SBERBANK OF RUSSIA

APPROVED BY
Resolution of the Supervisory Board
of Sberbank

Minutes No. 4
dated February 15, 2019

Conflict of Interest Management Policy of Sberbank Group

Moscow

2019

IRD Details

IRD Name	Conflict of Interest Management Policy of Sberbank Group (Version 3)
Business unit responsible for IRD development	Compliance Division

CONTENTS

1. GENERAL 4
2. CONFLICT OF INTEREST MANAGEMENT GOALS AND OBJECTIVES 4
3. POTENTIAL RISKS IN CONFLICT OF INTEREST MANAGEMENT AND CONFLICT OF INTEREST TYPES. 4
4. GENERAL PRINCIPLES OF CONFLICT OF INTEREST MANAGEMENT 5
5. PARTICIPANTS IN THE CONFLICT OF INTEREST MANAGEMENT PROCESS, THEIR FUNCTIONS AND EMPOWERMENT 6
6. CONFLICT OF INTEREST MANAGEMENT STAGES 9
7. SPECIFICS OF ORGANIZATION OF THE CONFLICT OF INTEREST MANAGEMENT SYSTEM AT THE GROUP MEMBERS 16
8. LIABILITY OF THE BANK/GROUP MEMBERS AND THEIR EMPLOYEES 17
9. FINAL PROVISIONS 17
APPENDIX 1 18
APPENDIX 2 20
APPENDIX 3 21

1. General

1.1. This Policy is a part of the compliance risk management system, it stipulates the management and organizational framework for preventing conflicts of interest, including potential ones, the measures for mitigating and/or eliminating their consequences, sets the main goals, objectives and principles for managing conflicts of interest, including potential ones, at Sberbank (hereinafter, "the Bank") and the members of Sberbank Group (hereinafter, "the Group members", "the Group member").

1.2. This Policy has been developed in accordance with the requirements of the Russian and international legislation, as well as taking into account the best Russian and international principles and practices.

1.3. The Bank expects all employees of the Bank/the Group members to comply with certain ethical principles, approaches and requirements established hereby.

1.4. This Policy is the basis for development of other internal regulatory documents (hereinafter, "IRDs") in the area of conflict of interest management by the Bank and the Group members.

2. Conflict of interest management goals and objectives

The purpose of this Policy is to determine the procedures and instruments aiming to prevent, detect, control and resolve (avoid) conflicts of interest in a timely manner, formalize the measures for mitigating their consequences, and stipulate the rules of conduct for employees of the Bank/the Group members in case of a conflict of interest, including a potential one.

The main objectives of this Policy are to:

- increase customers' and partners' confidence toward the Bank and the Group members; provide services to customers in accordance with the high standards of corporate governance based on the principles of openness, transparency and predictability
- ensure compliance with international standards and best practices in order to improve the Bank's business reputation, including at the international level
- establish the principles for disclosing information on potential conflicts of interest, the instruments for making management decisions, and the standards of conduct of employees of the Bank/the Group members in case of a conflict of interest
- provide employees with general information about measures taken by the Bank in order to manage (prevent, detect and settle) conflicts of interest, including potential ones, and help them find the most appropriate ways to resolve such situations
- stipulate the standards for managing conflicts of interest, including potential ones, that are mandatory for compliance at the Bank and the Group Members.

3. Potential risks in conflict of interest management and conflict of interest types

3.1. A conflict of interest is inherent in any area, including banking and securities market activity. A conflict of interest in itself will not be deemed to be a violation of the Bank's internal procedures, provided that adequate measures have been taken in a timely manner to disclose, detect, assess and manage such a conflict.

A conflict of interest (or a perceived existence of such a conflict), in relation to which appropriate measures have not been taken, constitutes a threat to the Bank/Group member in the opinion of its employees and other persons, including customers, shareholders, counterparties, the State and government bodies, trade union organizations, professional associations, and securities market participants.

3.2. Inadequate management of a conflict of interest by the Bank/Group member may, among other things, entail realization of the following types of risks:

- risk of noncompliance with legislative and regulatory requirements
- reputational risk (risk of losing business reputation)
- legal risk
- risk of material financial losses.

Conflicts of interest may be of the following types:

- between customers of the Bank/Group member, including when interests of a customer (a group of customers) contradict interests of another customer
- between a customer and the Bank/Group member, including when transactions with a customer are settled at nonmarket prices contravening investment goals or otherwise infringing a customer's interests to the benefit of the Bank/Group member
- between a customer and an employee of the Bank/Group member, including when an employee renders advantages to one customer to the detriment of another customer's interests in order to obtain a personal benefit
- between the Bank/Group member and its employee, including when an employee misuses his/her official position / confidential information in order to obtain a personal benefit.

Typical examples of conflicts of interest are listed in Appendix 3 hereto. The list of situations is not exhaustive. Employees should also be able to assess possible existence of a conflict of interest, including a potential one, in other situations similar in their essence, and subsequently report relevant information to their line manager and/or the Compliance Unit.

4. General principles of conflict of interest management

4.1. In a situation of a conflict of interest, the Bank and the Group members shall prioritize customers' interests. In case a conflict of interest arises between an employee and the Bank/Group member and it is impossible to eliminate such a conflict of interest, interests of the Bank/Group member shall prevail over personal interests of its employees.

