Ensuring the security of information assets when providing cloud services is determined by the management of GNC-ALFA CJSC (hereinafter referred to as the Company) as a key condition for the implementation of the Company's activities.

Ensuring information security is necessary for the Company to fulfil its contractual obligations to Clients, maintain the Company's competitiveness, ensure compliance with the requirements of the Company's Information Security Policy, legislation and regulatory framework, as well as build the Company's business reputation as a reliable Contractor and Partner.

This Policy in the field of the Information Security Management System for the provision of cloud services GNC-ALFA CJSC (hereinafter referred to as the Policy) applies to the Company's Information Security Management System for the provision of cloud services (hereinafter referred to as the ISMS).

INFORMATION SECURITY MANAGEMENT SYSTEM

The ISMS implemented in the Company, which complies with the requirements of international standards ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 and PCI DSS, is designed to ensure effective information security management when providing cloud services.

The scope of ISMS includes the Company's information assets and the processes operating within it, presented in the form of documented information, aimed at protecting the information assets of both Clients and the Company itself when providing cloud services.

The process approach to ensuring and managing information security, implemented in the Company to implement the provisions of this Policy, is documented in the format of the ISMS process model. Each process corresponds to specific internal regulatory documents of the Company regarding information security.

ISMS is a mechanism that provides the ability to share secure use of assets, carry out electronic transactions, and reduce information risks to an acceptable level.

As part of the implementation of ISMS processes, the following activities are fundamental:

- prevention of intentional or accidental unauthorized access to the Company's assets, including restricted information;
- ensuring the availability of assets for authorized users when they need them, timely detection and response to threats that may lead to unavailability of assets;
- preventing intentional or accidental, partial or complete unauthorized modification or destruction of data;
- development and change management of business continuity plans, procedures for restoring the Company's information systems after a disaster, procedures for data backup and recovery, procedures for protecting against malware and network attacks, access control, security incident management and incident reporting, change management and improvement;
- systematic review and improvement of ISMS.

The Company aims at:

- creation and constant maintenance in the Company of conditions under which risks associated with ensuring the security of the Company's assets, including those associated with the technical and operational specifications of cloud services, are constantly monitored and are at an acceptable level by ensuring the main aspects of information security: integrity, availability, privacy and confidentiality;
- defining guidelines for the implementation of information security measures, including those specific to cloud services, threats and information security risks in the relationship between consumers and cloud service providers;
- protection of confidential information (including when using cloud services) in accordance with the requirements of the current legislation of the Republic of Armenia, international legislation, industry requirements and best information security management practices, including information security threats and risks specific to cloud services;
- achieving compliance with applicable legislation on the personal data protection and contractual terms

agreed between the Company as a provider of cloud services and the processor of personal data, and its clients (consumers of cloud services);

- creation of a unified set of categories and information security measures that can be implemented by the company as a provider of cloud services and acting as a processor of personal data;
- ensuring continuity in the provision of cloud services to the Company;
- continuous improvement of the Company's ISMS in accordance with information security requirements and business requirements.

Information security goals in the Company are determined based on the following strategic objectives:

- stable operation of the Company, guaranteeing the achievement of its goals;
- ensuring the protection of assets belonging to the Company, its Clients and Partners;
- ensuring the personal data protection entrusted to the Company;
- ensuring compliance of the Company's activities with the requirements of the legislation of the Republic of Armenia, Armenian and international standards in the field of information security;
- acceptance and implementation of current requirements of the Company's Clients and Partners regarding information security;
- continuous improvement of the Company's ISMS in accordance with the requirements of international standards ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019 and PCI DSS.

Information security goals are achieved by:

- clear definition of requirements and expected results in the field of information security;
- implementation of a set of measures to protect information assets, developed on the basis of information security risk management;
- providing ISMS with the resources necessary for its real and effective functioning;
- conducting periodic assessments of effectiveness and efficiency in terms of fulfiling the requirements of this Policy and Goals in the field of information security;
- informing the Company's management about the results of the assessment for subsequent analysis and decision-making;
- taking corrective and preventive actions on an ongoing basis based on the results of internal audits or other relevant information for the purpose of continuous improvement;
- annual confirmation of compliance of the operating ISMS with the requirements of international standards ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 and PCI DSS with the results of control audits conducted by an independent certification body.

The management of GNC-ALFA CJSC takes responsibility for the implementation of this Policy and the strict implementation of the principles set out in it by all employees of the Company.

In order to maintain the relevance and effectiveness of the ISMS and its compliance with the conditions of its operation, the Company regularly reviews this Policy.

The Company may also initiate a revision of this Policy based on the results of risk analysis, audits of compliance with information security requirements, and implementation of changes in ISMS.