

**PUBLIC OFFER -
INTERNET BANKING iDBA REMOTE BANKING SERVICING AGREEMENT
FOR LEGAL ENTITIES AND INDIVIDUAL ENTREPRENEURS**

(Version of the Public Offer as amended and supplemented as of 25.08.2025
(Management Board Protocol #IMG/LGD/HO/25/91 dated 07.08.2025))

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, the first paragraph of the preamble is amended and supplemented (the amendment shall come into force from 01.06.2022).

This document, published by KDB Bank Uzbekistan JSC (hereinafter – **the Bank**) in the Internet at the official website www.kdb.uz is a public offer, i.e. an offer addressed to legal entities, including financial institutions and individual entrepreneurs (hereinafter – **the Client**) to conclude "Internet Banking iDBA" remote banking servicing agreement in accordance with Articles 364 and 367 of the Civil Code of the Republic of Uzbekistan.

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, the second paragraph of the preamble is supplemented (the amendment shall come into force from 01.06.2022).

In accordance with paragraph 2 of Article 369 of the Civil Code of the Republic of Uzbekistan, the Public Offer - "Internet Banking iDBA" remote banking servicing agreement for legal entities, including financial institutions and individual entrepreneurs (hereinafter - the **Agreement**) between the Bank and the Client shall be considered concluded upon acceptance by the Client of the terms and conditions of this Public Offer, and the Bank and the Client together shall be considered as the Parties to the Agreement.

The acceptance of this Public Offer, i.e. the consent of the Client to conclude this Agreement is the fact of submission by the Client of duly completed and signed Application for user registration in the "Internet Banking iDBA" remote banking system (hereinafter - **Application**) in the form established by the Bank.

Submission by the Client of the Application also means the Client has read and unconditionally agrees with the terms of the Agreement, Appendices to this Agreement and Bank Tariffs.

The terms of the Agreement are regulated and drafted in compliance with the current legislation of the Republic of Uzbekistan, including laws, by-laws, regulatory acts of the Central Bank of the Republic of Uzbekistan and other state bodies (hereinafter - the **Legislation**) and in accordance with the business practices of the Bank.

Certain banking services along with the present Agreement shall be governed by separate agreements, under separate terms prevailing in the event of a dispute.

1. DEFINITIONS

Bank – the Head Office and branches of KDB Bank Uzbekistan JSC.

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, Chapter 1 of the Public Offer is supplemented by the following definition (the amendment shall come into force from 01.06.2022).

“Internet Banking iDBA” remote banking servicing agreement (**Agreement**) – an agreement between the Bank and the Client concluded upon acceptance by the Client of the terms and conditions of this Public Offer.

Bank Account Agreement - the agreement governing the relationship between the Bank and the Client when the Client performs operations on the account (demand deposit (current or settlement) account, including special accounts; loan accounts; transit accounts, etc.).

Bank's Official Website - the Bank's website located on the Internet at: www.kdb.uz.

Bank Tariffs - the fees and commissions charged by the Bank to the Client for bank services rendered.

[Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, the definition of the “Business Day” was set out in the new wording \(the amendment shall come into force from 01.06.2022\).](#)

Business Day - is a period of time during which the Bank accepts and processes the Client's instructions. The duration of the business day shall be determined by the Bank's internal documents.

Call-Back Authorization – the procedure for additional confirmation of EPDs in foreign currency carried out by the Bank by means of telephone communication with a Contact Person authorized by the Client.

Call-Back Contact Details – the list of Contact Persons and telephone numbers for carrying out Call-Back Authorization procedure.

Contact Person – the person indicated in the list of Call-Back Contact Details and authorized by the Client to confirm the Client's EPD in foreign currency.

[Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, the definition of the “Client” was set out in the new wording \(the amendment shall come into force from 01.06.2022\).](#)

Client - a legal entity, including a financial institution or an individual entrepreneur that has entered into the Agreement with the Bank and has accepted the terms and conditions of this Public Offer.

Compromising (of Login, Password and/or Token) - loss of trust that the used Login, Password and/or Token ensure the security and confidentiality of information.

Creator - the User entitled to access the System to view the information, create an ED/EPD and send it to the 1st Authorizer for signature.