4.2. The Bank/Group members adhere to the following principles for managing conflicts of interest, including potential ones:

- equal and fair attitude towards all customers of the Bank/Group member within consultations provided for them or transactions settled with them or on their behalf and/or by their orders
- delineation of empowerment: the Bank/Group member shall clearly delineate decision-making powers of the management bodies of the Bank/Group member and those of its employees so as to avoid conflicts of interest. Employees must exercise their official powers and capabilities solely to the benefit of the Bank/Group member. Stakeholders whose interests are or may be affected by a conflict of interest shall not be involved in its settlement.
- fair and independent assessment of possible risks for the Bank/Group member in case of detection of conflicts of interest, including potential ones

- maintenance by executives of the Bank/Group member of the appropriate culture of employees' behavior where they are aware of and understand their duties and freely notify the management of their doubts and problems ("tone from the top")
- involvement of all employees, regardless of their positions at the Bank/Group member, in the processes of detection and settlement of a conflict of interest, including a potential one
- development of measures to resolve a conflict of interest, including a potential one, comprising, among other things, acceptance, avoidance and mitigation of risk
- protection of nonpublic, confidential, and insider information and data received in the course of disclosure of information on a conflict of interest, including a potential one
- forming an open communication environment that includes protection of employees of the Bank/Group members against any sanctions/prosecution related to reporting of a conflict of interest, including a potential one, disclosed by an employee in a timely manner and settled (prevented) owing to adequate measures taken
- ensuring adequacy of the regulatory framework, including establishment of the rules and restrictions to minimize the risk of a conflict of interest, including a potential one
- organizing training events, including those with subsequent testing of employees for knowledge and understanding of the key statutes in conflict of interest management
- ensuring storage of customers' securities and funds separately from the assets owned by the Bank/Group member
- open interaction with supervisory authorities and the regulator.

5. Participants in the conflict of interest management process, their functions and empowerment

5.1. The Bank's Supervisory Board:

- approves this Policy
- exercises overall control over the conflict of interest management process and measures taken to manage conflicts of interest, including potential ones.

5.2. The Bank's Executive Board:

- is responsible for the compliance of the Bank's operations with the legislation, ensuring fulfillment of the requirements of the legislation by organizing systems, processes, controls and procedures needed to manage conflicts of interest, including potential ones
- exercises control over compliance with this Policy, including efficient and prompt resolution of issues by other collegial bodies within the system for management of conflicts of interest, including potential ones
- determines the need to involve representatives of the Bank's Compliance Unit in the work of the Bank's collegial bodies.

5.3. The Bank's Compliance Committee:

- makes decisions on matters and measures taken within management of conflicts of interests, including potential ones, in accordance with /14/.

5.4. The Regional Bank's Compliance Committee:

- reviews issues and makes decisions on issues related to managing conflicts of interest, including potential ones, within its purview and in accordance with /15/.

5.5. Employees of the Bank's Compliance Unit within the powers provided to them and their competence shall:

- take part in developing the common method for managing conflicts of interest, including potential ones, and ensure the uniformity of the approaches applied by the Group members, including advisory support
- carry out expert reviews of IRDs and organizational-administrative documents (hereinafter, "OADs"), contracts and agreements, including those under development and approval, as requested by relevant persons drafting them, in order to manage and minimize the risk of a conflict of interest
- implement measures to identify, analyze and resolve conflicts of interest, including potential ones
- take part in the implementation of procedures and measures aimed at developing culture in the area of conflict of interest management, which includes provision of relevant information to employees, organization of trainings and consultations on implementation of this Policy, other standards and rules, as well as changes in the regulatory requirements
- submit issues for consideration by the Bank's Compliance Committee / the Regional Bank's Compliance Committee in accordance with /14/ and /15/
- initiate and/or take part in internal audit reviews on issues related to managing conflicts of interest, including potential ones, and may also involve employees from other business units of the Bank, where needed
- report to the Bank's Security Unit about all committed or intended actions that have caused/may cause a conflict of interest
- prepare training materials in the area of conflict of interest management
- consult the Bank's employees on issues related to managing conflicts of interest, including potential ones.

5.6. Employees of the Bank's Security Unit within their competence shall:

- prepare and implement measures aimed at detecting and suppressing any actions of the Bank's employees that have caused/may cause a conflict of interest
- initiate and take part in internal audit reviews within their competence
- cooperate with the law enforcement bodies with regard to provision of materials on detected violations committed by the Bank's employees, when needed, in order to subject such employees to liability in compliance with the effective legislation of the Russian Federation
- cooperate with the Compliance Units so as to reveal information on actions intended or committed by the Bank's employees that have entailed/may entail a conflict of interest.

