SBERBANK OF RUSSIA

APPROVED BY
A Resolution of Sberbank Executive Board
dated September 20, 2023
Minutes No. 711/61a

September 20, 2023 **No. 4757-3**

Sberbank POLICY
on Countering Illegitimate Use of Insider Information and Market Manipulation
Version 3

Moscow
2023

CONTENTS

1. General Provisions

1.1. This Sberbank Policy on Countering Illegitimate Use of Insider Information and Market Manipulation (hereinafter, the Policy) has been developed in accordance with Federal Law No. 224-FZ dated July 27, 2010 'On Counteracting the Illegitimate Use of Insider Information and Manipulation of the Market, and on Making Amendments to Separate Legislative Acts of the Russian Federation' (hereinafter, 224-FZ) /1/ and statutory regulations of the Russian Federation (hereinafter, the RF), subject to internal regulatory documents (hereinafter, the IRDs) of Sberbank (hereinafter, the Bank).

1.2. The requirements of this Policy for use of information on financial instruments of the Bank, its customers and counterparties, and transactions therewith that is not publicly available and illegitimate use or disclosure of which may materially affect the market value of financial instruments of the Bank and/or its customers and counterparties, shall apply to any members of the Supervisory Board of the Bank, all employees of the Bank, the Bank's relationships with its shareholders, customers, counterparties, as well as bidding process organizers and government authorities.

1.3. This Policy makes part of the Internal Control Rules for prevention, identification and suppression of the illegitimate use of insider information and/or manipulation of the market at Sberbank (hereinafter, the ICR) /8/.

1.4. Any organizations in which the Bank is a member or a shareholder, where such subsidiaries are subject to 224-FZ, shall develop their own regulatory documents on protecting insider information and countering market manipulation in accordance with the principles and standards of this Policy.

1.5. According to the requirements of 224-FZ[1], the Bank may act as:

1.5.1. a securities issuer

1.5.2. a credit institution (the Bank acting as a third-party insider)

1.5.3. a professional securities market participant or an entity that carries out transactions with financial instruments, foreign currencies, and/or commodities for the benefit of its customers and that has obtained insider information from its customers

1.5.4. an entity entitled to directly or indirectly (through controlled entities) control at least 25 percent of votes in the supreme management body of entities specified in Clauses 1, 3, 4 of Article 4 of 224-FZ, as well as by virtue of ownership of equity (interest) in the charter capital of entities specified in Clauses 1, 3, 4 of Article 4 of 224-FZ having access to insider information pursuant to federal laws, its constituent documents or its internal documents

1.5.5. an entity with access to the drafting and/or sending of a voluntary, mandatory or competing securities acquisition offer, a notice of the right to request a securities buyout, or a securities buyout request in accordance with Chapter XI.1 of the Federal Law dated December 26, 1995 No. 208-FZ, On Joint-Stock Companies /2/

2. Goals and Objectives

2.1. The goal of this Policy is to protect the legitimate interests of shareholders and investors, prohibit and prevent any actions by the Bank, the Bank's employees, members of the Supervisory Board of the Bank, customers or counterparties of the Bank that are aimed at illegitimate use of insider information or market manipulation.

[1] Article 4, 224-FZ

2.2. The main objectives of this Policy are to:

2.2.1. strengthen the trust in the Bank of its customers and counterparties, including potential ones, and to ensure fair pricing for financial instruments of the Bank and the Bank's customers

2.2.2. ensure compliance with best practices in order to maintain high reputation of the Bank

2.2.3. provide the Bank's employees and members of the Supervisory Board of the Bank with general information on the measures taken by the Bank to protect insider information of the Bank, Bank's customers and counterparties and counter market manipulation

2.2.4. determine the procedure for access to insider information and the rules for protecting its confidentiality

2.2.5. verify compliance with 224-FZ and this Policy by the Bank, the Bank's employees, members of the Supervisory Board, customers and counterparties of the Bank

2.2.6. determine the conditions for unimpeded and effective verification of compliance with 224-FZ and this Policy at the Bank by any officers responsible for verification of compliance with the applicable law.

3. Potential Risks Inherent in Illegitimate Use of Insider Information and Market Manipulation

In case of violation of 224-FZ, the Bank, its customers, counterparties, employees of the Bank, or members of the Supervisory Board of the Bank may incur the following types of risk:

3.1. regulatory risk

3.2. legal risk

3.3. reputational risk

3.4. operational risk

4. Classification of Insider Information of the Bank and the List of the Bank's Insiders

4.1. Insider Information Criteria

4.1.1. Pursuant to 224-FZ, insider information includes precise and specific information that has not been made public (including any information constituting a commercial secret, official secret, banking secret, communication secret (as regards postal money transfers) or any other secret protected by law), distribution of which can have a substantial impact on the prices of financial instruments, foreign currencies and/or commodities (including information concerning one or more issuers of issue-grade securities, one or more asset management companies of investment funds, mutual investment funds and non-governmental pension funds or one or more financial instrument(s), foreign currency(ies) and/or commodity(ies)).

