Approved by Order of

JSCB Togliattikhimbank (CJSC)

No. 52 dated 28.04.2015

# AGREEMENT

**of E-Banking Using the "iBank" System**

# (accession agreement)

**(as amended by Order No. 11 dated 31.01.2019)**

Togliatti, 2019

**TABLE OF CONTENTS**

1. TERMS AND DEFINITIONS …………………………………………………3

2. GENERAL PROVISIONS ………………………………………………………….7

3. REPRESENTATIONS AND WARRANTIES OF THE PARTIES ………………………………..8

4. SERVICE PROCEDURE …………………………………………………10

5. RIGHTS AND LIABILITIES OF THE PARTIES …………………………………………15

6. COST OF SERVICES AND SETTLEMENT PROCEDURE ……………………………22

7. LIABILITIES OF THE PARTIES ………………………………………………23

8. PROCEDURE FOR AMENDING AND/OR SUPPLEMENTING

THE AGREEMENT AND/OR THE BANK'S FEES ………………………………………25

9. PUBLICATION OF INFORMATION ………………………………………25

10. TERM AND TERMINATION ………….26

11. FINAL PROVISIONS …………………………………………27

# TERMS AND DEFINITIONS

**AWS** – an automated workstation (computer) from which the Client works with the "iBank" System.

**MC Attack** – the impact of MC on automated systems, software, workstations, computer equipment, telecommunication equipment, carried out locally or via information and telecommunication networks, including the Internet.

**Authentication** – an authentication procedure.

**Bank** – Joint Stock Company Togliattikhimbank.

**MC Database** – a database containing samples of known MC signatures.

**Browser** – application software used by the Client to operate the "iBank" System, designed for browsing websites, content of web documents, computer files and their directories, managing web applications, requesting web pages, processing them, their output and switching from one page to another, as well as for other tasks. The names of the browsers allowed to be used by the Client when working with the "iBank" System, as well as their versions, are given in the documentation for the respective service channels (interfaces, modules) of the "iBank" System, which is available on the Bank's website at https://ibank.thbank.ru.

**Certificate Holder** – an authorised person in whose name a Public DS Key Certificate is issued and who holds the corresponding Private DS Key, which allows creating his/her/its own DS in the ED using the means of the DS.

**Malicious Code (MC)** – a computer program designed to infiltrate automated systems, software, computer hardware, telecommunication equipment resulting in the destruction, creation, copying, blocking, modification and (or) transfer of information (including that protected in accordance with clause 2.1 of Regulation No. 382-P), as well as creating conditions for such destruction, creation, copying, blocking, modification and (or) transfer.

**Agreement** – this Agreement of E-Banking Using "iBank" System.

**Private (secret) DS key** – a unique sequence of characters generated by an authorised person using "iBank" System and intended for creating the DS in the ED.

**MC Protection** – the organised activity of protecting automated systems, software, computer hardware and telecommunications equipment against MC Attacks and eliminating their consequences.

**Security Software** – specialised software used to implement protection against MC**.**

**Other Equipment** – a specialised software and hardware device (equipment) provided by the Bank to the Client that generates one-time passwords.

**Other Confirmation** – one-off passwords obtained using Other Equipment.

**Communication Channel** – a channel for transmitting information, including the Internet, enabling Clients to independently transmit to and receive information from the Bank via public telecommunication channels.

**Card** – a card with specimen signatures and a seal (form 0401026 under OKUD (General Russian Classification of Management Documentation)) submitted by the Client to the Bank for opening of the Client's Account and executed in accordance with Instruction of the Bank of Russia No. 153-I dated 30 May 2014 "On Opening and Closing of Bank Accounts and Deposit Accounts".

**Client** – a legal entity or an individual entrepreneur who has at least one bank account with the Bank or another banking service agreement providing for electronic document management via the "iBank" System and has entered into this Agreement with the Bank.

**Access Code** – a unique digital code given by the Client's Authorised Person to whom the Client has authorised the use of the service channels (interfaces, modules) "Mobile Bank for Smartphones" and "Mobile Bank for Tablets", which is known only to that Client's Authorised Person. The Access Code is stored in encrypted form in the secret storage of the Mobile Device's operating system. The Access Code cannot be recovered. If the Access Code is lost or misplaced, it must be reset.

A fingerprint can be used as the Access Code on devices equipped with the appropriate sensors. The operating system of the Mobile Device is used to process the fingerprint information, and the fingerprint information does not leave the Mobile Device. The Bank does not process biometric personal data. Touch ID and Android Fingerprint Authentication are supported.

**Comprometation** – the fact that an unauthorised person has access to, or is suspected of accessing, protected information.

**DS Comprometation** – an event the occurrence of which results in a loss of confidence that the DS used ensures the security of information.

Events of DS Comprometation include, but are not limited to, the following:

* loss (including theft) of the DKH;
* loss of the DKH followed by discovery;
* dismissal (transfer to another job) of the Client's Authorised Person who had access to the key information recorded on the DKH;
* violation of the rules for storing the Private (Secret) DS Key;
* unauthorised copying or suspected unauthorised copying of the Private (Secret) DS Key;
* suspicion of information leakage or misrepresentation;
* cases where the DS is recognised as an incorrect DS;
* the unauthorised person's knowledge of the Private (Secret) DS Key, or suspicion that such knowledge has taken place;
* access by unauthorised persons to the DKH or suspicion that such access has taken place;
* cases where it cannot be reliably established what has happened to the DKH (including cases where the DKH has failed and/or the possibility that this fact has occurred as a result of unauthorised actions by unauthorised persons has not been proven);
* other circumstances directly or indirectly indicating the possibility of unauthorised access by third parties to the Private (Secret) DS Key.

**MC Checks** – continuous, periodic or occasional checks of automated systems, software, computer hardware and telecommunications equipment to detect MC.

**Correct DS (DS Correctness)** – the DS in the ED, the Public DS Key validity term of which has not expired (the DS is not blocked or terminated), whose verification with the Public DS Key gives a positive result of the DS belonging to the Certificate holder's ED (confirms the DS authenticity in the ED) and absence of alterations in the ED signed with the DS.

**Mobile Phone** – the Client's portable device intended for operative mobile communication with the Client's Authorised Persons, for sending SMS messages being SMS confirmation, SMS notification as well as SMS messages within the SMS Notification Service to the Client's Authorised persons.

**Mobile Device** – the Client's portable device, such as a smartphone or tablet computer, used for the provision of E-Banking Services via the "Mobile Bank for Smartphones" and "Mobile Bank for Tablets" service channels (interfaces, modules).

**Mobile Control** – enabling the Client to monitor the Account(s) by means of the Mobile Device. Provided when using "Information" mode

service channels (interfaces, modules) "Mobile Bank for Smartphones" and "Mobile Bank for Tablets".

**Mobile Application** – specialised software installed on the Client's Mobile Device. Is an integral part of the service channels (interfaces, modules) of "Mobile Bank for Smartphones" and "Mobile Bank for Tablets". The developer of the mobile applications is BIFIT JSC.

**Digital Key Holder (DKH)** – a removable medium designed to store and use the Client Authorised Person's DS key pair. For example: floppy disk, compact disk (CD/DVD), USB flash drive (flash drive), special device for digital signature keys storage, special digital key holder (SDKH).

**Processing of Personal Data** – any action (operation) or set of actions

(operations) performed with or without the use of automation means with personal data of individuals, including collection, recording, systematization, accumulation, storage, clarification (updating, change), extraction, use, transfer (provision, access), anonymization, blocking, removal and destruction.

**Public DS Key** – a unique sequence of characters corresponding to the Private (Secret) DS Key generated by the Client's Authorised Person using the "iBank" System and intended to confirm the correctness of the DS in the ED.

**No Alteration of the ED** means that the ED has been created in the "iBank" System without deviations from the "iBank" System technology, that no alterations have been made to the content of the ED after its creation and signing by the DS.

**DS Key Pair** – a Private (Secret) DS Key and its corresponding Public DS Key.

**Software** – package of computer programs.

**Regulation No. 382-P** – Regulation of the Bank of Russia No. 382-P dated 09.06.2012 “About requirements to ensuring information security when implementing money transfers and about procedure the Bank of Russia of control of observance of requirements to ensuring information security when implementing money transfers”.

**"Indicator" Service** – a service provided to the Client through the "Internet Bank", "Mobile Bank for Smartphones" and "Mobile Bank for Tablets" service channels (interfaces, modules), designed to check the reliability of counterparties based on information from publicly available sources. Based on the results of this Service, the Client receives a list of facts about the recipient of the payment, which enables a conclusion to be drawn about the current status of the counterparty.

**Public DS Key Certificate** – a hardcopy document with the Public DS Key represented in hexadecimal form, the start and end date of the Public DS Key, the signature of the Certificate Holder, and intended to verify the correctness of the DS and identify the Certificate Holder.

**Internet** – the information and telecommunication network "Internet".

**iBank" System ("iBank 2" System)** – a corporate information system, a set of software and hardware tools operated by the Client and the Bank in concert, as well as organisational measures carried out by the Client and the Bank in order to provide services to the Client in accordance with this Agreement. The "iBank" System software was developed by BIFIT JSC. Trademark No. 182 "iBank" is owned by BIFIT JSC based on Trademark Certificate No. 182 dated 11 May 2017.

In addition to the name "iBank" System, the identical name "iBank 2" System may also be used in the developer's documentation.

The "iBank" System consists of:

* the Bank's software and hardware operated by the Bank at its own expense;
* software and hardware tools (AWS), completed and operated by the Client at the Client's own expense;
* the software and hardware means of communication that enable the exchange of EDs between the Parties;
* the "iBank" System software installed on the Client's AWS and operated independently by the Client;
* A Mobile Application installed on the Client's Mobile Devices and independently operated by the Client.

The software module "Cryptographic Information Security Tool "Crypto-COM 3.4", rev. 40/41", providing hashing, digital signature, encryption of the file container of the Private (Secret) DS Key that is part of the "iBank" System is certified in accordance with the current legislation of the Russian Federation and ensures information protection in accordance with the following standards: GOST R 34.10-2012, GOST R 34.10-2001, GOST R 34.11-2012, GOST R 34.11-94.

The list of the Bank-supported service channels (interfaces, modules) of the "iBank" System permitted for use by the Client shall be determined by the Bank and specified in this Agreement. If the Bank allows the Client to use several service channels (interfaces, modules) of the "iBank" System simultaneously, the Client shall have the right to use any of them at his/her/its discretion, taking into account all possibilities, features and risks specified in this Agreement and in the respective user manuals for using each of the service channels (interfaces, modules) of the "iBank" System. The service channels (interfaces, modules) of the "iBank" System that are permitted to be used by the Clients of the Bank are:

"iBank for 1C", "Mobile Bank for Smartphones" and "Mobile Bank for Tablets" in

"Info" and "Internet Bank" mode.