5.7. Members of the collegial bodies and their deputies shall:

- take into account the conflict of interest management principles, the requirements of this Policy, as well as other IRDs/OADs when making decisions on issues reviewed by the collegial body
- make sure they and their relatives have no conflict of interest (personal interest) in relation to an issue being reviewed by the collegial body of the Bank/Group member

- ensure that all members of the Bank's collegial body and the Bank's Compliance Unit are notified about a conflict of interest (personal interest) or risk of its occurrence in relation to an issue being reviewed by the Bank's collegial body, in order to assess the level of risk of such a conflict of interest and measures for its mitigation. Information on a conflict of interest (personal interest), including a potential one, shall be submitted before the collegial body makes a decision on the relevant issue.
- be responsible for timely submission of the above information to the full extent
- not participate in the discussion of and voting on issues reviewed by the collegial body of the Bank/Group member, when they have a conflict of interest (personal interest), including a potential one
- comply with the rules for reporting information on existence of a conflict of interest (personal interest), including a potential one.

5.8. Heads of independent structural units and their deputies shall:

- urge employees to fully comply with the requirements hereof and the ethical standards of behavior, and set an example of appropriate behavior; identify areas, activities and business processes involving the risk of a conflict of interest, including a potential one, based on the empowerment and functions of independent structural units; develop and implement measures to mitigate the risk of a conflict of interest, including a potential one, and cooperate with the Compliance Unit when needed
- make sure employees read and understand this Policy and other IRDs devised in furtherance of the provisions and principles hereof, and put their signatures to confirm this
- ensure compliance with the principles and requirements hereof by their subordinates
- take into account whether employees strictly and efficiently fulfil the requirements hereof when evaluating their individual performance for staff motivation purposes.

5.9. All employees of the Bank, regardless of their positions, shall:

- identify situations that may entail a conflict of interest, and cooperate with the Compliance Unit on all issues related to implementation of the requirements of this Policy
- take reasonable measures to prevent a conflict of interest, including a potential one
- prioritize interests of the Bank/the Bank's customers over personal interests and avoid violation of rights and legitimate interests of the Bank and its customers
- strictly adhere to the requirements of the legislation in the area of conflict of interest management, this Policy, and the Bank's other IRDs/OADs on compliance, the principles of professional ethics and ethical standards of doing business, as well as the obligations stipulated by the Compliance Unit
- performing their functional duties or carrying out activities on behalf of the Bank in a foreign country, comply with the national legislation of such a country and the standards of international law in the area of conflict of interest management, as well as the requirements of this Policy and the Bank's other IRDs/OADs on compliance
- refrain from committing acts and making decisions that may entail a conflict of interest
- in a timely manner, report any conflict of interest and situations that may entail a conflict of interest for their mandatory assessment by the Compliance Unit
- in a timely manner, take training programs on conflict of interest management issues
- notify the Compliance Unit of any known/potential/revealed violations of this Policy and the Bank's other IRDs/OADs on compliance and/or report them to the Compliance Hotline

- assist their colleagues and the Compliance Unit in resolving an existing/potential conflict of interest
- comply with the rules of dealing with confidential and insider information
- comply with the Bank's ethical principles, approaches and requirements established herein
- address their line manager and/or the Compliance Unit for explanations in case of any doubts regarding permissibility of actions or other issues related to the provisions hereof.

6. Conflict of interest management stages

To more efficiently manage conflicts of interest, including potential ones, as well as to clearly align actions of the management bodies and employees of the Bank/Group members, the conflict of interest management process comprises the following stages:

- conflict of interest prevention – implementation of measures to avoid a conflict of interest
- detection and assessment of a conflict of interest – continuous monitoring and assessment of potential situations that may entail a conflict of interest
- settlement of a conflict of interest – a complex of measures aimed at full and prompt resolution of a conflict of interest.

6.1. Conflict of interest prevention

The main measures to prevent a conflict of interest in the course of operations of the Bank/Group members are as follows:

- strict compliance by the management bodies and employees of the Bank/Group members of the procedures established by the effective legislation, the Charter and IRDs/OADs of the Bank/Group members, and job descriptions, including when carrying out banking operations and transactions
- building the organizational structure of the Bank/Group members that would clearly delineate the areas of responsibility, empowerment and reports
- forming the membership of the collegial bodies of the Bank/Group members and holding meetings of the relevant collegial bodies in accordance with the principle of preventing a conflict of interest, including a potential one, as well as independence of decision-making
- implementation of the practice of making collective decisions on the most critical and large-scale issues
- implementation of the double control practice (the four eyes principle)
- reviews by the Internal Audit Service
- implementation of a multi-level internal control system at the Bank
- establishment of information barriers (the Chinese wall principle)
- adherence to the principles of independence of business units and the "need to know" principle in distribution of information flows
- establishment of the rules on how employees shall perform transactions with securities and related derivative financial instruments
- establishment of restrictions on using mobile phones for certain categories of employees
- disclosure of information on conflicts of interest, including potential ones.

In order to prevent, minimize and resolve a conflict of interest, including a potential one, the Bank/Group members may require the employees to observe additional (individual) obligations stipulated by the Compliance Unit.

6.1.1. Information barriers (the "Chinese wall" principle)

The "Chinese wall" principle is the principle of organizing a business process or interaction of several business processes to separate information for each stage of a business process or several business processes and to allow information transfer only in accordance with the established rules.