4.1.2. The list of the Bank's insider information shall be approved by an order of the Bank's CEO and Chairman on Executive Board, and shall include:

4.1.2.1. insider information the list of which is approved by a regulatory act of the Bank of Russia/5/ (hereinafter, the Standard List)

4.1.2.2. insider information included in the Bank's proprietary list of insider information compiled subject to the Bank's operating specifics (hereinafter, the Proprietary List).

4.1.3. To be included in the Proprietary List of Insider Information, such information must meet all of the criteria specified below:

4.1.3.1. it should apply to the Bank as an entity specified in sub-paragraph 1.5.1. and sub-paragraph 1.5.3. of the Policy

4.1.3.2. it should not be included into the Standard List

4.1.3.3. if disclosed, it could have a material effect on the prices of financial instruments (stocks, bonds or any other financial instruments)

4.1.3.4. if disclosed (in cases stipulated by the Bank) to an unlimited number of persons, it would ensure a fair pricing for the Bank's financial instruments, an equal footing for investors and a strengthening of investors' trust in the Bank's financial instruments.

4.1.4. The Proprietary List and any amendments thereto shall be developed by the Compliance Division of Central Head Office (hereinafter, CD CHO) based on information obtained from the Bank's units and collegial bodies.

4.1.5. Employees of the Bank's units and members of its collegial bodies independently determine information that is not included in the Standard and Proprietary Lists, but has features of insider information, and bring such information and supporting documents (if any) to the attention of the CD CHO in an official manner with the provision of a reasoning on the need to include the attached information in the Proprietary List.

4.1.6. Upon receipt of information to be included in the Proprietary List, the CD CHO organizes, in accordance with the procedure established by the Bank, the approval of the updated Proprietary List, as well as the Procedure for Disclosing Insider Information Not Included in the Standard List of insider information approved by the Bank of Russia (if necessary).

4.1.7. The Bank's list of insider information is subject to prompt disclosure on the Internet on the Bank's official website[2] according to the procedure established by the Bank.

4.2. **The Bank Insiders List**

4.2.1. The Bank maintains the Insiders List in accordance with 224-FZ. The procedure for its maintenance is determined in the Bank's process IRDs and OADs related to insider information protection.

4.2.2. The Insiders List includes individuals and legal entities in accordance with applicable law.

[2] The Bank's list of insider information is disclosed at: https://www.sberbank.com/ru/compliance/im

4.2.3. The Bank Insiders List shall be maintained continuously in real time.

4.2.4. The insiders list of the Bank shall be maintained and updated by CD CHO together with Compliance Units at Regional Banks (hereinafter, CU RB). The Insiders List is formed on the basis of information received from the heads of standalone structural units (hereinafter, SSU) of the Bank or responsible officers of the units, based on verification activities of the CD CHO/ CU RB, as well as information from the Bank's automated systems on personnel movements of insiders.

4.2.5. When concluding an agreement with a legal entity that obtains access to the insider information of the Bank according to the concluded agreement, the said legal entity must be informed in accordance with the procedure established by the Bank on the requirements of 224-FZ and the responsibility for the unlawful use of insider information, as well as the fact that it will be included in the Bank Insiders List. Insider information may be transferred to legal entities according to concluded agreements only after the specified persons are included in the Bank Insiders List.

4.2.6. Legal entities and individuals included in the Bank Insiders List, as well as those excluded from the List, shall be notified no later than seven (7) business days from the date of making a corresponding entry in the Bank Insiders List.

4.2.7. CD CHO and CU RB shall maintain a register of notices of inclusion in (exclusion from) the Bank Insiders List and ensure storage of complete information on any notices sent to CD CHO or CU RB, respectively, within at least five (5) years of the date the person was excluded from the Bank Insiders List.

4.2.8. The Bank shall give notices of transactions with financial instruments of organizations that have included the Bank in their insiders list upon request of any such organizations.

4.2.9. The CD CHO shall generate the Bank Insiders List and transfer it to market operators upon their request and according to the procedure established by the regulation of the Bank of Russia /6/, and to the Bank of Russia upon the request of the corresponding regulator.

4.2.10. In order to manage the conflict of interest, the Bank regulates the distribution of control and operational functions for maintaining the Insiders List and other processes for protecting insider information through the issuance of IRDs, OADs, and employee job descriptions.

5. General Principles

5.1. **Responsibilities**

5.1.1. In accordance with the provisions of the Code of Administrative Offenses of the Russian Federation /3/ and the Criminal Code of the Russian Federation /4/, any person that violates the requirements of 224-FZ or any statutory regulations adopted thereunder may be brought to administrative or criminal liability.