**Special Digital Key Holder (SDKH)** – a removable specialised hardware and software device (token, etc.) with integrated operating system with built-in Cryptographic Information Protection Facility (CIPF), connected to the Client's AWS, intended for storage and use of the Client's Authorised Person's DS Key Pair. The SDKH provided to the Client by the Bank is certified in accordance with the current legislation of the Russian Federation and provides DS in accordance with GOST R34.10-2001 standard.

**MC Safeguards** – software and hardware tools used to implement protection against MCs.

**Parties** – the Bank and the Client.

**Client's Account** – the Client's bank account opened with the Bank and connected to the "iBank" System. **Bank's Tariffs** – the Bank's commission fee rates approved by the Bank's authorised management body for servicing accounts of legal entities and/or

individual entrepreneurs.

**Client's Emergency Telephone Number** – the Mobile Phone Number specified in the Public DS Key Certificate of the Client's Authorised Person with the right of first signature of the ESD, using which Bank shall promptly inform the Client at any time (24/7) in accordance with the terms and conditions of this Agreement.

**Bank's Authorised Person** – an individual, an employee of the Bank authorised to work in the "iBank" System.

**Client's Authorised Person –** an individual, who is:

1. the sole executive body of the corporate Client or individual entrepreneur, or a person engaged in private practice and/or other person(s), who is (are) the Client's employee(s), indicated in the Card and empowered in accordance with the current legislation of the Russian Federation with the first and/or second signature on the settlement documents;
2. the sole executive body of the corporate Client or individual entrepreneur, or a person engaged in private practice (when entering into this Agreement for the purpose of execution of the Cash Services Agreement for legal entities, individual entrepreneurs, persons engaged in private practice).

**Electronic Document (ED)** – a document presented in electronic digital form in the form of a file (or database entry) prepared by means of

the "iBank" System software and signed with the DS. If a document (letter, message) to be sent using the "iBank" System contains files attached thereto, both the document itself and the files attached thereto are signed with the sender's DS simultaneously, and the document with attached files constitutes a single document signed with one DS.

**Electronic Settlement Document (ESD)** – an ED, which is the basis for transactions on the Client's Account, signed with the DS of the Client's Authorised Persons, prepared using the "iBank" System software and which has the same legal effect as a settlement document submitted in hard copy.

**Digital Signature (DS)** – an ED requisite intended to protect such ED from forgery, obtained as a result of cryptographic transformation of information using the Private (Secret) DS Key and allowing to identify the Certificate Holder, as well as to establish the absence of information corruption in the ED.

**IP-Filtering** – allowing access to the "iBank" System only from one or more computers with specific IP addresses. Information sent to the Bank shall only be processed if the public (Internet-accessible) IP-address (address range) of the Client's AWS or local network matches the IP-address (address range) of the Client stored in the Bank's database. **SMS, e-mail informing** – a service of sending SMS messages to the Client's Mobile Phone Number and/or e-mail messages to the Client's

e-mail address in accordance with the terms and conditions of this Agreement.

**SMS Confirmation** – the use of SMS messages containing one-time passwords sent by the Bank to the Client's Mobile Phone Number indicated in the "iBank" System in accordance with the terms and conditions of this Agreement.

**SMS, e-mail notification** – sending of SMS messages to the Client's Mobile Phone Number or e-mail messages to the Client's e-mail address in order to notify the latter of transactions made on the Client's Account(s).

**iBank for 1C** – service channel (interface, module) of the "iBank" System, designed for remote banking services directly from the user interface of 1C:Enterprise application software systems.

**Mobile Bank for Tablets** – a service channel (interface, module) of the "iBank" System designed for the Client's use of the "iBank" System via Mobile Devices – tablets. The use of this module requires the installation of the Mobile Application on the Client's Mobile Device(s). The specifics of using this interface are described in the "Internet Bank for Corporate Clients" ("Internet Bank for Corporate Clients (Web Interface)") User Guide, available on the Bank's website at [https://ibank.thbank.ru.](https://ibank.thbank.ru/)

**Mobile Bank for Smartphones** – a service channel (interface, module) of the "iBank" System designed for the Client's use of the "iBank" System via Mobile Devices – smartphones. The use of this module requires the installation of the Mobile Application on the Client's Mobile Device(s). The specifics of using this interface are described in the "Internet Bank for Corporate Clients" ("Internet Bank for Corporate Clients (Web Interface)") User Guide, available on the Bank's website at https://ibank.thbank.ru.

**Internet Bank** – a service channel (interface, module) of the "iBank" System intended for use by the Client via the AWS (personal computer). The specifics of using this interface are described in the "Internet Bank for Corporate Clients" ("Internet Bank for Corporate Clients (Web Interface)") User Guide, available on the Bank's website at [https://ibank.thbank.ru.](https://ibank.thbank.ru/)

# GENERAL PROVISIONS

* 1. Under this Agreement, the Bank shall provide the Client, and the latter shall pay for the following services provided by the Bank (depending on the agreement already concluded between the Bank and the Client):
     1. accepting and executing the Client's ESDs for non-cash settlements on the Client's Accounts opened with the Bank:

in Roubles:

* Payment orders;
* Applications for a letter of credit;
* Collection orders;
* Payment requests;
* Declarations of acceptance (including pre-approved acceptance);
* Statements cancelling the acceptance given in advance;
* Applications for cash;
* Applications for an irreducible balance;
* Applications for deposits in foreign currencies:
* Applications for transfer;
* Orders to buy or sell (compulsory) foreign currency;
* Orders to sell back foreign currency;
* Currency conversion orders;
* Applications for an irreducible balance;
* Applications to open deposits.
  + 1. to accept copies of the following documents that are the basis for the settlement transactions from the Client:
* agreements;
* invoices;
* consignment notes, etc;
  + 1. acceptance of documents from the Client which are the basis for a currency exchange transaction on the Client's account in accordance with Part 4 of Article 23 No. 173-FZ "On Currency Regulation and Currency

Control" with the files attached thereto:

* Transaction certificates under contracts;
* Transaction certificates for loan agreements;
* Applications for reissuance of transaction certificates;
* Currency transaction certificates;
* Currency receipts certificates;
* Certificates of supporting documents;
* other foreign exchange control documents;
  + 1. accepting EDs from the Client when executing other banking service agreements that provide for electronic document flow through the "iBank" System (cash service agreements for legal entities, individual entrepreneurs, persons engaged in private practice):
* Payroll registers for the Client's employees;
  + 1. accepting other documents from the Client:
* Registers of documents submitted for collection;
* Letters and other documents drawn up in any form;
* Feedbacks;
* Confirmations of transactions;
* Confirmation of balances.
  1. This Agreement establishes the procedure of interaction between the Parties when carrying out electronic document flow using the "iBank" System.
  2. This Agreement is a standard form of the Bank for all Clients and an adhesion agreement in accordance with the applicable laws of the Russian Federation.
  3. The Bank shall publish this Agreement for the purpose of making the Client aware of the terms and conditions of this Agreement in the manner prescribed in Section 9 hereof.
  4. Conclusion of this Agreement between the Parties shall be effected by the Client's accession to this Agreement in accordance with Article 428 of the Civil Code of the Russian Federation, and shall be effected by the Bank's acceptance (the Bank's registration mark and assignment of the Agreement number in the registration program for contracts concluded by the Bank) of the **APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System**, prepared on paper **in the form of Appendix No. 1 hereto**.
  5. The rights and obligations of the Parties shall arise from the date of the conclusion of this Agreement. The date of conclusion of this Agreement shall determined and confirmed by the Bank's mark of acceptance (the Bank's registration mark and assignment of the Agreement number in the registration program for contracts concluded by the Bank) of the **APPLICATION for Accession to the Agreement of E-Banking Using "iBank" System (Appendix No. 1 hereto).** The Bank shall mark the acceptance after checking the information and documents submitted by the Client and their compliance with the terms and conditions of the "iBank" System.
  6. The Client's procedure for entering into this Agreement and connecting the Client (the Client's Authorised persons) to the "iBank" System shall be specified in the **Client's "iBank" System Connection REGULATION (Appendix No. 2 hereto).**
  7. This Agreement shall apply to all of the Client's Accounts connected to

the "iBank" System.

* 1. The Client's Account shall be connected to the "iBank" System in accordance with **the APPLICATION for Accession to the Agreement of E-Banking Using "iBank" System (Appendix No. 1)** or **the APPLICATION for Connection/Disconnection of the Client's Account to the "iBank" System (Appendix No. 3 hereto)**.
  2. This Agreement shall form an integral part of the respective bank account agreement governing the relationship between the Parties in servicing the Client's Account or the Cash Services Agreement for legal entities, individual entrepreneurs and persons engaged in private practice.

# REPRESENTATIONS AND WARRANTIES OF THE PARTIES

* 1. The Parties acknowledge that the software module

"Cryptographic Information Security Tool "Crypto-COM 3.4", rev. 40/41", as well as

the software used together with the "iBank" System, which provides encryption, integrity control, access delimitation and signing of the EDs with Correct DS, as well as the SDKHs permitted for use by the Client together with the "iBank" System, are sufficient to ensure the confidentiality of information during its transmission over data transmission networks, including the Internet, protection of transmitted information from unauthorised access, control of the integrity of EDs, confirmation of authorship and authenticity of EDs.

* 1. The Parties acknowledge that the "iBank" system and communication channels used by them under this Agreement are sufficient to ensure reliable and efficient operation in processing, storing, receiving and transmitting information.

