard tools and technological software (debuggers, utility utilities), independently developed programs or standard additional technical tools.

"Scammer" is an employee of the Company (or another organization registered as a user in the company's information systems) who may attempt to perform illegal technological operations, enter false data and similar actions for personal gain, under duress or out of malicious intent, but using only standard (installed on the workstation and accessible to them) hardware and software on their own behalf or on behalf of another employee (knowing their name and password, using their short-term absence from the workplace, etc.).

"Internal Intruder" is an employee of the Company, registered as a user in the company's information systems, acting purposefully out of selfish interests or revenge for an insult, possibly in collusion with persons who are not employees of the Company. They can use the entire range of methods and means of hacking a security system, including undercover methods of obtaining access details, passive means (technical means of interception without modifying system components), methods and means of active influence (modifying technical means, connecting to data transmission channels, introducing implant tools and the use of special instrumental and technological programs), as well as a combination of influences both from within and from the outside, that is from public networks.

Malicious Insider may be a person from the following categories of Company personnel:

- registered end users in the company's information systems (Company's employees);
- employees not allowed to work with the Company's information assets;
- personnel servicing technical means of information assets (engineers, technicians);
- employees of software development and support divisions (application and system programmers);
- building maintenance personnel (cleaners, electricians, plumbers and other workers who have access to buildings and areas where critical information systems and assets are located);
- employees of the information security and IT divisions;
- managers at various levels.

"External Violator (Intruder)" is an outsider or former employee of the Company or other organization, acting purposefully out of selfish interests, revenge or curiosity, possibly in collusion with other persons. They can use the entire range of radio-electronic methods of violating information security, methods and means of hacking security systems characteristic of public networks (especially networks based on the IP protocol), including remote injection of implant tools and the use of special instrumental and technological programs, using the existing weaknesses of the exchange protocols and the protection system of the Company's network nodes.

Categories of persons who may be external violators:

- fired employees of the Company;
- representatives of organizations interacting on issues of ensuring the life of the organization (energy, water, heat supply, etc.);
- visitors (invited representatives of organizations, citizens), representatives of companies supplying equipment, software, services, etc.;
- members of criminal organizations, intelligence officers or persons acting on their instructions;
- persons who accidentally or intentionally entered the Company's network from external (relative to the Company) telecommunications networks ("hackers").

Users and service personnel from among the Company's employees have the widest opportunities to carry out unauthorized actions, due to the fact that they have certain powers to access resources and good knowledge of information processing technology and protective measures. The actions of this group of people are directly

related to the violation of current rules and instructions. This group of violators poses a particular danger when interacting with criminal structures or intelligence services.

Fired workers can use their knowledge of work technology, protective measures and access rights to achieve their goals. The knowledge and experience acquired at the Company sets them apart from other sources of external threats.

Criminal structures represent the most aggressive source of external threats. To implement their plans, these structures can openly violate the law and involve the Company's employees in their activities with all the forces and means available to them.

Professional "hackers" have the highest technical qualifications and knowledge of software and hardware vulnerabilities. The greatest threat is posed when interacting with working and fired employees of the Company and criminal structures.

Organizations involved in the development, supply and repair of equipment and information systems pose an external threat due to the fact that they occasionally have direct access to information resources. Criminal structures and intelligence services can use these organizations to temporarily employ their members in order to gain access to protected information and information assets.

7. MONITORING THE EFFECTIVENESS OF THE PROTECTION SYSTEM

Monitoring the effectiveness of information protection is carried out with the aim of timely detection and prevention of information leakage through technical channels, due to unauthorized access to it, as well as the prevention of possible special influences aimed at destroying information and destroying information means.

Monitoring can be carried out both by dedicated information security employees and by competent organizations engaged for this purpose and licensed for this type of activity.

The effectiveness of information security measures is assessed using hardware and software controls for compliance with established requirements.

Monitoring can be carried out both using standard means of the information protection system from unauthorized access, and using special software monitoring tools.

8. AUDIT

The information security division must ensure and verify, through internal and external audits, the extent, correctness of implementation and efficiency of the instructions of this Policy and the internal regulations emanating from it, as well as ensure the implementation of established corrective measures in order to continuously improve the functioning.

9. RESPONSIBILITY FOR COMPLIANCE WITH THE POLICY

Responsibility for keeping the provisions of this Policy up to date, organizing coordination, implementation, and making changes to the processes of the Company's information security management system rests with the information security division.

The responsibility of the Company's employees for failure to comply with this Policy is determined by the relevant provisions included in employment contracts with the Company's employees, as well as the provisions of the Company's internal regulatory documents.

10. FINAL PROVISIONS

The requirements of this Policy may be supplemented and clarified by other internal regulatory documents of the Company.

In the event of changes in current legislation and other regulations, as well as the Charter of the Company, this Policy and changes to it apply to the extent that does not contradict newly adopted legislative and other regulations, as well as the Charter of the Company. In this case, the Responsible Division is obliged to immediately initiate the introduction of appropriate changes.

Changes to this Policy are made on a periodic and unscheduled basis:

- periodic changes to this Policy should be made to reflect changes in legislation and regulations, industry principles and technical regulations;

- unscheduled changes to this Policy may be made based on the results of an analysis of information security incidents, the relevance, sufficiency and effectiveness of information security measures used, the results of internal information security audits and other control measures.

Control over compliance with the requirements established by the Policy is assigned to the Information Security Committee.

Issues not regulated by the Policy are resolved in accordance with the legislation of the Republic of Armenia.