5.1.2. The Bank’s employees who violate the requirements of this Policy, other IRDs and OADs of the Bank related to insider information protection and countering market manipulation may be subject to disciplinary action, including dismissal, to be applied as stipulated by the existing laws of the Russian Federation and IRDs/OADs of the Bank.

5.2. **Enforceability**

5.2.1. The requirements of this Policy and other IRDs and OADs in the field of protecting insider information and countering market manipulation are subject to mandatory fulfillment by all employees of the Bank and members of the Supervisory Board of the Bank.

6. Participants

6.1. The Supervisory Board of the Bank shall:

6.1.1. approve the procedure and timing for disclosure of insider information included in the Proprietary List of Insider Information

6.1.2. establish conditions for making transactions with financial instruments by persons specified in paragraphs 7 and 13 of Article 4 of 224-FZ and by any related persons

6.1.3. ensure overall supervision of the Bank's compliance with the requirements related to countering illegitimate use of insider information and market manipulation (hereinafter, CIUII/MM), and review reports on the Bank's compliance with applicable legislation on protecting insider information and countering market manipulation where required.

6.2. The Executive Board of the Bank shall review and approve the Policy and other IRDs on insider information protection and countering market manipulation within its competence.

6.3. CEO, Chairman of the Bank Executive Board shall:

6.3.1. designate (appoint) a structural unit (an officer) responsible for supervising compliance with 224-FZ and other applicable regulations

6.3.2. review quarterly reports on supervision of the Bank's compliance with applicable legislation and the Bank's IRDs for the purposes of CIUII/MM (hereinafter, the Quarterly Report)

6.3.3. exercise overall supervision of the process and measures taken in the area of CIUII/MM

6.3.4. assist and provide resources for responsible officers in charge of supervision of the Bank's compliance with 224-FZ to enable them to exercise their duties and functions in an unimpeded and effective manner

6.3.5. approve the ICR and the List of Insider Information of the Bank

6.4. Responsible officers in charge of supervision of the Bank's compliance with 224-FZ shall:

6.4.1. exercise ongoing and subsequent supervision of compliance by the Bank, its employees, or any other persons with the CIUII/MM legislation

6.4.2. compile the Quarterly Report and send it to the CEO and Chairman of the Executive Board of the Bank, as well as to the Supervisory Board for review

6.4.3. exercise control over the implementation of measures to minimize the risks of violation of law on CIUII/MM.

6.5. The employees of CD CHO and CU RB[3], in accordance with their powers and competencies, shall:

6.5.1. update the Bank's Insiders List and implement a set of procedures for notifying insiders in accordance with the CIUII/MM legislation

6.5.2. participate in the development of a general methodology on CIUII/MM at the Bank (applicable only to CD CHO)

6.5.3. implement measures to identify, analyze and resolve conflicts of interest in the area of CIUII/MM within their competence

6.5.4. hold events for training and development of the CIUII/MM culture, which includes providing employees with information and advice concerning the requirements of this Policy, any other rules or standards, or changes in regulatory requirements

6.5.5. present initiatives of responsible officers (hereinafter, RO) to amend the processes and documents of the Bank aimed at improving the methods and instruments for insider information protection

6.5.6. coordinate applications for personal transactions of insiders in accordance with the Rules for Transactions with Financial Instruments applied at Sberbank /14/

6.6. The Corporate Secretary Service shall disclosure insider information in accordance with the existing legislation and IRDs of the Bank.

6.7. SSU and CSU heads and deputy heads shall:

6.7.1. guide their subordinate employees to fully comply with the requirements of this Policy, and set an example of appropriate behavior

6.7.2. take into account cases of non-compliance of employees with the requirements hereof when evaluating their individual performance for staff motivation purposes

6.7.3. promptly notify CD CHO and CU RB of any persons gaining access to insider information according to the procedure established by the Bank

6.7.4. identify sources for obtaining actual access to insider information by their subordinate employees that they work with in the course of fulfilling their official duties

6.7.5. supervise completion of mandatory training in countering the illegitimate use of insider information and manipulation of the market by their subordinate employees in a timely manner

6.7.6. provide CD CHO (upon request by regulators, trading organizers and/or CD CHO) with written explanations of their or their subordinate employees' actions when making/executing (by virtue of their official duties)[4] transactions/ any other actions aimed at acquisition, alienation, or any other change in title to financial instruments, foreign currencies and/or commodities, or related to assumption of obligations to take any such actions

[3] The list of insiders is maintained by employees of CD CHO, while employees of CU RB may be involved in maintaining the Insiders List to perform certain procedures on behalf of CD CHO

[4] Applies to Bank employees (and their managers) whose duties include making transactions with financial instruments, foreign currency and/or commodities, making transactions and taking any other actions aimed at acquisition, alienation, or any other change in title to financial instruments, foreign currencies and/or commodities, or actions related to assumption of obligations to take any such actions, including posting bids (giving instructions) and accepting client orders.