# Requirements for Ensuring Information Security of "iBank" System

**are set out in Appendix 4 hereto.**

The level of information security at work in the "iBank" System can be increased by activation of IP-filtering**, SMS Confirmation or Other Confirmation modes using the equipment provided by the Bank to the Client, as well as SMS, e-mail informing services.**

* 1. The Parties acknowledge that forging of the DS of the authorised persons of the Parties, i.e. creation of the Correct DS of the ED on behalf of the Parties, is not possible without knowledge of the Private (Secret) DS Keys of the respective DS of the authorised persons of the Parties.
  2. The Parties acknowledge that the confirmation of the DS Correctness by the Public DS Key during the transmission of the ED enables to reliably establish that the ED comes from the Contracting Party, whose authorised person's DS is contained in the ED and is authentic.
  3. The Parties acknowledge that after signing the ED, changing, adding or deleting characters of the significant data of the DS (data involved in the calculation of the DS) makes the DS invalid, i.e. the verification of the DS gives a negative result.
  4. The Parties acknowledge that an arbitrary alteration of an ED certified with the DS means that the ED has been created in the "iBank" System with deviations from the "iBank" System technology, that the ED has been created with distortion.
  5. The Parties acknowledge that the Client's Authorised Person's Public DS Key contained in the Certificate Holder's Public DS Key Certificate belongs to the relevant Client's Authorised Person.
  6. The Parties acknowledge that the receipt of duly executed EDs signed by the other Party's authorised persons is legally equivalent to the receipt of paper documents signed by authorised persons and executed in accordance with the requirements of the applicable laws of the Russian Federation and the regulations of the Bank of Russia. The Parties shall have the right to use EDs signed with the required number of DSs in the same way as signed and sealed paper documents.
  7. The Parties acknowledge that scanned copies of the documents transmitted as attached files via the Communication Channels using the "iBank" System, together with the covering letter signed with the required DS, are legally equivalent to receiving copies of the documents certified in accordance with the requirements of the applicable laws of the Russian Federation.
  8. The Parties acknowledge that the receipt by the Client of the Client's Account Statements signed with the Bank's Authorised Person's DS is equivalent to the receipt of the Client's Account Statements in hard copy.
  9. The Parties acknowledge that EDs with DSs transmitted via the "iBank" System shall serve as evidence for resolution of disputable issues, which shall be settled in accordance with the **PROCEDURE for Dispute Resolution due to the use of EDs (Appendix No. 5 hereto)**. EDs that do not have the necessary number of DSs are not evidence material if there are disputed issues.
  10. The Parties guarantee that the information contained in the EDs generated and transmitted under this Agreement will remain confidential and accurate.
  11. The Parties acknowledge that all statements, notifications, acts provided for in this Agreement and set out in the appendices to the Agreement, except for:

# APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System (Appendix No. 1 hereto);

* **The Client's "iBank" System Connection Certificate (Appendix No. 7 hereto);**

# The Equipment Acceptance Certificate (Appendices Nos. 12-A, 12-B hereto);

* **NOTICE of Termination (Appendix No. 13 hereto),**

may be submitted by the Client to the Bank both on paper and in the form of the ED signed by the Client's Authorised Person's DS and sent via the "iBank" System.

* 1. The Parties acknowledge that the following cryptographic encryption/ hashing algorithms used for data encryption during transmission over the Internet are sufficient to ensure confidentiality of information during its transmission over data transmission networks, including the Internet, and to protect transmitted information from unauthorised access:
     1. For iBank for 1C service channel (interface, module): TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
     2. For "Mobile Bank for Smartphones" and

"Mobile Bank for Tablets" service channels (interfaces, module) depending on the Mobile Device operating system used by the Client, and for "Internet Bank" service channel (interface, module) depending on the Browser used by the Client and the AWS operating system: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, RSA\_WITH\_AES\_128\_CBC\_SHA256.

* 1. The Client shall agree to receive services through the "iBank" System via the Internet, being aware that the Internet is not a secure communication channel, and agree to bear all risks associated with the connection of his/her/its AWS and Mobile Devices to the Internet, possible breach of confidentiality and integrity of information when working through the Internet. The Parties also acknowledge that the failure of the Client's AWS, Mobile Devices as a result of third party intervention via the Internet shall be deemed to be the failure due to the Client's fault.
  2. The Parties acknowledge that the creation of a Correct ED DS is only possible by using the DS Key Pair.
  3. The Parties acknowledge that it is not possible to identify the Private (Secret) DS Key from the content of the DS signed ED and the Public DS Key;
  4. The Parties acknowledge that Client is fully liable for ensuring the confidentiality and security of its Private (Secret) DS Keys and for the actions of his/her/its personnel.
  5. The Parties acknowledge that the Client may have several DS Key Pairs, with each Private (Secret) DS Key corresponding to his/her/its own Public DS Key.
  6. The Parties acknowledge that the EDs signed with the Client's DS, as well as the ED logs kept in the "iBank" System and the logs of the Client's actions in the "iBank" System may be submitted by the Bank as evidence in case of a dispute arising from the use of the "iBank" System.
  7. The Client's authorised persons shall form their own DS Key Pairs in the course of a session with the "iBank" System.
  8. The Client recognises all EDs sent by it or received via the "iBank" System as equivalent to paper documents signed with the handwritten signatures of authorised officials and the seals (if any) of the Parties.
  9. The Parties acknowledge that all the Applications named as appendices hereto, except for the **APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System (Appendix No. 1** hereto**), as well as the NOTICE of Termination of the Agreement of E-Banking Using "iBank" System** in the form of **Appendix No. 13** hereto, may be submitted to the Bank either in hard copy or as an ED via the "iBank" System.

# APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System (Appendix No. 1 hereto), as well as the NOTICE of Termination of the Agreement of E-Banking Using "iBank" System (Appendix No. 13 hereto) shall be submitted to the Bank only in hard copy.

3.24 The Parties acknowledge that the date and time of SMS or e-mail message sending to the Client, which is an SMS confirmation, SMS, e-mail notification, or a message under the SMS, e-mail notification service, shall be the date and time determined by the system clock of the Bank's hardware at the time of recording information about the message sending

in the "iBank" System operating protocol.

# SERVICE PROCEDURE

* 1. **General terms and conditions of service under this Agreement:**
     1. The Bank shall service the Client using the "iBank" System in accordance with this Agreement, the regulations of the Bank of Russia, and the applicable laws of the Russian Federation.
     2. The Bank shall accept EDs transmitted via the "iBank" System around the clock, except for the time when the Bank carries out maintenance works in the "iBank" System, of which the Bank shall notify the Client at least 1 (one) calendar day before the start of the maintenance works by sending a respective notice via the "iBank" System.

Other obligations under this Agreement shall be fulfilled by the Bank daily from 9:00 a.m. to 5:15 p.m. (Friday from 9:00 a.m. to 4:00 p.m.) local time, except on weekends and public holidays.

* + 1. EDs sent by the Client to the Bank using the "iBank" System shall be prepared by the Client using document templates (forms) available in the "iBank" System, taking into account the requirements of regulatory acts of the Bank of Russia and applicable laws of the Russian Federation, and in the absence of such templates – in accordance with the requirements of regulatory acts of the Bank of Russia and applicable laws of the Russian Federation.

4.1.4 Terms for the implementation of the ESD:

А) For non-cash settlements on the Client's accounts opened in Russian roubles, the ESDs received by the Bank before 7.00 p.m. of the business day shall be accepted by the Bank for execution on the current day, the ESDs received after 7.00 p.m. of the business day shall be accepted by the Bank for execution on the next business day, except for the ESDs whose execution procedure and terms are established by other agreements between the Bank and the Client.

B) For non-cash settlements on the Client's Accounts opened in a foreign currency, as well as on the Client's transactions in Russian roubles, the ESDs containing attributes of a currency transaction in accordance with Federal Law No. 173-FZ dated 10.12.2003 "On Currency Regulation and Currency Control", which are received by the Bank on a business day before 4 p.m. and on Friday before 3 p.m. on a business day, shall be accepted by the Bank for execution on the current day. The ESDs received on a business day after 4 p.m. and on a Friday after 3 p.m. shall be accepted by Bank for execution on the next business day, except for the ESDs whose execution procedure and deadlines are established by other agreements between Bank and Client.

C) The Client's ED, which are the basis for settlement transactions, and the EDs, which are the basis for conducting a currency transaction on the Client's account in accordance with part 4 of Article 23 of Federal Law No. dated 10.12.2003 173-FZ "On Currency Regulation and Currency Control" with the files thereto received by the Bank on a business day before 4 p.m. and on Friday before 3 p.m. shall be accepted by the Bank on the current business day; the EDs received by the Bank on a business day after 4 p.m. and on Friday after 3 p.m. shall be accepted by the Bank on the next business day.

* + 1. ESDs received by the Bank for execution on a non-working day (day off and/or non-working holiday in accordance with the current legislation of the Russian Federation) shall be accepted by the Bank for execution on the next following working day.
    2. EDs sent by the Client to the Bank via the "iBank" System shall be signed with the Correct DS of the Client's Authorised Person authorised to sign the relevant ED in accordance with the applicable laws of the Russian Federation. If this requirement is breached, the ED will not be accepted by the Bank for execution.
    3. ESDs sent by the Client to the Bank via the "iBank" System shall be signed with the Correct DS of any Client's Authorised Person authorised under the applicable laws of the Russian Federation to give the first signature on settlement documents, and the Correct DS of any Client's Authorised Person authorised under the applicable laws of the Russian Federation to give the second signature on settlement documents (if any).

If this requirement is breached, the ESD will not be accepted by the Bank for execution.

* + 1. Upon receipt of the Client's ED, the Bank shall verify the correctness of the Client's Authorised Persons' EDs, including checking that the EDs are free of misrepresentations. If the Client's Authorised Person's DS is recognised as a Correct DS, including confirmation that the DS is free of misrepresentations, the Bank accepts the ED for execution. If the Client's Authorised Person's DS is recognised by the Bank as an incorrect DS, including if the DS is found to be corrupted, the ED will not be accepted for execution.
    2. Confirmation of the receipt of the Client's ED by the Bank is the change of the document to

the "Delivered" status in the "iBank" System.

* + 1. Confirmation of the execution or non-execution of the Client's ED by the Bank is the transition of the document in the "iBank" System from the status "Processing" to the status "Executed" or "Rejected" (indicating the reason for non-execution).
    2. The "iBank" System enables the Client to view the Client's account statements at any time. If the status of the statement in the "iBank" System is shown as "Preliminary", the information on the Client's Account transactions is not final. The final status of the statement shall be set by the Bank no later than 1 p.m. on the business day following the day of transactions on the Client's Account.

If the Bank has provided the Client with duly executed documents via the "iBank" System (EDs signed with the Bank's DS), the Bank shall reserve the right to refuse to provide the Client with paper copy of the Client's Account Statements and executed ESDs submitted to the Bank via the "iBank" System and other EDs.