In accordance with the "Chinese wall" principle, the Bank's business units are divided into two categories based on information available to them:

- "Private side" – business units that, due to their functional duties, may access nonpublic information that can create advantages for its possessor
- "Public side" – business units that, due to their functional duties, may not access nonpublic information that can create advantages for its possessor.

Access to nonpublic information can be provided to a "public side" employee after approval of such access by the Compliance Unit, provided that such access has been agreed upon by the head of the business unit of the employee and the head of the "private side" business unit.

Some employees of the Bank whose duties require access both to public information and to nonpublic information providing advantages to its possessor may get the "above-the -wall" status.

The Compliance Unit is responsible for determining employees' status in relation to the "Chinese wall" and for assigning the "above-the-wall" status.

To maintain the information barriers, the Bank uses the following methods:

- limitation of information availability within certain facilities of the Bank's buildings with ensuring physical and technological safety of the said information
- differentiation of access to various data categories in information systems among users of various business units
- usage of code words when communicating price-sensitive information
- adequate supervision over the Bank's employees having access to price-sensitive information, as well as employees' training in how to use and abide by the information barriers
- assignment of certain confidentiality obligations to the persons having access to insider information
- restriction of access to confidential information when its disclosure is not required
- use of the "need to know" principle in distribution of information flows (in accordance with clause 6.1.3)
- monitoring of transactions in securities conducted for personal purposes by employees having access to nonpublic information.

6.1.2. Independence of business units' operations

When resolving conflicts of interest, including potential ones, the Bank/Group members shall ensure an appropriate and reasonable extent of independence in operations of all internal business units of the Bank/Group members.

In view of simultaneous execution of transactions for different customers, additional measures may also include:

- delineation of managers responsible for executing customer transactions

- full delineation of teams involved in executing customer transactions
- establishment of a “blackout period” for performing transactions
- establishment of the “Chinese Wall’ (according to Clause 6.1.1 hereof).

6.1.3. The “need to know” principle of information flow distribution

Measures being implemented to prevent disclosure of confidential, nonpublic and insider information include, among other things, the ”need to know” principle. It must be observed by all employees of the Bank/Group members and prohibits disclosure of information to employees who do not need access to such information to perform their direct duties.

6.1.4. Rules for financial instrument transactions performed by employees for personal advantage

The Bank/Group members encourage long-term investment and do not encourage speculative securities trading.

Within control over financial instrument transactions carried out by employees for personal advantage, the following general rules and restrictions are applicable:

- employees of the Bank/Group members shall rely on common sense and avoid personal investments that can jeopardize the reputation of the Bank/Group member or entail a conflict of interest; among other things, employees may not conduct personal transactions to the detriment of performance of their duties
- employees of the Bank/Group members are prohibited from carrying out financial instrument transactions for personal advantage violating the effective legislation, the internal procedures and restrictions established at the Bank/Group members, including transactions in financial instruments of the Bank during a blackout period, transactions deemed to be market manipulation or illegal use of insider information, important nonpublic information, and other information protected by law
- in cases stipulated by IRDs/OADs, employees shall disclose information on brokerage accounts used to execute personal transactions with financial instruments, obtain approval from the Bank/Group member prior to carrying out such transactions, and submit relevant reports upon performance of financial instrument transactions.

6.1.5. Mobile phone use rules

In order to prevent abuses, as well as to ensure that the employees fulfill customer service fairness requirements, the Bank imposes restrictions on the use of mobile phones by certain categories of employees when performing their job and functional duties. The Bank may use technologies allowing recording and control of conversations held by such categories of employees using landline phones, in accordance with the effective legislation.

The Bank’s employees dealing with acceptance and coordination of customer orders for transactions in securities must hold any conversations using the phone line recorded by the Bank.

6.1.6. Measures aimed at identification, control and mitigation of consequences of conflicts of interest when carrying out professional activities in the securities market

When servicing customers as a professional participant of the securities market, the Bank shall:

- identify a conflict of interest that may arise when providing services to a customer, before rendering relevant services (in the course of development of products, marketing materials, coordination of transactions, etc.)

- take measures aimed at avoiding identified conflicts of interest (e.g. decline one of transactions entailing a conflict, create information barriers between business units, delineate project teams, etc.)
- prioritize customer's interests over the Bank's interests when settling a conflict of interest
- perform financial instrument transactions to the benefit of customers based on their orders. Transactions without relevant orders are only allowed within the empowerment provided for by the effective legislation and the contract with a customer
- execute customers' orders pursuant to the requirements set therein on the best conditions available in particular circumstances and within a shortest possible period, with appropriate competence, accuracy and commitment
- ensure implementation of information barriers between business units (employees) involved in different activities, when absence of such barriers entails a conflict of interests, including between the Bank (its employees) and customers
- limit the number of employees having access to nonpublic, confidential and/or insider information of a customer (issuer), as well as implement, among other things, the "need to know" principle stipulated hereby (according to Clause 6.1.3.)
- implement other measures provided for hereby that are necessary to detect and eliminate conflicts of interest in the Bank's professional activities in the securities market.

If mitigation (avoidance) measures have not enabled to completely eliminate a conflict of interest involving the Bank or its employee, prior to performance of a transaction affected by a conflict of interest the Bank shall notify a customer, including a securities issuer, of a conflict of interest and of measures being implemented to resolve it, as well as provide any other information to a customer required by the applicable legislation and by the contract with a customer.