6.7.7. ensure that job descriptions[5] of their subordinate employees include provisions requiring the employees to comply with requirements, obligations and responsibilities in accordance with any applicable legislation and the Bank's IRDs and OADs in the area of insider information protection.

6.7.8. ensure the identification of insider information not included in the Standard and Proprietary Lists, and bring such information and supporting documents (if any) to the CD CHO

6.8. Process owners shall:

6.8.1. ensure the development and design of processes, as well as their automation, taking into account the requirements set by 224-FZ, IRDs and OADs of the Bank related to insider information protection, which would ensure the provision of access to insider information only to persons included in the Bank Insiders List subject to the necessity criterium

6.8.2. when developing or modifying processes, customer pathways, IRDs and OADs drafts, shall check their compliance with the requirements of this Policy and of other IRDs on insider information protection, and, if necessary, they shall indicate the presence of insider information in accordance with the CookBook on Process Design and the Regulation on the Customer Pathway Management System and Sberbank Processes /12/

6.9. Owners of automated systems (hereinafter, the AS) of the Bank and analysts shall:

6.9.1. ensure the development and implementation of such a role model of access to insider information in the AS, which guarantees access to the relevant information only to persons included in the Insiders List subject to the necessity criterium

6.9.2. take into account requirements[6] approved by the Bank that are related to insider information protection in the AS while designing and updating an AS

6.10. Employees of the Global Markets Department and the Treasury (or their successors) whose duties include making transactions with financial instruments, foreign currencies and/or commodities (hereinafter also, transactions)making transactions and taking any other actions aimed at acquisition, alienation, or any other change in title to financial instruments, foreign currencies and/or commodities, or actions related to assumption of obligations to take any such actions, including posting bids (giving instructions), accepting client orders, shall receive annual training on countering financial market manipulation.

6.11. CD CHO shall be involved in organizing CIUII/MM training for the Bank's employees and individual insiders, including the development of training materials within its area of responsibility.

6.12. The HR Competencies Department shall:

6.12.1. assist CD CHO in organizing and carrying out CIUII/MM training, including off-schedule training initiated by RO

6.12.2. ensure inclusion in the employment contract template and in the job description template of the Bank of provisions requiring the employees to comply with requirements, obligations and responsibilities in accordance with any applicable legislation and the Bank's IRDs and OADs related to insider information protection

[5] Current standard template of the job description contains provisions that require the employees to comply with requirements, obligations and responsibilities in accordance with any applicable legislation and the Bank's IRDs and OADs in the area of insider information protection.

[6] Adopted according to the procedure established by the Bank, including by the Architecture Board of the Bank.

6.12.3. ensure that newly hired employees familiarize themselves with the provisions of this Policy.

6.13. All employees of the Bank shall:

6.13.1. identify (detect) insider information for inclusion in the Proprietary List

6.13.2. identify situations that may lead to illegitimate use of insider information or market manipulation, and work together with their direct supervisors and ROs on all matters related to managing such situations

6.13.3. strictly comply with the requirements of this Policy, of other IRDs and OADs of the Bank on illegitimate use of insider information and market manipulation

6.13.4. provide timely explanations of their actions or actions by their subordinate employees upon request by regulators, trading organizers or CD CHO

6.13.5. report cases of non-compliance to the Compliance Hotline, including potential non-compliance, by the Bank and/or the Bank's employees of the legislation and IRDs/OADs of the Bank on CIUII/MM in accordance with the PC on the Compliance Hotline at Sberbank /9/

6.13.6. assist ROs in the implementation of their functions

6.13.7. if it is necessary to gain access to insider information in the Bank's AS, inform their direct supervisor or the head[7] of the SSU that they need to be included in the Insiders List to perform official duties in the Bank's AS.

6.14. Employees required to complete training in countering illegitimate use of insider information and/or market manipulation in financial markets shall complete such training within established deadlines and in full.

7. Process Organization

Organization of CIUII/MM at the Bank shall include:

- determining the procedure for access to insider information
- maintaining the Insiders List
- establishing restrictions on the use of insider information
- supervising compliance with the RF legislation on CIUII/MM
- cooperating with supervisory authorities
- ensuring the operation of the Compliance Hotline.

7.1. Procedure for Access to Insider Information

7.1.1. Access to insider information at the Bank shall be granted according to the following principles:

7.1.1.1. the Bank Insiders shall have access to insider information of the Bank only under federal laws of the RF, applicable law, regulations, constituent documents of the Bank, and employment and/or independent contractor agreements

7.1.1.2. the Bank’s employees shall have access to insider information of the Bank and insider information of the Bank’s customers and counterparties only as part of exercising their duties stipulated in business unit regulations, regulations on collegial bodies, IRDs

[7] The responsible official in charge of maintaining the SSU Insiders List (if any)

and OADs of the Bank, and their job descriptions, subject to their timely inclusion in the Bank Insiders List

7.1.1.3. the Bank's employees that are authorized to liaise with shareholders, investors or the public in connection with performance of their official duties shall ensure equal opportunities for simultaneous access to disclosed material information about the Bank's activities for all interested persons, and also take steps to refute any inaccurate information.