* + 1. The "iBank" System uses the local time at the location of the Bank as the standard time scale. The reference time is the time set on the system clock of the Bank's hardware.
    2. The Client shall independently and at its own expense ensure the connection of his/her/its own AWS and Mobile Devices to the Internet, access to the Internet, and protect his/her/its own AWS, Mobile Devices, Access Codes, DKH, SDKH, Other Equipment from unauthorised access and exposure to MC.
    3. When exchanging an ED, the date of receipt of the ED is the date of delivery of the ED by the "iBank" System, the Send Date is the date of transmission of the ED to the "iBank" System.
    4. The aggregate size of attached files sent via the System, including those packed by data compression software, shall not exceed the size specified in the System.
    5. The documentation on the use of the "iBank" System, which is available on the Bank's website at https://ibank.thbank.ru, as it is amended by the developer

of the "iBank" System, may be changed by the Bank at any time to a more up-to-date version without prior notice to the Client.

# Registration (activation) / blocking / unblocking / termination (cancellation) of the Client's Authorised Person' DS:

* + 1. The validity period of the Client's Authorised Person's DS is determined by the Bank, but cannot be more than 1 (one) year 3 (three) months from the date of registration (DS activation) of the Authorised Person's Public DS Key Certificate by the Bank. The validity period of the Client's Authorised Person's DS and the date of registration (DS activation) by Bank of the Authorised Person's Public DS Key Certificate shall be specified in the Public DS Key Certificate.
    2. The blocking (suspension)/ termination (revocation) of the DS (DS Key Pair) of the Client's Authorised Persons shall be performed at the Client's request or without such request (at the initiative of the Bank) in accordance with the terms and conditions of this Agreement.
    3. The Client's Authorised Person's DS (DS key pair) shall be blocked (suspended) by the Bank at the Client's request no later than the business day following the day on which the **APPLICATION to Block/Unblock/Terminate (Cancel) the DS** drawn up in the form of **Appendix 6** hereto is submitted to the Bank;
    4. The Client's Authorised Person's DS (DS key pair) shall be terminated (cancelled) by the Bank at the Client's request no later than the business day following the day on which the **APPLICATION to Block/Unblock/Terminate (Cancel) the DS** drawn up in the form of **Appendix 6** hereto is submitted to the Bank;
    5. The Client's Authorised Person's DS may be blocked (suspended)/ terminated (cancelled) by the Bank without the Client's application (at the Bank's initiative) in accordance with the terms of this Agreement on the day at least one of the following events occurs:
* the Bank has information about the DS Comprometation;
* powers of the Client's Authorised persons expires and documents confirming the extension of the powers of the Client's Authorised persons are not submitted to the Bank;
* the Client's Authorised Person's Public DS Key expires, as specified in the Public DS Key Certificate;
* the Client submits to the Bank of a **NOTIFICATION of Termination** of the Agreement

prepared on paper in the form of **Appendix No. 13** hereto;

* in other cases stipulated by the Russian Federation laws, documents (including methodological recommendations) of the Bank of Russia and this Agreement.
  + 1. The unblocking (renewal of validity) of the Client's Authorised Persons' DS shall be performed by the Bank:
* in case of blocking the Client's Authorised Persons' DS at the Client's initiative – not later than on the business day following the day of receipt of the **APPLICATION to Block/Unblock/Terminate (Cancel) the DS**, drawn up on paper in the form of **Appendix No. 6** hereto**;**
* in case of blocking the Client's Authorised Persons' DS at the initiative of the Bank – not later than on the business day following the day of termination of the circumstances that have given rise to the blocking of the DS.
  + 1. The blocked DSs of the Client's Authorised Persons shall cease to be valid if the Bank has not received an application from the Client to unblock them within the period specified in the Client's Authorised Person's Public DS Key Certificate.
    2. The Parties shall ensure the safekeeping of inactive DS (blocked DSs, DSs terminated (cancelled) at the Client's request or DSs whose Public DS Key has expired) in accordance with this Agreement.

Inactive DS shall be kept for the same period of time as the ED signed by such DS.

# IP-Filtering:

* + 1. When the Client is connected to the "iBank" System, the IP-Filtering mode is activated by the Bank only at the Client's request based on the **APPLICATION for Activation/Deactivation of IP-Filtering Mode/Change of IP Address in the "iBank" System**, drawn up according to the form of **Appendix No. 8** to this Agreement.
    2. The Client shall be entitled to refuse to use IP-Filtering mode in the "iBank" System, if such mode has been connected to the Client by the Bank.

The Bank shall disable the IP-Filtering Mode upon the Client's application no later than the business day following the day on which the Bank receives the **APPLICATION for Activation/Deactivation of IP-Filtering Mode/Change of IP Address in the "iBank" System** drawn up according to the form of **Appendix No. 8** hereto.

* + 1. The Bank shall enable the IP-Filtering Mode/Change of IP Address upon the Client's application no later than the business day following the day on which the Bank receives the **APPLICATION for Activation/Deactivation of IP-Filtering Mode/Change of IP Address in the "iBank" System** drawn up according to the form of **Appendix No. 8** hereto.
    2. The Bank shall not charge a fee for providing services related to activation/deactivation of IP-Filtering Mode, change of IP-address when working in the "iBank" System.

# SMS, e-mail notification service:

* + 1. Access to **SMS, e-mail** **notification** settings in the "iBank" System is chargeable and is provided only on the basis of the Client's application and the Client shall pay the Bank a relevant commission for this service in accordance with the Bank's Tariffs.
    2. The Client wishing to use **the SMS, e-mail notification service shall,** upon entering into this Agreement, shall make a relevant note **in the APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System (Appendix No. 1 hereto).**

The Client who has concluded this Agreement without simultaneous provision of **SMS, e-mail notification** service and wishes to use this service during the validity period of this Agreement, or who has concluded this Agreement with simultaneous provision of **SMS, e-mail notification** service and wishes to disable this service, shall submit to the Bank an **APPLICATION for Enabling/Disabling SMS, E-mail Notification** of the Client, drawn up in the form of **Appendix No. 9** hereto, containing respective notes.

* + 1. The Client shall set up the following types of notifications and the information contained therein independently in the "iBank" System:
* about viewing the Client's Account statement;
* about logging on to the "iBank" System;
* on the movement of funds in the Client's Account;
* on the receipt of an ED by the Bank;
* on the current balance of the Client's Account;
* about logging on;
* about incoming bank letters;
* on the movement of funds in the Account;
* Account Statement;
* on the receipt of the document by the Bank;
* on "Rejected" status of the document;
* on a change in the key status;
* on current balances;
* on changes to the monitoring parameters.

It is up to the Client to choose how the information messages are sent:

* SMS messages;
* e-mail messages;

# SMS – message:

* + 1. An SMS message sent to the mobile phone of the Authorised Person or another employee of the Client, containing a one-time password to be entered in the input fields offered by the "iBank" System, and which is used only to confirm the Client's right to access the "iBank" System.
    2. The Bank shall change the SMS confirmation phone number upon the Client's application not later than on the business day following the day when the Bank receives an **APPLICATION for Change of Information for SMS Confirmation, SMS, E-mail Notification in the iBank**

**System**, which is prepared according to the form of **Appendix No. 10** hereto.

* + 1. The Bank does not charge a fee for providing SMS confirmation services.

# Mobile Control Service.

**This service is chargeable and is provided only under the Client's application and the Client shall pay the Bank a commission for this service in accordance with the Bank's Tariffs.**

* + 1. When using the Service, the Client is given the opportunity to carry out the following activities using Mobile Devices:
* view a list of the Client's accounts;
* view the Client's account balances;
* receive statements of the Client's accounts;
* view a list of payment orders;
* view the selected payment order;
* view the bank details of the Client's Accounts;
* send the selected payment order to the printer.
  + 1. In order to receive the service, the Client may only use Mobile Devices that meet the technical requirements specified in the user manuals for the respective service channels (interfaces, modules): "Mobile Bank for Smartphones" and "Mobile Bank for Tablets", available on Bank's website at https://ibank.thbank.ru.
    2. The Client may perform the following actions using the designated service channel (interface, module) of the "iBank" System by following the sequence of actions specified in the user manuals of the respective service channels (interfaces, modules): "Mobile Bank for Smartphones" and "Mobile Bank for Tablets", available on the Bank's website at [https://ibank.thbank.ru](https://ibank.thbank.ru/):
       1. Submit an application to the Bank to activate the service.
       2. If necessary, independently deactivate the service or change the following settings determining the service access parameters: Mobile Devices, telephone numbers for Mobile Devices, first names and positions of your employees.
    3. The Bank allows anonymous registration of the Client's Mobile Devices.
    4. The bank will fulfil the application for the service within no more than 2 (two) working days.
    5. To protect against unauthorised access to the Client's confidential information via the Mobile Device, the Client's Authorised Person may use the following means and methods to improve the security of the Mobile Device:
* set a password to unlock the Mobile Device;
* activate SIM card security with a PIN code;
* enable data encryption on the Mobile Device if this functionality is not activated on the device by default;
* if the device is equipped with a fingerprint sensor, use it to unlock the Mobile Device and authenticate in the Mobile App. The Mobile App supports Touch ID and Android Fingerprint Authentication technology;
* Install special (anti-virus) software on the Mobile Device and update it regularly to protect against the effects of MCs;
* avoid using wireless Internet access points when using the "iBank" System, the security of which is not known (e.g. wireless access points located in cafés, hotels and other public places).

# iBank for 1C Service.

**This service is chargeable and is provided only under the Client's application and the Client shall pay the Bank a commission for this service in accordance with the Bank's Tariffs.**

* + 1. When using the Service, the Client is given the opportunity to do the following:
* transmit the documents generated in its accounting system to the Bank;
* receive documents from the Bank within its accounting system.
  + 1. The Client's connection to the "**iBank for 1C**" service channel (interface, module) is performed by the Bank on the basis of a written **APPLICATION for Connection to the iBank for 1C Service** according to **Appendix 14** hereto within 2 working days from the date of receipt of the **APPLICATION** by the Bank.
    2. The specifics of using this interface are described in the User Guide

"Module "iBank for 1C:Enterprise" (Regular Application)" as well as in the User Guide

"Module "iBank for 1C:Enterprise" (Managed Application)", which are available on the Bank's website at [https://ibank.thbank.ru](https://ibank.thbank.ru/).

* 1. To resolve potential disputes, the Bank maintains control archives of digitally signed EDs, as well as archives of Public DS keys. The ED's control archives shall be kept for at least five (5) years from the date of the transaction.

# RIGHTS AND OBLIGATIONS OF THE PARTIES

* 1. **The Client shall:**
     1. Provide the Bank with documents confirming powers of the Client's Authorised Persons, including providing the Bank with documents confirming that the Client's Authorised Persons have the right of first and/or second signature (if any) on settlement documents in accordance with the applicable laws of the Russian Federation, banking regulations, the relevant agreement governing the relationship between the Parties for servicing the Client's Account and this Agreement.