6.1.7. Disclosure of information on conflicts of interest

The Bank/Group members minimize and prevent the risk of a conflict of interest, including a potential one, through disclosure of information on such a conflict of interest by employees, including:

- when an employee gets work
- as situations occur that have caused and/or may cause a conflict of interest, including a potential one
- on an annual basis
- in other cases, prior to certain events and/or receipt of a certain kind of information.

Information that must be disclosed to the Compliance Unit covers the following:

- any activities carried out by employees outside the Bank, including participation in third parties' charter capital (except for entities whose shares are admitted for on-exchange trading, provided that a stake does not exceed 2% of the charter capital), membership in third parties' management bodies, including audit commissions, doing business, and combined job
- receipt by an employee of any offer to join third parties' management bodies and/or participate in third parties' charter capital (except for entities whose shares are admitted for on-exchange trading, provided that a stake does not exceed 2% of the charter capital), or to have a combined job
- relatives working together at the Bank and the Group members, including joint involvement of relatives in business processes and/or membership in collective bodies (including when relatives are involved in the same business process, and when one of relatives represents the Bank's interests and the other one – interests of the Group member)

- changes in circumstances of an employee and/or employee's relatives, including changes in job or functional duties performed at the Bank/Group members
- participation of an employee's close relatives in third parties' charter capital (except for entities whose shares are admitted for on-exchange trading, provided that a stake does not exceed 2% of the charter capital) and their membership in third parties' management bodies, business of an employee's relatives when such entities are competitors, customers and/or counterparties of the Bank/Group members, as well as any changes in the said circumstances
- other cases that may cause a conflict of interest, including a potential one.

All reported information on situations that have caused and/or may cause a conflict of interest, including a potential one, shall be checked by an authorized employee of the Compliance Unit in order to assess risks arising for the Bank/Group member and to choose the most appropriate way to settle such situations.

Disclosure of information on a conflict of interest, including a potential one, does not release the Bank/Group members and their employees from the obligation to implement and maintain efficient organizational and administrative measures aimed at settling and preventing similar situations in the future. Employees of the Bank/Group members should suggest ways to resolve conflicts of interest, including potential ones, depending on their duties and the level of competence.

The Bank/Group member shall disclose information on an existing or potential conflict of interest in relation to a customer prior to concluding a transaction with such a customer, if the procedure and measures implemented to resolve such a conflict of interest do not enable prevention of the risk.

Information on activities and/or involvement of the Bank's employees and/or their relatives in management of housing cooperatives, housing and construction cooperatives, garage cooperatives, horticultural, gardening, and countryside housing consumer cooperatives, property owners associations, and trade union organizations performed free of charge is not subject to disclosure.

The Bank's employees shall disclose information according to the procedure and within the period stipulated by the provisions of /10/.

6.1.8. Checklists

In the course of its operations in financial markets, the Bank shall maintain and monitor checklists that are key instruments for conflict of interest management and enable monitoring of the Bank's activities, identifying potential conflicts of interest in a timely manner, and promptly settling them.

Checklists shall include, among other things, the following:

- the watch list – a list of issuers in relation to whom the Bank has confidential or insider information regarding expected credit and investment banking transactions, as well as transactions that have not been announced
- the restricted list – a list of issuers and financial instruments that are subject to certain restrictions associated with carrying out transactions in the securities market, or reference to certain issuers in analytical reviews
- the deal team list – a list of the Bank's employees involved in an investment banking transaction of an issuer in relation to whom the employees have or may have access to confidential or insider information
- the blackout list – a list that includes information on economic sectors and/or issuers in relation to which the Bank has restrictions on performance of analytical studies and provision of recommendations to investors

- the register of analytical coverage containing, among other things, information on the companies covered therein, with references to analysts preparing relevant reports.

6.1.9. Handling gifts and hospitality expenses

The Bank and the Group members consider gifts received/offered by employees of the Bank/Group members, as well as any hospitality expenses as a potential source of a conflict of interest.

The Bank establishes the minimal rules and restrictions as regards receipt/granting of gifts and services in the course of business communication associated with performance of job duties by employees of the Bank/Group members, as well as by the Bank's executives (namely, CEO, Chairman of the Bank's Executive Board, the Deputy Chairmen of the Bank's Executive Board, as well as the Chief Accountant of the Bank (hereinafter, "the Bank's executives)), including the lists and criteria of permitted and prohibited gifts, as well as occasions when they may be received/presented. Any prohibited gifts must be declined.

When establishing and maintaining business relations with customers/partners, including potential ones, employees of the Bank and the Group members should respect the restrictions related to anti-corruption measures publicly disclosed by such customers/counterparties on their official websites.

The procedure for handling gifts is stipulated by /10/.

6.2. Conflict of interest identification and assessment

All employees of the Bank/Group members, regardless of their job positions, shall take appropriate measures to identify conflicts of interest, including potential ones, namely the measures described in Clause 6.1. for conflict of interest prevention in all processes of the Bank/Group members, including development of new products and new business processes.