7.1.2. It is prohibited to use insider information:

7.1.2.1. to carry out transactions, including cancellation or changing a request for transaction or providing recommendations to cancel or change a request on transaction to another person, with financial instruments, foreign currencies and/or commodities covered by such insider information, whether at their own expense or at the expense of any third party, except for the transactions carried out as part of discharging an obligation to purchase or sell financial instruments, foreign currencies and/or commodities that has become due, provided that such obligation arose as a result of a transaction that had been completed before insider information came to such person's knowledge

7.1.2.2. by means of transferring it to another person, except when such information is communicated to a person on the Insiders List in connection with performing their duties stipulated by the Federal Laws of the Russian Federation, applicable regulations, or in connection with performing their job duties or contractual obligations[8]

7.1.2.3. by giving direct or indirect recommendations to third parties, as well as by engaging or otherwise encouraging them to acquire or sell financial instruments, foreign currency and/or goods.

7.1.3. It is prohibited to take any actions that constitute market manipulation.

7.1.4. Whenever the Bank enters into independent contractor agreements with legal entities whose employees, by virtue of obligations assumed by the legal entity to perform work or provide services, have the right of access to insider information, the heads of the Bank's SSU or CSU responsible for initiating independent contractor agreements with such legal entities shall ensure the inclusion of the following terms and conditions therein:

7.1.4.1. an obligation of these entities and their employees to comply with the requirements of 224-FZ

7.1.4.2. a clause on non-disclosure by such legal entity or its employees of insider information that has become known to them in the process of performing independent contractor agreements with the Bank, that involve transfer of insider information, as well as an obligation not to use any obtained insider information to derive a profit or try to derive a profit

7.1.4.3. a clause on indemnification against any losses incurred by the Bank as a result of illegitimate use of insider information and/or market manipulation

7.1.4.4. a clause on transfer to the Bank and/or destruction of any physical media held by them containing insider information upon termination or cancellation of an

[8] In case of transferring insider information to any person included in the insiders list due to discharge of obligations established by the laws of the Russian Federation or discharge of official duties or independent contractor agreements, the person which is an insider transferring insider information shall ascertain that the recipient is included in the Bank insiders list and, thus, is obliged to comply with the non-disclosure regime applicable to obtained insider information

independent contractor agreement with the Bank (unless otherwise provided for in applicable laws.)

7.1.5. The Bank shall ensure that employment agreements and job descriptions as well as independent contractor agreements with individuals, legal entities and individual entrepreneurs contain provisions on compliance with the requirements of applicable legislation on insider information protection.

7.1.6. The transfer of the Bank's insider information by insiders (legal entities) to other legal entities is not allowed unless the right to transfer the Bank's insider information is included in the contracts concluded with such entities for the purpose of performing such contracts and only after such entities are included in the Bank Insiders List. The provision stipulating the right of insiders (legal entities) to transfer the Bank's insider information to other legal entities may be included into contracts only after receiving a preliminary approval of the CD CHO within the framework of the procurement procedure approved by the Bank.

7.1.7. The transfer by the Bank of insider information of other persons who have included the Bank in their Insiders List to other legal entities is not allowed unless the Bank's right to transfer such insider information to other legal entities is included in the contracts concluded with such entities for the purpose of performing such contracts. The provision stipulating the Bank's right to transfer the insider information of legal entities that have included the Bank into their Insiders List to other legal entities may be included into contracts only after a preliminary approval of the CD CHO according to the procedure approved by the Bank.

7.1.8. The insider information shall be transferred by the Bank at the request of legal entities, including governmental bodies, according to the procedure approved by the Bank including subject to the Process Charts, OADs and IRDs adopted by the Bank.

7.2. Establishing Restrictions on the Use of Insider Information

7.2.1. The Bank shall provide the necessary organizational and technical conditions for the observance of the confidentiality regime established in the Bank by persons having access to insider information, in accordance with the Cybersecurity Policy of Sberbank /10/ and the Book of Standards on Access Control /11/.

7.2.2. The Bank may introduce special procedures aimed at protecting the confidentiality of insider information against illegitimate use, including restricting the right of access to insider information by employees or officers of the Bank in order to comply with the requirements herein.

7.2.3. The Bank's employees shall notify[9] their direct supervisor and ROs of any facts known to them:

7.2.3.1. about any insider information of the Bank or the Bank's customers and/or counterparties that is not subject to disclosure by Bank's employees in accordance with their official duties but that has become known to them, including by virtue of mistakenly obtained/granted access to an insider information medium, or from the Bank insiders/any other persons orally or in writing

[9]If there is a conflict of interest between an employee and their supervisor, information may only be communicated to a RO.