In the event of changes in the composition of the Client's Authorised Persons and/or changes in the powers of the Client's Authorised Persons, immediately provide the Bank with information and documents about such changes.

# Use hardware and software complying with the REQUIREMENTS set out in the "Requirements" section of the full "Internet Bank for Corporate Clients" ("Internet Bank for Corporate Clients (Web Interface)") User Guide available on Bank's website at https://ibank.thbank.ru.

* + 1. To connect to the "iBank" System, generate DS (DS Key Pair) of the Client's Authorised Persons in the "iBank" System in accordance with **the Client's "iBank" System Connection REGULATION (Appendix No. 2 hereto)** by performing the list of actions specified **in the "Internet Bank for Corporate Clients" ("Internet Bank for Corporate Clients (Web Interface)") User Guide available on the Bank's Internet website at https://ibank.thbank.ru.**

Each Client's Authorised Person must generate his/her own DS (DS Key Pair).

When connecting new service channels (interfaces, modules) and (or) services of the iBank

System, independently configure his/her/its own AWS in accordance with the user manual on the use of the respective service channel (interface, module) of the "iBank" System, which is available on the Bank's website at https://ibank.thbank.ru.

* + 1. If the Bank provides the Client with a SDKH upon his/her/its request – to use the SDKH when working in the "iBank" System in accordance with the terms and conditions of this Agreement.
    2. To keep secret and not to disclose to third parties passwords for DS keys, Private (Secret) DS keys, DKH containing Private (Secret) DS keys, access code for authentication when providing Mobile Control service, to comply with the **REQUIREMENTS for Ensuring Information Security of "iBank" System (Appendix No. 4 hereto)**.
    3. Immediately submit to the Bank the **APPLICATION to Block/Unblock/**

**Terminate (Cancel) the DS** in the form of **Appendix No. 6 hereto** in order to block the compromised DS in accordance with the provisions of this Agreement, create a new Private (Secret) DS Key and its corresponding Public DS key, set a new password for the DS Key using the relevant capabilities of the "iBank" System

and apply to the Bank for activation of the Client's Public DS Key Certificate in the following cases:

* + - 1. In case of ES Comprometation, loss, compromise of DKH and/or Private DS (Secret) Key and/or the password to the Private DS (Secret) Key.
      2. Upon the dismissal of the Client's Authorised Person who had access to the Client's Private DS (Secret) Key and/or DS Key Password.
      3. If any MC is detected in the AWS.
      4. In case of unauthorised access to the "iBank" System or unauthorised debiting of funds from the Client's Account(s).
      5. In case of change of the Head(s), for whose DSs certification the DS Keys have been created and registered in the "iBank" System, and/or other persons in whose name the DS Keys have been created and registered in the "iBank" System.
      6. In case of transfer to another subdivision (to another position), exclusion from the functional duties of the Client's Authorised Person to perform work in the "iBank" System.
      7. When the data specified in the Public DS Key Certificate and allowing to identify the Client (Client's name, phone number, etc.) and the Certificate Holder (name, surname, position, passport data, signature group, etc.) are changed.
      8. In case of a change in the composition of the Client's Authorised Persons;
      9. At the Bank's request.
    1. Organise and carry out an internal investigation into the DS Comprometation, the results of which should be reflected in a Statement submitted to the Bank
    2. Regularly, but at least once every 5 (five) working days, log on to the iBank

System (establish a communication session with the Bank) to receive and view information messages, notifications and other information coming from the Bank.

* + 1. Read the information published by the Bank pursuant to Section 9 hereof at least once every five (5) working days.
    2. In case of disputes related to the use of the "iBank" System, provide, upon Bank's written request, the necessary documents and information related to the drawing up of the ED, the ED itself and other documents and information related to the disputed ED.
    3. Upon termination and/or expiry of this Agreement, termination of the use of the SDKH provided by the Bank:
* return the SDKH to the Bank under the **Equipment Acceptance Certificate** drawn up on paper in the **form of Appendix No. 12-B** hereto,

or

* provide a free-form statement explaining why they cannot be returned.
  + 1. Upon entering into this Agreement, notify the Bank by completing the relevant sections of **the APPLICATION for Accession to the Agreement of E-Banking Using "iBank" System (Appendix No. 1 hereto):**

1) the Client's federal Mobile phone number and e-mail address to which the following SMS messages or e-mail messages from the Bank will be received:

* on the transactions carried out under the ESD on the Account(s) (**SMS**, **e-mail notification**);
* on the confirmation of the transaction made on the Account(s) (**SMS confirmation**);
  + 1. If it is necessary to have an additional Client's Mobile phone number or e-mail address where SMS, e-mail messages from the Bank sent to notify or inform the Client will be received – submit to the Bank an **APPLICATION for Change**

# of Information for SMS Confirmation, SMS, E-mail Notification in the iBank

**System**, drawn up in the form of **Appendix No. 10** to this Agreement.

* + 1. If a Mobile phone number belonging to an individual is provided to receive SMS messages, obtain the individual's consent to share his/her Mobile phone number with the Bank and consent to use the Mobile phone number to receive SMS messages regarding transactions on the account(s) in accordance with Federal Law No. 152-FZ dated 27.07.2006 "On Personal Data", the Bank processes the specified Mobile phone number as depersonalized personal data.
    2. Be responsible for the completeness, accuracy and timeliness of the provision of information on the Mobile phone number in order to receive messages on the transactions carried out on the account(s).

If an incorrect Mobile phone number is provided to receive SMS messages – compensate the Bank for the payments made on the claim of the owner of the incorrectly provided Mobile phone number, if such payments have been made and confirmed by the Bank with documentary evidence.

* + 1. If the Mobile phone number specified for receiving SMS messages is changed or lost for any reason (change, theft, loss, etc.) – **immediately, during the day in which the phone number was changed or lost**, notify the Bank thereof by submitting to the Bank the **APPLICATION for Change of Information for SMS Confirmation, SMS, E-mail Notification in the "iBank" System**, drawn up in accordance with the form of **Appendix No. 10** hereto.
    2. In case of change of the e-mail address, loss or compromise of the username (login) and (or) password for access to the electronic mailbox, immediately, during the day in which the change, loss or compromise occurred, notify the Bank thereof by submitting to the Bank an **APPLICATION for Change of Information for SMS Confirmation, SMS, E-mail Notification in the "iBank" System**, drawn up in accordance with the form of **Appendix No. 10** hereto, and enter the changed e-mail address in the iBank

System settings using respective capabilities of the "iBank" System.

* + 1. Notify the Bank in writing of any changes to the Client's Authorised Persons and any changes to the personal details of the Client's Authorised Persons that may affect the fulfilment of the Bank's obligations, including telephone and fax numbers, etc., no later than the day following the day of such changes.
    2. Notify the Bank in writing of any other changes to the information not specified in clauses 5.1.16 - 5.1.18 of the Agreement contained in **the APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System (Appendix No. 1 hereto):**
    3. Avoid breaching the terms and conditions of the service provider's tariff plan which results in the blocking of reception of incoming SMS messages to the Mobile phone specified for receiving SMS messages.
    4. In order to avoid risks associated with unauthorised e-banking transactions via the "iBank" System and to ensure safe use of the "iBank" System – **to comply with the Requirements for Ensuring Information Security of "iBank" System (Appendix No. 4 hereto).**

The Client's failure to comply with the **Requirements for Ensuring Information Security of "iBank" System (Appendix No. 4 hereto)** shall be grounds for refusing to refund to Client the amount of the transaction performed without Client's consent in accordance with Part 12 of Article 9 of Federal Law No. 161-FZ dated 27.06.2011 "On National Payment System".

* + 1. Pay the Bank's commission fee for the provision of services under this Agreement in accordance with the terms and conditions of this Agreement.
    2. Ensure that there are sufficient funds in the Client's Account to pay the Bank's fees in accordance with the terms and conditions of this Agreement.
    3. Use SMS confirmation or Other Confirmation when using the "iBank" System.
    4. Compile EDs using document templates (forms) available in the "iBank" System, taking into account the requirements of regulatory acts of the Bank of Russia and applicable laws of the Russian Federation, and in the absence of such templates – in accordance with the requirements of regulatory acts of the Bank of Russia and applicable laws of the Russian Federation.
    5. Verify the timeliness and correctness of the Bank's execution of the ESD on the basis of statements signed by the Bank's Authorised Person's DS.
    6. Receive the Client's Account statements and notify Bank in writing of identified discrepancies (non-recognition (non-confirmation) of the balance) as well as funds credited to the Client's Account by mistake and return the said funds to Bank within 10 (ten) calendar days from the date of the Client's Account transaction using the "iBank" System. If there are no claims from the Client, the balances and transactions in the Client's Account shall be deemed confirmed.
    7. Provide a settlement document drawn up on paper in compliance with the requirements of the regulations of the Bank of Russia and the current laws of the Russian Federation at the Bank's request.
    8. If requested by the Bank by e-mail or through the iBank interface, confirm the fulfilment

of the requirements for protection the APM against MC of in the manner specified in the request.