Potential conflicts of interest shall also be identified and assessed during inspections carried out with involvement, among others, of the Security Unit and the Internal Audit Unit.

The Bank has the Compliance Hotline, which is a safe and confidential channel for reporting any cases of personal interest and/or official abuses committed by the Bank's employees, as well as situations related to the Bank's employees having an unsettled conflict of interest or concealing information about existence of such a conflict of interest. The Compliance Hotline operates on a continuous basis using all available communication channels and technical means for automated receipt of reported information: their details are available on the Bank's official website.

If an employee reveals any information on an existing conflict of interest or probability of its occurrence, an employee shall immediately notify his/her line manager and/or the Compliance Unit. In case an employee has notified his/her line manager, but the latter has not taken adequate measures to prevent or eliminate an identified conflict of interest, or if implemented measures have not eliminated a conflict of interest, an employee shall report this to the Compliance Unit.

Heads of structural units of the Bank/Group members shall implement reasonable and adequate measures to resolve a conflict of interest, including a potential one.

If an employee of the Bank/Group member and/or his/her manager have any doubts whether a conflict of interest exists or regarding how to mitigate the risk of a conflict of interest and/or its consequences, an employee should seek help from the Compliance Unit of the Bank or the Group member respectively.

6.3. Conflict of interest resolution

For the purposes of management of conflicts of interest, including potential ones, the Bank and the Group members apply the following instruments for their resolution:

- restricting an employee's access to specific information that may be associated with such employee's personal interests
- voluntary refusal or (permanent or temporary) removal of an employee from a discussion, a decision-making process or other actions that may influence the subject of a conflict of interest
- change of an employee's job (official) duties and powers
- transfer by an employee of his/her securities being the subject of a conflict of interest into trust management
- refusal of an employee from the subject of his/her personal interest causing a conflict of interest, including a potential one
- banning an employee's access to relevant information when a high probability of occurrence of a conflict of interest is identified
- an employee's unsolicited dismissal
- employer-initiated dismissal of an employee for a breach of discipline, including failure to perform or improper performance of his/her job duties, in accordance with the labor legislation and employment contract with an employee.

Measures taken to manage and resolve a conflict of interest, including a potential one, depend, among other things, on the following:

- scope of a conflict of interest
- nature of a conflict of interest
- conditions of occurrence of a conflict of interest
- damage that may be inflicted to the Bank and the Group members, employees of the Bank/Group members, their customers, counterparties and other third parties in case of occurrence of a conflict of interest.

In order to avoid a conflict of interest, an employee of the Bank/Group member may not:

- represent the Bank/Group member in relations with entities whose operations are associated with an employee's considerable personal interest differing from interests of the Bank/Group member, including (but not limited to) cases when an employee and/or his/her relatives hold a dominant equity stake in the charter capital or are members in management bodies of such entities
- be involved in settling/concluding transactions/contracts with the Bank/Group member or any customers or suppliers, if an employee and/or his/her relatives are interested in a transaction/contract or can directly or indirectly benefit from such transaction, unless information about a transaction/contract, potential benefit and interest have been disclosed to the Compliance Unit and permitted by the Compliance Unit in writing
- use any confidential information received (learnt) by an employee in the course of performance of his/her duties for personal needs
- carry out activities during business hours related to membership in third parties' management bodies, doing business, rendering consulting or agency services, and combined job
- do business (including participate in the charter capital or be involved in management of legal entities) that has become possible taking into account one's position at the Bank/Group member, including through using business relations and opportunities of the Bank/Group member, unless the Bank has directly assigned such business or participation to an employee according to the stipulated procedure, i.e. for the purposes of performance by an employee of his/her professional duties

- work together with relatives in cases when one of relatives reports to or is functionally subordinate to another relative
- carry out internal checks in relation to a relative who is also employed at the Bank/Group member
- an employee of a controlling business unit of the Bank/Group member may not carry out checks and coordinate operations that are the responsibility of such employee's relative
- carry out control procedures and audit of operations of a business unit where such employee's relative is employed
- have any role in a project when its implementation is the responsibility of an employee's relative and/or an employee's relative is authorized to make key decisions on such project.

The Bank's executives are also prohibited from:

- being members of management bodies, boards of trustees or supervisory boards, and other bodies of foreign non-profit nongovernmental organizations and their structural units operating in the Russian Federation, unless otherwise is provided for by an international treaty of the Russian Federation or the effective legislation of the Russian Federation
- carrying out paid activities being financed solely from funds of foreign countries, international and foreign organizations, foreign citizens and stateless persons, unless otherwise is provided for by an international treaty of the Russian Federation of the effective legislation of the Russian Federation, without a written authorization[1]
- working at the Bank in case of immediate or in-law relationship (parents, spouses, children, brothers, sisters, as well as brothers, sisters, parents and children of spouses, and children's spouses) with an employee of the Bank, when work at the Bank involves direct subordination or accountability of one of them to another.

The list of restrictions and ways of resolving conflicts of interest provided in this Clause is not exhaustive. Other measures may be taken in each particular case in order to settle a conflict of interest, provided that they comply with the effective legislation.