7.2.3.2. about any circumstances that may lead to or result in a disclosure of insider information, or about any facts of disclosure of such information that became known to such person

7.2.3.3. about illegitimate use of insider information of the Bank, its customers or counterparties, including use by the Bank's employees, insiders or their relatives for their own benefit

7.2.3.4. about any transaction(s) with financial instruments, foreign currencies, and/or commodities made by the Bank's employees or customers, in respect of which there are reasons to believe that any such transaction constitutes a market manipulation.

7.2.4. In order to prevent market manipulation, the Bank shall implement the following procedures in relation to customers:

7.2.4.1. notify customers of inadmissibility of submitting orders for transactions that have attributes of market manipulation

7.2.4.2. obtain their consent to a possible refusal of the Bank to execute an order to complete a transaction, as well as a unilateral refusal of the Bank to execute (terminate) a brokerage service agreement with a customer if there are signs of manipulation

7.2.4.3. monitor, identify and analyze potentially non-standard transactions and/or requests with financial instruments, foreign currency and/or goods, including by using an automated transaction monitoring system.

7.2.5. The Bank's employees with access to insider information must fully comply with the procedure of storing electronic and physical documents containing insider information, namely:

7.2.5.1. store physical documents in safes or locked cabinets/ drawers of the desk

7.2.5.2. store documents on electronic media on network resources, the AS, in which access to insider information is provided to authorized persons and/or persons with a role model that provides access to insider information

7.2.5.3. when leaving the working premises, shut down the computer, do not leave documents with the Bank's insider information on the desks

7.2.5.4. do not use personal email to send and forward documents containing insider information of the Bank

7.2.5.5. unless needed, do not carry out electronic or physical documents containing insider information outside the Bank's working premises

7.2.5.6. when presenting the information verbally, inform the other party of the insider nature of the information and of the liability that its illegal use entails in accordance with Russian law

7.2.5.7. transfer insider information only to persons included in the Insiders List based on a characteristic attribute of an insider

7.2.5.8. use for processing insider information only those computers that have the necessary level of protection and are controlled by the Bank.

7.2.6. In case the Bank's employees detect the facts of loss of the Bank's insider information on tangible media (electronic, magnetic, optical, or paper), the absence of documents, files

containing the Bank's insider information, or cases of unauthorized, erroneously obtained/provided by/to them or other employees access to the Bank's insider information, they shall immediately notify their direct supervisor and their ROs.

7.2.7. It is prohibited to pursue any actions that qualify as market manipulation including those specified in Annex 4, ICR /8/.

7.2.8. Heads of SSUs, CSUs, and Regional Banks are responsible for taking the necessary measures to prevent access to automated systems, including other insider information carriers, on the part of their subordinates excluded from the Bank Insiders List or of those who obtained the respective access illegally/erroneously.

7.2.9. Bank employees shall cooperate with the RO and promptly and fully provide the information and documents requested by the RO. The Bank's employees responsible for interacting with the Bank's customers shall deliver enquiries prepared by a RO to the customer within two business days from receiving such an enquiry from a RO.

7.2.10. The Bank may impose restrictions on insiders included in the Bank Insiders List as an issuer of securities, establishing a ban on transactions with the Bank's securities and derivative financial instruments on such securities within Thirty (30) calendar days before and Two (2) business days after the publication of the interim consolidated financial statements (for three, six and nine months) and the annual consolidated financial statements prepared in accordance with IFRS requirements. Information on the dates of IFRS financial statements publication is available on the Bank's website in the 'Investor Relations' section, in the Investor Calendar at http://www.sberbank.com/ru/investor-relations/ir/calendar.

7.3. Verification of Compliance with the RF Laws on CIUII/MM in the Bank

7.3.1. Compliance with the Russian laws on CIUII/MM at the Bank, by virtue of the Order of CEO, Chairman of the Executive Board, shall be controlled by:

7.3.1.1. RO in charge of control over compliance with 224-FZ at the Bank in terms of countering illegitimate use of insider information (hereinafter, CIUII RO)

7.3.1.2. RO in charge of control over compliance with 224-FZ at the Bank in terms of countering market manipulation (hereinafter, CMM RO).

7.3.2. Compliance with RF laws on CMUII/MM in the Bank is verified according to ICR /8/.

7.4. Cooperation with Supervisory Authorities

7.4.1. Due to the fact that activities involving insider information may damage its business reputation, the Bank reserves the right to notify the Bank of Russia of any transactions with financial instruments, foreign currencies, and/or commodities carried out on the basis of insider information, which are known to the Bank, and also apply to court for compensation for damages.