* + 1. In case of AWS failure or incorrect operation of the "iBank" System or signs of MC, signs of unauthorised access to the AWS, as well as non-standard behaviour of the AWS, immediately perform the requirements of Sub-clauses 9.1.1 – 9.1.3 of Appendix No. 4 **"Requirements for Ensuring Information Security of "iBank" System" to this Agreement**.
    2. Keep the confidentiality of the Private (Secret) DS Keys and the passwords to the DS keys used in the "iBank" System.
    3. Immediately, but no later than on the business day following the detection of unauthorised access or attempted unauthorised access to the "iBank" System, notify the Bank thereof in writing or by sending an ED signed by the DS of the Client's Authorised Person via the "iBank" System.
    4. **If the Client detects an unauthorised write-off of funds from the account(s), the Client shall act in accordance with the "Action Plan for Detecting an Unauthorised Write-off of Funds from the Account(s) by the Client" set forth in Clause 9 of Appendix No. 4 "Requirements for Ensuring Information Security of "iBank" System" hereto.**
    5. Exercise regular control (at least monthly) over the fulfilment of organisational and technical requirements for ensuring information security when using the "iBank" System as specified in **Appendix No. 4 "Requirements for Ensuring Information Security of "iBank" System"** hereto.
    6. Ensure that there is no MC on the AWS and that the safety and integrity of the AWS runtime environment is maintained.
    7. Take full responsibility for and independently ensure the security, non-disclosure and non-distribution of its Private (Secret) DS Keys. In the event of loss, theft, unauthorised copying or compromise of the DKH containing the Private (Secret) DS Keys, the Client shall immediately notify the Bank thereof.
    8. Provide the Bank with correct e-mail address.
    9. If the Bank blocks the Client's Authorised Persons' DS for reasons specified in clause 4.2.6 of the Agreement – to submit to the Bank the documents and information requested by the Bank and necessary for making a decision on unblocking the Client's Authorised Persons' DS within the term specified by the Bank.
    10. Perform other obligations stipulated by the current laws of the Russian Federation, documents (including methodological recommendations) of the Bank of Russia and this Agreement.
    11. Inform the Client's Authorised Persons to avoid situations where the memory of the Mobile Phones for receiving and storing SMS messages overflows, which may be an obstacle for receiving SMS confirmations and SMS, e-mail notifications.
    12. Ensure that the Client's Authorised Persons use their personal Mobile Phones to receive SMS confirmations and SMS, e-mail notifications.
    13. Ensure that Mobile Devices with the Mobile App installed are kept safe.
    14. In case of compromise, immediately replace the Access Code used by the Client's Authorised Person for authentication when logging into the "iBank" System through the "Mobile Bank for Smartphones" and

"Mobile Bank for Tablets" service channels (interfaces, modules) independently.

* + 1. Immediately and independently remove the lost Mobile Device from the Mobile Devices through which access to the "Mobile

Bank for Smartphones" and "Mobile Bank for Tablets" service channels (interfaces, modules) is authorised using the designated service channel (interface, module) of the "iBank" System by following the sequence of actions specified in the user manuals of the respective service channels (interfaces, modules): "Mobile Bank for Smartphones" and "Mobile Bank for Tablets", available on the Bank's website at https://ibank.thbank.ru:

# The Client shall be entitled to:

* + 1. Determine the composition of the Client's Authorised Persons allowed to work in the "iBank" System and define their powers in accordance with the requirements of the regulations of the Bank of Russia, the applicable laws of the Russian Federation and this Agreement (including the **Client's "iBank" System Connection REGULATION (Appendix No. 2 hereto**).
    2. At his/her/its own discretion, generate (form new) Client's Authorised Persons' DSs and register (activate an DS) at the Bank new Client's Authorised Persons' Public DS Keys an unlimited number of times, with the validity of the Client's Authorised Persons' DSs previously registered with the Bank being terminated (cancelled) by the Bank without the Client's further applications.
    3. Block the Client's Authorised Person's DS in accordance with the terms and conditions of this Agreement.
    4. Prematurely terminate (cancel) the Client's Authorised Person's DS in accordance with the terms and conditions of this Agreement.
    5. Connect/disconnect the IP-Filtering mode, change the IP-address, in accordance with the terms and conditions of this Agreement.
    6. If necessary, submit to the Bank a written request for a paper copy of Client's Account Statements and ESDs submitted to the Bank using the "iBank" System, certified in accordance with the procedure prescribed by the regulations of the Bank of Russia and the applicable laws of the Russian Federation.
    7. Revoke the EDs submitted to the Bank via the "iBank" System. The revocation of an ED shall be made by sending a relevant message via the "iBank" System, containing the details of the ED to be revoked and the reasons for the revocation, signed by the Client's Authorised Person's DS.

The ESD can only be revoked:

* until the funds have been credited to the beneficiary's account, if the beneficiary's account has been opened with the Bank;
* until the funds have been debited from the Bank's correspondent account, if the recipient of the funds is served by another credit institution;
* in cases provided for in other agreements concluded between the Bank and the Client.
  + 1. Activate / deactivate / modify the SMS and e-mail notification settings in accordance with the terms and conditions of this Agreement.
    2. Change the Mobile phone number (e-mail address) for SMS, e-mail notification, SMS confirmation in accordance with the terms and conditions of this Agreement.

# The Bank shall:

* + 1. Perform registration (DS activation) of the Client's Authorised Person's Public DS Key in the "iBank" System after the Client performs all necessary actions in accordance with the **Client's "iBank" System Connection REGULATION (Appendix No. 2 hereto)**, as well as the Client pays the Bank's commission fee in accordance with the provisions of this Agreement.

Registration (DS activation) with the Bank of the Client's Authorised persons' Public ES keys together with the **Client's Authorised persons' Public ES key Certificates** shall be formalised by the Client's "iBank" System Connection Certificate drawn up on paper in the form of **Appendix No. 7** hereto and signed by the authorised representatives of the Bank and the Client.

.3.2. Provide services to the Client using the "iBank" System in accordance with the terms and conditions of this Agreement, the requirements of the regulations of the Bank of Russia and the applicable laws of the Russian Federation.

* + 1. Provide the Client with the possibility to receive statements of the Client's

Accounts in the form of EDs, including executed ESDs via the "iBank" System.

* + 1. Transmit to the Client account statements in the form of EDs and reference information to the Client. Upon the Client's written request, provide the Client with paper statements

of the Client's Account and executed ESDs submitted to the Bank using the "iBank" System, certified in accordance with the procedure prescribed by the regulations of the Bank of Russia and the applicable laws of the Russian Federation.

* + 1. Ensure 24-hour reception of EDs from the Client via the "iBank" System, except for the time of routine maintenance work in the "iBank" System.
    2. Notify the Client in advance about maintenance work in the "iBank" System in accordance with the terms and conditions of this Agreement.
    3. Block/unblock/terminate (revoke) the Client's Authorised Person's DS in accordance with the terms and conditions of this Agreement.
    4. Activate/deactivate IP-Filtering, SMS, e-mail informing, change the Client's IP-address, activate/deactivate other services in accordance with the terms and conditions of this Agreement.
    5. Provide the Client, upon his/her/its **APPLICATION for the "iBank" System Equipment** drawn up according to the form of **Appendix No. 11**, with SDKH, Other Equipment in accordance with the terms and conditions of this Agreement.

The transfer of the SDKH or Other Equipment shall be documented by the **Equipment Acceptance Certificate** in hard copy in the form of **Appendix No. 12-A** hereto.

* + 1. Advise the Client's Authorised Persons on the operation of the "iBank" System.
    2. Accept for execution the ESDs received from the Client via the "iBank" System, executed and certified in accordance with the terms and conditions of this Agreement.
    3. Provide the Client with a possibility to send a notification about the loss or compromise of the Private DS Key and DS password used in the "iBank" System and (or) their use without the Client's consent by organising the acceptance of the Client's written requests during the Bank's working hours at the Bank's offices and by organising the acceptance of the Authorised Person's ED signed by the Client and containing the above mentioned information through the "iBank" System during the Bank's working hours.
    4. Notify the Client of each transaction on the Client's Account(s) by sending an SMS (e-mail message) to the Mobile phone number (e-mail address) specified by the Client in the Application for Accession to the Agreement during the day of the transaction on the Client's Account(s).
    5. Perform other duties stipulated by this Agreement, regulations of the Bank of Russia and applicable laws of the Russian Federation.
    6. Set the parameters for the Client's Account transactions carried out via the "iBank" System under the respective Client's application on paper or in the form of an ED transmitted via the "iBank" System.

# The Bank shall be entitled to:

* + 1. Unilaterally amend and supplement this Agreement (including all appendices hereto) and/or the Bank's Tariffs in accordance with the terms and conditions of this Agreement with at least 10 working days prior notice to the Client about the amendments and supplements by posting the new Agreement on the Bank's official website [www.thbank.ru](http://www.thbank.ru/), as well as by sending a notice about the Agreement amendments via

the "iBank" System.

* + 1. Debit the Bank's commission amounts from the Client's Account in accordance with the terms and conditions of this Agreement without any additional instruction from the Client.
    2. Request from the Client documents and information that are the basis for transactions on the Client's Account and confirm their compliance with the regulations of the Bank of Russia and applicable laws of the Russian Federation (including currency laws of the Russian Federation and anti-money laundering legislation).
    3. Suspend the execution of the ESD and request from the Client documents and information that are the basis for transactions on the Client's Account and confirm their compliance with the regulations of the Bank of Russia and applicable laws of the Russian Federation (including currency laws of the Russian Federation and anti-money laundering legislation).
    4. Refuse to accept and/or execute the ED received by the Bank via the "iBank" System in the following cases:
* compromise of the Client's Authorised Person's DS;
* EDs do not comply with the requirements for EDs in accordance with this Agreement, regulations of the Bank of Russia and applicable laws of the Russian Federation;
* the ESDs do not comply with the requirements for settlement documents set out in the regulations of the Bank of Russia and the applicable laws of the Russian Federation;
* non-compliance of the transaction conducted on the Client's Account with the applicable laws of the Russian Federation (including currency laws of the Russian Federation and anti-money laundering legislation);
* if the Client fails to provide the documents and information requested by the Bank in accordance with the terms and conditions of this Agreement;
* in other cases stipulated by the current laws of the Russian Federation, documents of the Bank of Russia (including methodological recommendations), this Agreement and the Bank Account Agreement concluded between the Client and the Bank.
  + 1. Request the submission of a document drawn up in paper form and complying with the requirements

of the regulations of the Bank of Russia and the current laws of the Russian Federation if the Client refuses to accept and/or execute the ED received by the Bank via the "iBank" System.

* + 1. Upon prior notification, refuse to accept and execute any EDs submitted to Bank via the "iBank" System and signed by the Client's Authorised Person's DS, if the Client's transactions are found to be suspicious. The Client may, however, submit settlement documents to the Bank on paper.
    2. Block/unblock/terminate (revoke) the Client's Authorised Person's DS in accordance with the terms and conditions of this Agreement.
    3. Demand that Client terminates (cancels) and/or replaces the Client's Authorised Person's DS in accordance with the terms and conditions of this Agreement.
    4. Suspend the provision of services under this Agreement and block the Client's access to the "iBank" System in accordance with the terms and conditions of this Agreement.
    5. Refuse to accept and register (activate the DS) the Public DS Key Certificate:
* issued to a person not authorised by the Client (an individual who is not the Client's employee and is not named on the Card, unless the access level is "without signatory rights");
* failure to submit documents confirming that the Client's Authorised Person has the right of first and/or second signature on settlement documents in accordance with the applicable laws of the Russian Federation, as well as the existence of such documents with expired validity;
* failure to pay the Bank's fees in accordance with the terms and conditions of this Agreement;
* the information in the Public DS Key Certificate does not match the Client's documents submitted to the Bank;
* incorrect/incorrect completion of the Public DS Key Certificate;
* in other cases provided for in this Agreement.
  + 1. Independently and subject to the requirements hereof, establish the procedure for appointment and access of the Bank's Authorised Persons to the "iBank" System, the procedure for creation, registration and application of the Bank's Authorised Persons' DS, including the relevant procedures for registration of Public DS Key Certificates, for the exchange of DS in the "iBank" System;
    2. Suspend the exchange of ESDs, EDs with the Client in the event of technical failures or other circumstances, including changes in Russian laws, which make it impossible or undesirable to exchange ESDs, EDs from the security point of view.
    3. Suspend the provision of the Client's Account(s) service using the "iBank"

System if there is no alternative Mobile phone number to inform about the operations performed on the Client's account(s) in case the Client provides false information about the Mobile phone number, confirmed by the request of a government agency or

an individual or legal entity – the owner of the phone number specified by the Client as the phone number for receiving SMS messages about transactions on the account(-s) with a complaint about receiving SMS messages from the Bank containing information about transactions on the Client's account(-s) without the consent of the owner of the phone number, and providing the Bank with confirmation of information about the true owner of the Mobile phone number.

