

Approved by
"APRICOT CAPITAL"
closed joint stock company
Executive Director's decision
No. AC HP 10/03/2026-1 of March 10, 2026
Executive Director Vachik Gevorgyan



"APRICOT CAPITAL" CLOSED JOINT-STOCK COMPANY

RULES ON THE SECURE USE OF THE SYSTEM

YEREVAN 2026

a.

1. General Provisions

1.1 Purpose and Scope

The Rules on the Secure Use of the System (hereinafter referred to as the “Rules”) of “Apricot Capital” CJSC (hereinafter referred to as the “Company”) establish the requirements for the secure use of software and information systems utilized within the framework of services provided by the Company.

The purpose of these Rules is to minimize the adverse impact of information security incidents, reduce the risks of unauthorized access to the Company’s information systems, and ensure the proper protection of non-public data.

1.2 Definitions and Interpretation

1.2.1 The following key terms shall have the meanings set forth below for the purposes of this Policy:

- **“Client”** means a person (including such person’s representative) who uses investment services and/or ancillary services and/or crypto-asset related services provided by the Company.
- **“System”** means a telephone application or the “Trading Platform (Beta)” module (the link to which is available on the website www.apricotcapital.am), constituting an electronic (network/internet-based) tool with a corresponding interface, through which Clients, upon obtaining access, may submit Orders for the execution of transactions, as well as receive information regarding submitted Orders, executed transactions, and other relevant information.
- **“Information Security Incident”** means an incident that actually compromises, or is likely to compromise, the integrity, availability, or confidentiality of the System or of information processed, stored, or transmitted by the System, or constitutes a breach of security rules, procedures, or policies, or a threat directed at the compromise of data integrity.

1.2.2 Terms not defined in these Rules shall have the meanings assigned to them under the legislation of the Republic of Armenia, including the Law of the Republic of Armenia “On the Securities Market,” as well as in the General Terms for the Provision of Brokerage (Dealer) and Custody Services and the General Terms for the Provision of Crypto-Asset Services of the Company.

1.2.3 The headings of individual provisions of these Rules are for reference purposes only and shall not affect the interpretation of their content.

2. Requirements for the Secure Use of the System

2.1 General Use

2.1.1 The Client shall use the System solely in accordance with the rules established by the Company.

2.1.2 The Client shall ensure that access to the System is restricted exclusively to authorized persons and shall prevent any unauthorized or improper use of the System.

2.2 Security

2.2.1 The Client is responsible for maintaining the confidentiality of all data, including usernames, passwords, PIN codes, security tokens, and other identification information.

2.2.2 When using the System, the Client must not disclose or otherwise make available their passwords or any other identification information to any third party (unauthorized person), including family members, friends, or colleagues.

2.2.3 The Client undertakes to take all necessary measures, including changing the password provided by the Company after accessing the System (including upon first access), and to exercise proper control to prevent unauthorized persons from accessing the Client's authorized email addresses or other means of communication, and/or the System, or from gaining access thereto.

2.2.4 The Client must immediately notify the Company of any suspected threat, loss, or theft of passwords.

2.2.5 The Client is obliged to access and use the System exclusively from devices protected by antivirus software.

2.2.6 The Client must avoid using the System over public or unsecured networks, except when additional security measures (e.g., VPN) are applied.

2.2.7 The Client must not attempt to bypass the security functions of the System or use the System for malicious or unlawful purposes.

2.3 Monitoring and Reporting

2.3.1 The Client is obliged to immediately notify the Company of any suspicious transactions in the System, any unauthorized access to the System, or any breaches of availability, integrity, or confidentiality, as well as any other issues of any kind.

2.3.2 The Client is obliged to send the Company a corresponding notification in the event of loss of the password for using the System and/or if the password becomes accessible to any third party in any manner.

3. Other Provisions

All other provisions of these Rules, where reference is made to the provision of crypto-asset services or to the General Terms for the Provision of Crypto-Asset Services, shall enter into force only from the moment the Company is granted the required authorization by the Central Bank of the Republic of Armenia to provide crypto-asset services in accordance with the Law of the Republic of Armenia “On Crypto-Assets.”