7.4.2. Pursuant to the lawful motivated request of the Bank of Russia or any government authority, the Bank shall provide information pertaining to the Bank's insider information. Motivated request must be signed by an authorized official and contain the purpose and legal basis for requesting information, as well as the deadline for its submission.

7.5. Training the Bank's Employees in the Area of Countering Illegitimate Use of Insider Information and/or Market Manipulation

7.5.1. For the purposes of training the Bank’s employees, the ROs shall prepare field-specific methodology and materials in the area of countering illegitimate use of insider information and/or market manipulation.

7.5.2. The HR Competencies Department shall organize the process of training the Bank’s employees in the area of countering illegitimate use of insider information and/or market manipulation.

7.5.3. The Bank units shall assist in organizing and carrying out the respective training events within the scope of their duties.

7.6. Compliance Hotline

7.6.1. The Bank has a Compliance Hotline, which is implemented in accordance with the principles specified in the Conflict of Interest Management Policy of Sberbank Group /13/, and operates in accordance with the PC on the Compliance Hotline at Sberbank /9/.

7.6.2. The Bank shall ensure prompt and comprehensive consideration of queries regarding compliance by the Bank, its employees, counterparties, and customers with the requirements of 224-FZ, applicable regulations and the Bank's IRDs on insider information protection.

7.6.3. The Bank shall ensure anonymity and confidentiality when considering queries received by the Compliance Hotline.

7.6.4. Information on the Compliance Hotline is published on the official website of the Bank in the Internet and on the desktops of corporate computers of the Bank's employees.

7.6.5. The Compliance Hotline is available for inquiries from the Bank's employees, customers, counterparties and other third parties.

7.6.6. ROs participate in the consideration of applications related to CIUII/MM.

7.6.7. The Bank expects employees and other third parties to responsibly and promptly disclose information on the facts of unlawful use of insider information of the Bank, customers and counterparties of the Bank, as well as on events that have led and/or may lead to a violation of the requirements established by the applicable law and the IRDs/OADs of the Bank on insider information protection.

8. Final Provisions

If any specific clauses herein become contradictory to the statutory regulations of the RF and/or any other applicable law due to amendments thereto, these clauses shall be deemed void. Before this Policy is amended, one shall follow the statutory regulations of the Russian Federation and/or applicable law.

Annex 1.

List of Terms and Definitions

Bank shall mean Sberbank.

Bank of Russia shall mean the Central Bank of the Russian Federation (the Bank of Russia).

Closely Related Persons shall mean a spouse (partner) or a person having a similar status, underaged children; relatives residing with the person carrying out managerial functions for at least one year before the date of a transaction with the Bank's financial instruments; a legal entity, trust/partnership managed (controlled, whether directly or indirectly) by the person carrying out managerial functions or his/her spouse (partner or a person having a similar status), underaged children, or relatives residing with such a person for at least one year and created (operating) in the interests of the person with managerial functions.

Commodities shall mean items, except for securities, which are admitted to the organized trading in the Russian Federation or in respect of which an application has been filed for admission to such trading.

Credit Institution shall mean a legal entity that is entitled to perform banking transactions to derive income as the main purpose of its activity on the basis of a special permit (license) issued by the Central Bank of the Russian Federation (the Bank of Russia).

Customer shall mean an individual or a legal entity receiving services on the basis of concluded agreements including the one that has acceded to the Terms of Provision of Brokerage Services at Sberbank.

Financial Instrument shall mean a security or a derivative financial instrument.

Insider shall mean an individual or a legal entity that has access to insider information.

Insider Information shall be conceived in accordance with the definition provided in 224-FZ.

Internal Control Organization shall mean a set of measures undertaken by the Bank, including the development and approval of internal control rules as well as programs for their implementation, appointing officers responsible for monitoring compliance with the rules, and implementation of the programs.

Investor shall mean an individual being a resident of the Russian Federation or a legal entity that has acceded to the Terms of Provision of Brokerage and Other Services at Sberbank.

Issuer shall mean a legal entity, an executive authority, or a local government authority, which bears liabilities, on their own behalf or on behalf of a public-law entity, to the security holders to exercise the rights vested in these securities.

Legal Risk shall mean the possibility that the Bank incurs losses due to:

- any breach of concluded contracts by the Bank and/or its counterparties
- any breach of regulatory acts by the Bank and/or its counterparties
- errors of law made in the course of business (e.g., wrong legal advice or incorrect preparation of documents, including for judicial proceedings on disputed issues)
- deficiencies of the legal system (contradictory laws, lack of legal norms on regulating certain issues arising in the business activities of the Bank)
- location of branches of a credit institution, legal entities over which a credit institution exercises control or material influence as well as counterparties of a credit institution under the jurisdiction of other countries.

Market Manipulation shall mean willful actions defined by the laws of the Russian Federation on countering illegitimate use of insider information and market manipulation and statutory regulations of the Bank of Russia, which result in the deviation of price, demand, supply, or trading volumes of a financial instrument, foreign currency, and/or commodity from the level or their holding at the level which is drastically different from that which would have been achieved without such actions.