* + 1. Inform the Client in a manner determined by the Bank of new types of MC that threaten the security of the AWS, methods to protect against its effects and to eliminate the consequences of such effects.
    2. If any facts or indications of a security breach of the "iBank" System are identified, immediately suspend the use of the "iBank" System and notify the Client thereof by any available means.
    3. Delete requests for production of the Public ES Key Certificate if the Client's Authorised Representative fails to appear after generation (formation) of the DS (DS Key Pair) to the Bank for identification and personal certification of the information contained in the Public DS Key Certificate within 30 (thirty) calendar days.
    4. Block the use of the DS Key Pair and its corresponding Public DS Key Certificate of the Client in case of loss/damage/suspicion of compromise, as well as after the expiry of the Public DS Key Certificate, upon expiry of the Certificate Holder's authority or in case the Bank receives information about the death of the Certificate Holder.
    5. Restrict or completely terminate the provision of services to the Client under the Agreement in the event of any attempts to scan or attack the Bank's information resources, or any other indications of a security breach using the Client's AWS, Mobile Device or other software or hardware.
    6. The Bank shall have the right to request from the Client any documents and information necessary to verify the compliance of the Client's Account(s) with the applicable laws of the Russian Federation, as well as to ensure compliance with the applicable laws of the Russian Federation by the Bank itself.
    7. Exercise other rights stipulated by the current laws of the Russian Federation, documents (including methodological recommendations) of the Bank of Russia and this Agreement.

# COST OF SERVICES AND SETTLEMENT PROCEDURE

* 1. The Client shall pay the Bank a commission fee for the services provided by the Bank under this Agreement in accordance with the terms and conditions of this Agreement and the Bank's Tariffs in force at the Bank at the date of the service provision.
  2. the Client shall pay the Bank's Fee for entering into this Agreement prior to the Client's connection to the "iBank" System (registration (DS activation) by the Bank of the Client's Authorised Person's Public DS Key).

The Client shall be pay the Bank's fee for providing DKH to the Client prior to the actual provision of NEC and the signing of the **Equipment Acceptance Certificate** drawn up on paper in the form of **Appendix No. 12-A** hereto.

* 1. The Client authorises the Bank to debit the Client's Account without the Client's further order (advance acceptance) for the Bank's fees for the provision of services under this Agreement in accordance with the Bank's Tariffs.
  2. The Bank's fees for the provision of services under this Agreement to the Client shall be paid by debiting by the Bank, without the Client's further order, from any the Client's account opened with the Bank in Roubles, at the time specified in the current Bank's Tariffs, unless otherwise specified in this Agreement.

If the rouble account regime prohibits the debiting of fees from this account or if there are insufficient funds in the rouble account to pay fees to Bank, the Client shall authorise the Bank to debit any other account of the Client opened with Bank as payment for the Bank services under this Agreement without further instruction from the Client. In the case of debits in payment for the Bank's services from the Client's accounts in foreign currencies, the debit shall be made at the exchange rate of the Central Bank of the Russian Federation on the date of the debit.

* 1. The Bank's monthly fees for the provision of services under this Agreement to the Client

shall be charged by the Bank on a monthly basis on the first calendar day of the month of provision of services under this Agreement (advance payment). The Bank's monthly fees for the provision of services to the Client under this Agreement shall be paid by debiting the Bank's fee amount from the Client's Account without any further instruction from the Client.

The Bank's monthly fees for the provision of services under this Agreement to the Client shall be charged by the Bank for a full calendar month regardless of the actual number of calendar days (actual time) of using the service in accordance with this Agreement.

* 1. Upon termination and/or expiration of this Agreement and the Client's disconnection from the "iBank" System, the Bank shall not recalculate the Bank's fees the provision of services under this Agreement to the Client depending on the actual number of calendar days (actual time) of using the service in accordance with this Agreement.
  2. In addition to payment for the Bank's services under this Agreement, the Client shall reimburse the Bank for its expenses related to the provision of such services, such as postage, telegraph, telecommunication expenses, correspondent bank fees, etc. The said expenses shall be debited by the Bank from the Client's account without the Client's further order in accordance with the procedure specified in clause 6.4 hereof. The amount and terms of the costs to be borne by the Client shall be determined by the Bank's Tariffs.
  3. In the event of a change in the service provision procedure under this Agreement, the Client shall not pay a repeated fee for connecting to the "iBank" System.

# RESPONSIBILITY OF THE PARTIES

* 1. In case of failure to fulfill or improper fulfillment by the Parties of their obligations hereunder, the Parties will be liable in accordance with the current legislation of the Russian Federation.
  2. The Bank shall not be liable for non-execution or improper execution of the Client's EDs, including the Client's ESDs, due to the Client's breach of this Agreement and the provisions of other agreements entered into between the Client and the Bank regulating the legal relations concerning the procedure for the execution of the Client's EDs by the Bank.
  3. The Parties shall be liable for the accuracy of the information provided to each other, including via the "iBank" System.
  4. The Bank shall not be liable, including in the form of compensation for the Client's damages, in the event of inability to exchange EDs with the Client if it is caused by improper functioning of technical and software tools, Communication Channels owned by the Client or third parties and used in operation of (with) the "iBank" System.
  5. The Bank shall not be liable for any damage caused to the Client due to unauthorised access to the "iBank" System as a result of the use by third parties of the Private (Secret) DS Key and/or violation by the Client of the **Requirements for Ensuring Information Security of "iBank" System set forth in Appendix No. 4 hereto**.
  6. The Bank shall not be liable for any damage caused to the Client as a result of

the MC effect.

* 1. Upon termination of this Agreement, the Parties shall be liable for all EDs signed

with DSs of the Client's Authorised Persons generated in the "iBank" System in accordance with the applicable laws of the Russian Federation.

* 1. The Bank shall not be liable for possible misrepresentations, errors and misprints in the EDs sent by the Client via the "iBank" System and signed with the Correct DS of the Client's Authorised Persons.
  2. In case of conflicts between the Client and the Bank when using the "iBank" System, the Parties shall participate in the resolution of conflicts in accordance with the **PROCEDURE for Dispute Resolution due to the use of EDs (Appendix No. 5 hereto)**, comply with the requirements contained in the said procedure, implement decisions of the resolution committee and bear responsibility according to the findings on resolution of the conflict situation.
  3. If the Client fails to comply with the notification deadline set out in clause 5.3.7 hereof, and if the Client fails to return the amounts credited to the Client's Account by mistake within the term

specified in clause 5.3.7 hereof, and if Bank is unable to recover these amounts without the Client's further order, the Client shall pay Bank a penalty of 0.3 (zero point three) per cent of the erroneously credited amount in roubles or 0.15 (zero point fifteen hundredths) per cent of the amount in foreign currency for each day of violation of the notice period and/or delay in returning the amounts.

* 1. The Bank shall not be liable for delays in settlements resulting from the actions of other credit institutions, settlement centres and other entities involved in settlements.
  2. The Bank shall not be liable for non-performance or delayed performance of the Client's EDs if such has occurred due to the Client's failure to perform its obligations under this Agreement, including the obligation to establish a communication session with the Bank.
  3. The Bank shall not be liable for re-execution of the Client's ESD sent to the Bank repeatedly/ erroneously.
  4. The Bank shall not be liable if the information about amendments and/or additions to this Agreement and/or the Bank's Tariffs, published in the manner and within the terms set out in this Agreement, has not been received and/or reviewed and/or correctly interpreted by the Client.
  5. The Bank shall be liable for late notification (notification) of the Client about the Client's Account transactions in the amount of the Client's actual damage caused by such late notification, but not more than 1,000 (one thousand) rubles.
  6. When resolving economic and other disputes that may arise in connection with the use of the "iBank" System, the Parties shall submit their assessments, evidence and conclusions in writing at the request of the interested Party.
  7. Compensation by the Bank of losses incurred by the Client as a result of unreasonable non-execution or improper execution of the Client's ESDs, including untimely transfer of funds, shall be limited to payment by the Bank of an amount equal to 0.3 (zero point three) percent per annum when carrying out transactions in the currency of the Russian Federation and 0, 15 (zero point fifteen hundredths) percent per annum for transactions in foreign currency of the amount specified in the unexecuted or improperly executed Client's ESD, but not more than for 30 (thirty) calendar days of the unexecuted or improperly executed Client's ESD.
  8. If it is impossible to fulfill the terms of this Agreement due to force majeure circumstances, i.e. extraordinary and unavoidable circumstances, under specific conditions, of a particular period of time, which the Parties could neither foresee nor prevent by reasonable measures, the Parties shall be released from liability under this Agreement. Force majeure includes natural disasters, accidents, fires, floods, earthquakes, military actions, mass riots, mass diseases (epidemics), military coups, terrorist acts, national strikes, illegal actions of third parties, actions or decisions of public authorities and law enforcement agencies, as well as the adoption (publication) of regulations directly or indirectly prohibiting or preventing the full or partial performance of the Parties of their functions and other obligations under this Agreement. The fact of occurrence of force majeure circumstances shall be confirmed by the Parties by providing the relevant documents.
  9. The Client shall be fully liable for the actions of persons who on any grounds (including unlawful) gain access to the "iBank" System, Private DS Keys of the Client's Authorized Persons and other technical and information means provided by the Bank to the Client and ensuring the possibility to generate and send EDs to the Bank.
  10. The Client shall be liable for the content of any ED signed by the Client's Authorized Persons.
  11. The Client shall be liable for the accuracy and relevance of all documents (other information) submitted by him/her/it to the Bank at the conclusion and execution of this Agreement.
  12. The Bank shall be liable for ensuring the confidentiality of information containing personal data of employees of the Client and the information that is a bank secret, when they are transmitted via telecommunications networks and communication channels outside the Bank in the form of SMS-messages and letters sent by e-mail.
  13. The Bank shall not be liable for losses, expenses, as well as other negative consequences that may arise if the information transmitted during the transmission of SMS messages becomes known to third parties, including the consequences of the transfer by the mobile network operator of the Client's Mobile phone number, provided to the Bank for sending SMS messages, to another subscriber.
  14. As the Client independently chooses the e-mail service provider to communicate his/her/its e-mail address to the Bank, the Client shall be liable for ensuring the confidentiality of the data as a result of this choice.
  15. The Parties shall not be liable for the correctness of the other Party's ED.
  16. The Bank shall not be liable for consequences of compromise of the Client's Private (Secret) DS Key, permanent and one-time passwords of the Client's Authorized Persons, as well as for losses incurred by the Client in connection with unlawful actions of third parties.
  17. The Bank shall not be liable for consequences of execution of the ED, protected by the Client's correct DS, including in case of use of Mobile Phones, DKH, SDKH, software and hardware of the client part of the "iBank" System by an unauthorized person.
  18. The Bank shall not be liable for damages, regardless of the reasons, arising from the disclosure by unauthorized persons of the Client's Authorized Persons of their own Private (Secret) DS Keys, their loss or transfer.
  19. The Bank shall not be liable in case of threats of unauthorized access of unauthorized persons to the AWS, Mobile Devices (including remote network access) and the Client's Private (Secret) DS Keys, including threats from internal (local) and external (global) communication networks.
  20. The Bank shall not be liable for the inoperability of equipment and software of the Client and third parties, resulting in the inability of the Client to access the banking part of the System, and the resulting delays in the implementation of the Client's transactions, as well as for the possible destruction (in whole or in part) of information contained in the Client's AWS and (or) Mobile Devices connected to the Internet to ensure the provision of services under this Agreement.
  21. The Bank shall not be liable if the Client's Mobile Device is lost.
  22. The Bank shall not be liable for the accuracy of the information displayed in the "Indicator" Service, as the information displayed to the Clients in the "Indicator" Service is collected from public sources and provided to the Bank by BIFIT Analytics LLC. The Bank displays information received from BIFIT Analytics LLC to the Clients on an "as is" basis.

