RULES ON HANDLING INFORMATION ABOUT CUSTOMERS

1. Objectives and scope

1.1. These rules are established on the basis of Article 19 (b) of Act no. 161/2002 on Financial Undertaking for the purpose of ensuring the protection of information about customers of ACRO securities hf. (hereinafter "*the Company*").

1.2. The objective of these rules is to ensure that the Company's employees handle the information they hold on the Company's clients in accordance with good business practices and the basic principles of data protection and privacy, as stipulated in Act no. 90/2018 on Data Protection and the Handling of Personal Information and in accordance with the confidentiality provisions of Article 58 of Act no. 161/2002 on Financial Undertakings.

1.3. The rules apply to the work of all employees, board members, auditors, contractors and any other party undertaking work on behalf of the Company (hereafter jointly referred to as employees). The rules cover all information in the Company's custody regarding clients' trading or private matters in whatever form the information may be.

2. Saving of information about clients

2.1. The Company saves information that clients provide when they begin trading with the Company, as well as information acquired later from clients.

2.2. Depending on circumstances, information about clients is saved digitally or on paper. Information in digital form shall be saved in a secure medium where security measures are taken. Documents on paper shall be filed in document storage suitable for saving documents. When deciding on the storage media of paper documents and digital data, consideration shall focus on the value of the content being preserved and its importance.

2.3. Information about clients shall be destroyed when there is no longer an objective reason to preserve it. Objective reasons for storing information may, for example, be that it is required by law or that the Company is still using the information for the same purpose that it was originally collected. When information is to be deleted, care must be taken to ensure that it is done securely and permanently.

3. Employees' access to documents

3.1. Employees' authorisation to access and utilise information about the Company's clients solely covers what is necessary for their work.

3.2. Employees' access to documents shall be monitored to ensure this goal, by, for example, controlling access to workstations, the allocation of access and passwords.

3.3. When in doubt, the Compliance Officer shall be consulted.

4. Confidentiality and dissemination of information

4.1. Employees shall be bound by an obligation of confidentiality concerning any information which they may become aware of in the course of their duties concerning the business dealings or private concerns of the Company's clients, cf. Article 58 of Act no. 161/2002 on

Financial Undertakings. The obligation of confidentiality shall remain after employment ceases.

4.2. Notwithstanding Article 4.1, employees may provide information about clients:

4.2.1. based on a clear statutory duty to do so;
4.2.2. if a legitimate request comes from the client involved, the client's guardian or agent; or
4.2.3. if a legitimate request comes from public authorities, such as the police or the Financial Supervisory Authority of the Central Bank of Iceland.

4.3. Notwithstanding the above, the Company may, on its own initiative, need to disseminate information, for example, as a mandatory notification party, based on current provisions of law.

4.4. A request to disseminate information about clients to a third party shall be in writing. In doubtful cases, the Compliance Officer shall make a decision on the dissemination of information in consultation with the CEO.

4.5. If information is shared with a third party on the basis of the aforementioned authorisations, the employee shall remind the recipient that he/she is bound by a duty of confidentiality in accordance with Article 58 of Act no. 161/2002.

5. Clients' right to information

5.1. The Company's clients can request to know which information about them the Company has processed and the purpose of that processing.

5.2. Such a request shall be in writing, logically supported and objective, and sent to the Compliance Officer, who acts as an intermediary in the handing over of the documents. The Compliance Officer may reject the customer's request if the delivery of the information is contrary to the Company's principles of personal data protection and confidentiality pursuant to Article 58 of Act no. 161/2002 on Financial Undertakings.

6. Security measures

6.1. The Company is responsible for ensuring that the processing of personal data complies with laws and regulations and takes appropriate security measures to ensure this is so.

6.2. All information regarding clients' business or private matters shall be handled with the utmost caution to ensure that it is not lost or falls into the hands of unauthorised parties. Particular care shall be taken in its preservation, photocopying, transmission, computer registration and destruction.

6.3. Digital storage of data shall be in a secure medium, where security measures are in accordance with requirements in each case. In selecting security measures, consideration shall be given to the risk of the processing and the nature of the data to be protected.

7. Supervision

7.1. An internal auditor is responsible for ensuring that these rules are implemented.

8. Entry into force and publication

8.1. These rules enter into force once they have been signed by the Board of Directors and shall be published on the Company's homepage.

Approved by the Board of Directors of ACRO Securities hf. on 10 August 2021.

Reviewed and approved by the Board of Directors of ACRO Securities hf. on 6 July 2023.

Revised and approved by the Board of Directors of ACRO Securities hf. on 26 September 2024.