When a conflict of interest, including a potential one, cannot be resolved by methods available in existing circumstances, the Bank/Group member may make a decision to decline a particular transaction or refuse to provide services to a particular customer, in order to prevent occurrence of reputational risk, legal risk, compliance risk and other risks for the Bank/Group member.

7. Specifics of organization of the conflict of interest management system at the Group members

7.1. The requirements hereof shall be applicable to the Group members and the system for managing conflicts of interest, including potential ones, shall be organized with account of the assumptions and provisions of /7/, as well as the scope, nature and area of operations of the Group member.

7.2. The Group members shall adopt the provisions similar to the ones established herein to the extent permitted by the local legislation. Such provisions shall be approved and implemented by the Group members' management bodies according to the stipulated procedure.

7.3. If the Group members introduce any amendments to IRDs devised based on the relevant IRDs of the Bank, such IRDs of the Group members shall be aligned with the Compliance Division of

[1] The authorization referred to in this Clause hereof shall be provided to CEO, Chairman of the Bank's Executive Board by the Bank's Supervisory Board; to the Deputies and the Chief Accountant it shall be provided by CEO, Chairman of the Bank's Executive Board.

the Bank’s Central Head Office in case of any discrepancies with the provisions hereof and other IRDs on compliance applicable to the Group members.

7.4. Functions and powers shall be distributed among participants of the conflict of interest management process within the Group members in compliance with the distribution and approaches stipulated in Clauses 5 and 6 hereof.

8. Liability of the Bank/Group members and their employees

8.1. Regardless of their job positions, all employees of the Bank/Group members are personally liable for compliance with the principles and requirements hereof, as well as for actions (inaction) of their subordinates violating these principles and requirements.

8.2. The Bank and the Group members may be subjected to sanctions for violations committed by their employees that have entailed a conflict of interest. Therefore, internal checks shall be carried out in case of any reasonable suspicion or revealed fact within the scope permitted by the effective legislation.

8.3. If an internal check reveals that certain employees are guilty of breaching the requirements hereof and other IRDs/OADs in the area of conflict of interest management, such employees may be subjected to disciplinary liability, up to dismissal, as well as to civil liability in accordance with the applicable legislation.

8.4. Persons found guilty pursuant by the court ruling may be subjected to civil or criminal liability according to the procedure and on the grounds provided for by the effective legislations.

9. Final provisions

9.1. In case any changes are introduced into the Russian and international laws, before approval of a new version hereof this Policy remains valid to the extent complying with the laws. If any traditions, customs or someone's ideas about appropriate rules of behavior contradict individual provisions hereof, this Policy shall prevail.

9.2. In case of any doubts regarding interpretation of the provisions and requirements hereof and their applicability to particular situations, the Compliance Division of the Bank’s Central Head Office is the only authorized business unit entitled to make a decision on their proper interpretation.

9.3. All employees of the Bank/Group members shall read and understand the provisions of this Policy in accordance with the procedure applicable at the Bank/Group member, which shall be confirmed by their signatures or electronic signatures, if the latter is technically possible.

Appendix 1

Terms and Definitions

Bank – Sberbank of Russia; Sberbank.

Close relatives – spouses, children and parents, adopters and adoptees, whole-blood and half-blood brothers and sisters, grandparents, grandchildren.

Group – Sberbank and credit and non-credit institutions controlled or significantly influenced by Sberbank, in accordance with /7/ and /18/.

Insider information (within this Policy) – information classified as insider information of the Bank and insider information of the Bank's customers and counterparties that has been disclosed to the Bank. Insider information is understood to mean accurate and specific information that has not been distributed or disclosed (including trade, official, banking secrets, communication secret (regarding details of postal money transfers) and other secrets protected by law), dissemination or disclosure of which may have a considerable impact on prices for financial instruments, foreign currencies and/or commodities.

Customer – an individual or a legal entity receiving services from the Bank.

Counterparty – an individual or a legal entity being a party to a contract with the Bank that is not a customer of the Bank.

Confidential information (within this Policy) – information constituting trade secret, personal data and banking secret. Confidential information also implies private information that is not publicly available, or information disclosed by an external source (such as a customer of the Bank or any other third party) on the conditions of its confidentiality and its use solely for the purposes for which it has been disclosed. Confidential information may exist in any form (written, verbal, electronic or any other).

Conflict of interest – a direct or indirect contradiction between property and other interests of the Bank/Group members and/or their employees and/or one or more of their customers and/or counterparties, as a result of which actions (inaction) of one party may entail adverse consequences for the other party.

A conflict of interest arises, among others, in a situation where (direct or indirect) personal interest of an employee of the Bank influences or can influence proper, fair and unbiased performance of his/her job duties (exercising of his/her powers).

An employee's personal interest that influences or can influence proper performance of his/her duties shall mean possibility for an employee to receive income from third parties in the course of performance of his/her duties in the form of cash, valuables, other property or property-related services, other property rights or benefits for himself/herself or for third parties.

Contradictions between the Bank's business units and contradictions arising during negotiations on commercial conditions in the normal course of business, the terms of which have been disclosed or should have been known to a negotiating party, shall not be deemed a conflict of interest.