# PROCEDURE FOR AMENDING AND/OR SUPPLEMENTING THE AGREEMENT AND/OR THE BANK'S FEES

* 1. Amendments and/or additions to this Agreement (including appendices hereto) and/or the Bank's Tariffs, including approval by the Bank of a new version of this Agreement, shall be made on the initiative of the Bank in the manner prescribed by this Section.
  2. The Bank shall inform the Client about amendments and/or additions to this Agreement and/or the Bank's Tariffs, including the Bank's approval of a new version of this Agreement, not later than 10 (ten) calendar days prior to their entry into force by one of the ways specified in clause 9.1 of this Agreement.
  3. All amendments and/or additions made by the Bank to this Agreement and/or the Bank's Tariffs, including the new version of this Agreement approved by the Bank, shall take effect from the day following the date of expiry of the period specified in clause 8.2 of this Agreement.
  4. Any amendments and/or additions to this Agreement and/or the Bank's Tariffs, including the new version of this Agreement approved by the Bank, from the date of their entry into force shall equally apply to all persons who have acceded to this Agreement, including those who acceded to this Agreement before the date of entry into force of the amendments and/or additions. If the Client does not agree with the changes and/or amendments made by the Bank to this Agreement and/or the Bank's Tariffs, the Client shall be entitled to terminate this Agreement in the manner prescribed by Section 10 of this Agreement.

# PUBLICATION OF INFORMATION

* 1. Publication of information in this Agreement means the placement by the Bank of information stipulated by this Agreement in one of the following ways to ensure the possibility of familiarization with this information of the Clients, including:
* posting information on the Bank's website (http://www.thbank.ru);
* placement of information in the Bank's operating rooms (additional offices and other structural units of the Bank providing services to the Clients);
* sending informational messages through the "iBank" System;
* other ways that allow the Client to obtain information and establish that it comes from the Bank.

The publication of information does not mean that it must be disseminated through the media.

* 1. The moment of publication of this Agreement, as well as the moment of the Client's familiarization with the published Agreement shall be the moment of their first posting on the Bank's website (http://www.thbank.ru).

The moment of publication of the Bank's Tariffs and other information, as well as the moment of the Client's familiarization with the published Bank's Tariffs and information shall be the moment of their first posting in accordance with clause 9.1 of this Agreement.

* 1. Notification of an unlimited number of Clients on issues related to the execution of this Agreement shall be made by the Bank by publishing information in one or more of the ways listed in clause 9.1 of this Agreement, as well as by providing information when the Client personally visits the Bank offices and/or when the Client applies to the Bank using the "iBank" System, and notifications related to the issues of servicing the Client only – by sending a relevant notice to the Client using the "iBank" System and/or by postal communication means – by registered mail with return receipt requested at the location address specified by the Client in the **APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System (Appendix No. 1 hereto)**, or at another address provided by the Client to the Bank.

# TERM AND TERMINATION

* 1. This Agreement shall enter into force from the date of registration by the Bank of the Client's **APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System**, drawn up on paper in the form of **Appendix No. 1 to this Agreement**, in the registration program of contracts concluded by the Bank, and is concluded for an indefinite period until one of the events specified in Clause 10.4 herein occurs.
  2. This Agreement shall be suspended (the Bank's provision of services under this Agreement shall be suspended and the Client's access to

the "iBank" System shall be blocked) on the day when one of the following events occurs:

* the Client's failure to pay the Bank's fees (including the absence / insufficiency of funds on the Client's Account sufficient to pay the Bank's fees, the existence of restrictions on the disposal of funds on the Client's Account, making it impossible to pay the Bank's fees) in accordance with the terms and conditions of this Agreement;
* other cases provided for by this Agreement and the applicable laws of the Russian Federation.
  1. This Agreement shall be resumed (the Bank's provision of services under this Agreement shall be resumed and the Client's access to the "iBank" System shall be unblocked)

by the Bank no later than the business day following the day when the circumstances that served as the basis for the Bank's suspension of the Client's services under this Agreement and blocking the Client's access to the "iBank" System are eliminated.

* 1. This Agreement shall terminate on the date

of the occurrence of any of the following events:

* upon expiry of 6 (six) months from the expiration date of the last DS of the Client's Authorized Person or termination/blocking of the last DS of the Client's Authorized person.
* the Client closes the last Client's Account connected to the "iBank" System;
* after 3 consecutive months of absence of transactions on the account via **"iBank" System**/ non-receipt by the Bank of ESD from the Client during 3 consecutive months.
* other grounds provided for by this Agreement and the applicable laws of the Russian Federation.
  1. This Agreement may be unilaterally terminated on the initiative of either Party as follows:
     1. In the event of termination of this Agreement on the initiative of the Bank, the Bank shall notify the Client in writing. This Agreement shall be deemed terminated and the Parties' obligations to accept and execute EDs using the "iBank" System shall be deemed terminated as of the date and time specified in the notice. If such time is not specified, this Agreement shall be deemed terminated and the Parties' obligations to accept and execute EDs using the "iBank" System shall be deemed terminated from the day following the day of sending such notice;
     2. In case of termination of this Agreement on the Client's initiative, the Client shall notify the Bank and the other Party thereof by sending the **NOTICE of Termination of the Agreement of E-Banking Using "iBank" System**, prepared on paper in the form of **Appendix No. 13** hereto.

This Agreement shall be deemed terminated and the Parties' obligations to accept and execute EDs using the "iBank" System shall be deemed terminated as of the date and time specified in the notice. At the same time, the date of termination of this Agreement specified in such notice may not be earlier than the date of submission of the said notice to the Bank. If the date of termination of this Agreement specified in the notice is earlier than the day of submission of such notice to the Bank, this Agreement shall be deemed terminated from the date of receipt by the Bank of such notice.

# FINAL PROVISIONS

* 1. Disputes related to the use of EDs shall be resolved in accordance with the **PROCEDURE for Dispute Resolution due to the use of EDs (Appendix No. 5 hereto)**. If one of the Parties does not agree with the committee's decision, avoids forming an expert committee or participating in its work, or prevents one of the Parties from participating in the work of the expert committee, the other Party shall be entitled to refer the dispute to the Arbitration Court of the Samara Region under the Russian Federation laws.
  2. In all other matters not regulated by this Agreement, the Parties shall be governed by the provisions of the relevant agreement governing the relationship between the Parties with respect to servicing the Client's Account, or the relationship with respect to cash services to the Client.
  3. In the event of changes in the applicable laws of the Russian Federation, this Agreement shall apply to the extent not inconsistent with the requirements of the Russian Federation laws, until this Agreement is brought into compliance with the requirements of the applicable laws of the Russian Federation.
  4. The following appendices, which form an integral part of this Agreement, are attached hereto:

Appendix No. 1 APPLICATION for Accession to the AGREEMENT of E-Banking Using "iBank" System

Appendix No. 2 Client's "iBank" System Connection REGULATION.

Appendix No. 3 APPLICATION for Connection/Disconnection of the Client's Account to the "iBank" System. Appendix No. 4 Requirements for Ensuring Information Security of

the "iBank" System.

Appendix No. 5 PROCEDURE for Dispute Resolution due to the use of EDs

Appendix No. 6 APPLICATION to Block/Unblock/Terminate (Cancel) the DS.

Appendix No. 7 Client's "iBank" System Connection Certificate. Appendix No. 8 APPLICATION for Activation/Deactivation of IP-Filtering Mode/Change of

IP Address in the "iBank" System.

Appendix No. 9 APPLICATION for Enabling/Disabling SMS, E-mail Notification. Appendix No. 10 APPLICATION for Change of Information for SMS Confirmation,

SMS, E-mail Notification in the "iBank" System.

Appendix No. 11 APPLICATION for the "iBank" System Equipment. Appendix No. 12-А. Equipment Acceptance Certificate.

Appendix No. 12-B. Equipment Acceptance Certificate.

Appendix No. 13 NOTICE of Termination of the Agreement of E-Banking Using "iBank" System

Appendix No. 14 APPLICATION for Connecting the "iBank for 1C" Service