Media Containing Insider Information (information carrier, source) shall mean an electronic, magnetic, optical, paper object, used by the Bank's employees, able to store (contain) in itself the information recorded to it. Any object can be an insider information carrier, including an automated system available for readout (retrieval, copying) of insider information contained in (entered, recorded to) it.

Operational Risk is the risk of incurring losses due to defects in internal processes, functioning of information systems, unauthorized/illegal actions or errors of employees, or due to external events.

Professional Securities Market Participant shall mean a legal entity that carries out any types of activities stipulated by Chapter 2 of Federal Law No. 39-FZ "On the Securities Market" dated April 22, 1996.

Public Information shall mean publicly known information and other data in the public domain with an unrestricted access thereto.

Regulatory Risk is a risk of losses to be incurred by the Bank due to non-compliance with any applicable legislation, internal documents of the Bank, standards of self-regulatory organizations (if such standards or rules are mandatory for the Bank), as well as due to application of sanctions and/or other measures of impact by the supervisory authorities.

Reputational Risk shall mean the risk occurring as a result of negative perception of the Bank by its customers, counterparties, shareholders, investors, lenders, market analysts, and supervisory authorities, that may adversely affect the Bank's ability to maintain existing and establish new business relations and maintain continuous access to financial resources, e.g., in the interbank market.

Unit Responsible Officer means an employee, authorized on the basis of organizational and administrative documents of the SSU or CSU, responsible for identifying persons who have (receive) or lose actual access to insider information and send the relevant information to the CD CHO/CU RB.

Annex 2.

List of Abbreviations

CD CHO stands for Compliance Division of the Central Head Office

CIUII/MM stands for countering illegitimate use of insider information and market manipulation

CIUII RO stands for a responsible officer in charge of control over compliance with 224-FZ at the Bank in terms of countering illegitimate use of insider information

CMM RO stands for a responsible officer in charge of control over compliance with 224-FZ at the Bank in terms of countering market manipulation

CSU stands for a centrally subordinated unit, including remote workplaces (RWP)

CU RB stands for a Compliance Unit at a Regional Bank

FZ stands for a Federal Law

INN stands for a taxpayer identification number

IRD stands for an internal regulatory document

OAD stands for an organizational-administrative document

OGRN stands for a primary state registration number

PC stands for a process chart

PJSC stands for a public joint-stock company

RB stands for a Regional Bank

RF stands for the Russian Federation

RO stands for both CIUII RO and CMM RO

SSU stands for a stand-alone structural unit

Annex 3.

References

1. Federal Law No. 224-FZ dated July 27, 2010 ‘On Counteracting the Illegitimate Use of Insider Information and Manipulation of the Market, and on Making Amendments to Separate Legislative Acts of the Russian Federation'

2. Federal Law No. 208-FZ dated December 26, 1995 ‘On Joint-Stock Companies’

3. Code of Administrative Offences of The Russian Federation dated December 30, 2001 No. 195-FZ

4. Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996

5. Bank of Russia Ordinance dated September 27, 2021 No. 5946-U “On the List of Insider Information of Legal Entities Stipulated in items 1, 3, 4, 11 and 12 of Article 4 of the Federal Law No 224-FZ dated July 27, 2010 'On Counteracting the Illegitimate Use of Insider Information and Manipulation of the Market, and on Making Amendments to Separate Legislative Acts of the Russian Federation,’ and its Disclosure Procedure and Deadlines'”

6. Bank of Russia Ordinance No. 5129-U dated April 22, 2019 “On the Procedure of Submitting by the Legal Entities Specified in Clauses 1-4, 11 and 12 of Article 4 of the Federal Law 'On Counteracting the Illegitimate Use of Insider Information and Manipulation of the Market, and on Making Amendments to Separate Legislative Acts of the Russian Federation’ to a Market Operator, through which Transactions with Financial Instruments, Foreign Currency and/or Commodities Are Being Carried Out, a List of Insiders, at its Request'”

7. Part 7 of the Book of Compliance Risk Management Standards of Sberbank (Compliance Procedures Implementation Standard of Sberbank No. 4403), as amended

8. Internal Control Rules for Prevention, Identification and Suppression of the Illegitimate Use of Insider Information and/or Manipulation of the Market at Sberbank No. 5179 as amended

9. Sberbank Compliance Hotline Process Chart No. 3974 as amended

10. Cybersecurity Policy of Sberbank No. 4660 as amended

11. Sberbank Access Control Policy No. 4735 as amended

12. Regulation on the Customer Pathway Management System and Sberbank Processes No. 1927 as amended

13. Conflict of Interest Management Policy of Sberbank Group No. 3369 as amended

14. Rules for Carrying out Transactions with Financial Instruments at Sberbank No. 5008 as amended