Competing organization/competitor – an organization doing business in the following areas: banking and investment banking, insurance, lease, valuation, asset management, electronic payments, organization of electronic trading platforms, services for compilation, processing and storage of credit histories, digital companies and enterprises.

Gifts – any valuables in tangible or intangible form not involving an obligation to pay a regular price for them, including cash, securities and other property, benefits and property-related services (works, services, paid entertainment, leisure, transportation, loans, discounts, provision of property for use, including housing; charitable contributions, donations, etc.), received or granted in connection with one's employment at the Bank or the Group member. The following may also be deemed to be a gift:

- business breakfast / lunch /dinner
- entertainment event
- educational event.

Security Unit – the Intrabank Security Division of the Bank's Central Head Office (hereinafter, "the ISD") and/or regional sections of the ISD of the serviced regional banks.

Compliance Unit – the Compliance Division of the Bank's Central Head Office and/or the compliance units of the regional banks and/or the relevant business units of the Group members.

Legal risk – risk defined in accordance with /12/.

Bank employee – an individual having employment relations with the Bank or the Group member.

Reputational risk (risk of losing business reputation) – risk defined in accordance with /17/.

Compliance risk – risk defined in accordance with /16/.

Relatives (within this Policy) – close relatives, family members, as well as cousins, stepchildren, uncles and aunts, nephews and nieces, parents-in-law, spouses of children and parents.

Internal Audit Service – a complex of the Bank's structural units (the Internal Audit Division ("the IAD") of the Bank's Central Head Office and the IADs of the regional banks) carrying out their activities in accordance with the Statute on the Bank's Internal Audit Service.

Group Member – a legal entity being a member of the Group, other than the Bank.

Family members of an employee (within this Policy) – persons living together with an employee and running a common household with him/her, regardless of the relation degree, as well as any persons who are financially dependent on an employee or whom an employee is financially dependent on.

Appendix 2

References

1. Federal Law No. 224-ФЗ (224-FZ) “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” dated 27/07/2010
2. Federal Law No.39-ФЗ (39-FZ) “On the Securities Market” dated 22/04/1996
3. Federal Law No. 273-ФЗ (273-FZ) “On Counteracting Corruption” dated 25/12/2008
4. Civil Code of the Russian Federation
5. Code of Administrative Offences of the Russian Federation No.195-ФЗ (195-FZ) dated 30/12/2001
6. Regulation No. 242-П (242-P) dated 16/12/2003 “On the Organization of Internal Controls in Credit Institutions and Banking Groups”
7. Sberbank’s Compliance Risk Management Policy No. 2885 dated 01/04/ 2013
8. Sberbank’s Policy on Countering Unlawful Usage of Insider Information and Market Manipulation No. 4757 dated 14/02/2018
9. Sberbank’s Procedure for Handling Documents Containing Confidential Information No. 1091-2-p (1091-2-r) dated 18/07/2005 (as amended as of 18/11/2014)
10. Sberbank’s Book of Standards on Compliance Risk Management No. 4403 dated 29/11/2016
11. Sberbank Group’s Risk and Capital Management Strategy No. 3960-3 dated 17/04/2018
12. Sberbank Group’s Legal Risk Management Policy No. 3205-3 dated 28/12/2017
13. MiFID of the European Union (Markets in Financial Instruments Directive)
14. Regulation on Sberbank’s Compliance Committee No. 2886-2 dated 21/02/2017
15. Regulation on the Compliance Committee of Sberbank’s Regional Bank No. 2887-2 dated 21/02/2017
16. Regulation on Sberbank’s Internal Control Service No. 3497 dated 25/09/2014
17. Sberbank Group’s Reputational Risk Management Policy No. 4094 dated 18/12/2015
18. Policy on Sberbank’s Participation in Profit and Non-Profit Organizations (Except Foreign Banks) No. 2240-4 dated 30/03/2018.

Appendix 3

Conflict of Interest Examples

1. An employee abuses his/her powers when performing his/her job duties for personal advantage and to the detriment of a customer's interests.

2. An employee takes part in making HR decisions in relation to his/her close relatives, family members and other persons whom his/her personal interest is associated with.

3. An employee is involved in making decisions on purchasing goods owned/managed directly by an employee or by other persons whom his/her personal interest is associated with.

4. An employee has combined job at the Group member when his/her job duties at the Bank involve control powers in relation to such Group member.

5. An employee checks operations of a business unit where his/her relative is employed.

6. An employee uses information that has become known to him/her within his job (functional) duties in order to obtain benefits or competitive advantages when concluding commercial transactions for himself/herself or another person whom his/her personal interest is associated with.

7. An employee renders investment advice to customers on transactions solely in financial instruments issued by the Group member to the detriment of other financial market participants. Assets are acquired into one's portfolio relying on nonpublic information related to a potential transaction(s).

8. An employee participates in preparing an analytical report on an issuer whose securities are associated with an employee's personal interest.

9. The Group has its own investments in securities of an issuer and concurrently provides investment consulting services to customers in relation to the same issuer.

10. An employee works within a team consulting a customer on potential transactions with an issuer whose securities are associated with an employee's personal interest.

11. An employee carries out his/her own transactions to the detriment of similar transactions of a customer.