Electronic Payment Document (hereinafter – the **EPD**) - Client's remote instruction to carry out a transaction involving a Client's account with the Bank, transmitted to the Bank electronically, created and confirmed by the Client's duly authorized Users.

Electronic Document (hereinafter - the **ED**) – information recorded in electronic form, presented in the form of a file or database entry, created and transmitted by means of the System's software in accordance with the established procedure and confirmed by the Client's duly authorized Users.

Internet Banking System or the System – a set of technologies for remote banking services and execution of transactions by the Bank through software, hardware and telecommunication systems that enable interaction between the Bank and the Client by means of remote banking solutions.

Login (User name) - a set of alphanumeric characters chosen by the User during registration in the System to uniquely identify the User.

[Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/24/15 dated 05.03.2024, the term “OTP \(OTP device\)” was replaced with the term “Token” and the definition was set out in the new wording \(the amendment shall come into force from 25.03.2024\).](#)

Token – a mini-device generating the time-based one-time password (authentication code) that provides an extra layer of security to the System and consists of a string of numbers that are valid for only a brief period of time (typically 30 seconds or a minute).

Payment Session - the period of time from the moment the Client enters the System using the access credentials until the moment the Client exits the System.

User - the Client's responsible employee, whose name is stated in the Application, duly authorized to create and transmit the Client's ED/EPD and/or have access to the System in accordance with the terms of this Agreement.

Password - a set of alphanumeric characters chosen by the User during registration in the System which is unambiguously associated with the User name (Login) and used for the User authentication in the System.

1st Authorizer - the User entitled to authorize an ED/EPD after the Creator. This level of access is granted to the Client's responsible employee (User) whose name is indicated on the Client's specimen of signature and stamp provided to the Bank in accordance with the applicable Legislation.

2nd Authorizer - the User entitled to authorize an ED/EPD after the 1st Authorizer. This level of access is granted to the Client's responsible employee (User) whose name is indicated on the Client's specimen of signature and stamp provided to the Bank in accordance with the applicable Legislation.

3rd Authorizer - the User whose authorization is necessary to approve the ED/EPD already authorized by the 2nd Authorizer. This level of access shall be granted at the request of the Client.

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/25/91 dated 07.08.2025, Chapter 1 of the Public Offer is supplemented by the following definition (the amendment shall come into force from 25.08.2025).

Integration with ERP – the service that enables integration of a number of Internet Banking iDBA functions with the Client's ERP via Dibank service. The terms and procedure for integration with ERP are regulated by a separate agreement¹ forming an integral part hereof.

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/25/91 dated 07.08.2025, Chapter 1 of the Public Offer is supplemented by the following definition (the amendment shall come into force from 25.08.2025).

ERP Key – is a certified USB flash drive that securely encrypts the Client's electronic digital signature².

The definitions used in this Agreement shall be used and interpreted in the meaning of the relevant definitions set out in the Legislation or accepted by established practice.

2. SUBJECT OF AGREEMENT

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, clause 2.1 of the Public Offer was set out in new wording (the amendment shall come into force from 01.06.2022).

2.1 In accordance with the terms stipulated and conditions stipulated by this Agreement and the Bank Account Agreement, the Bank shall provide remote banking services in the System to the Client who has access to the Internet and appropriate technical equipment.

2.2 Access to the System, depending on the list of available functions, may be made using the Client's access credentials (Login/Password or Login/Password/Token).

2.3 Access option using Login/Password/Token credentials allows the Client to get access to the full list of services available in the System.

2.4 Access option using Login/Password credentials allows the Client to get access to a limited list of services available in the System.

2.5 The Parties acknowledge that an EPD which is duly created and authorized by the Client and transmitted to the Bank by means of the System software in accordance with all the information protection procedures provided for in this Agreement, is legally equivalent to a paper-based payment document.

2.6 The Parties acknowledge that the System is sufficient to ensure reliable operation in receiving, transmitting, processing and storing of information, as well as to protect information, ensure access

¹ Public Offer - Agreement on the integration of Client ERP with the Internet Banking iDBA system via "Dibank" service.

² The term is applied in accordance with the requirements of the Law of the Republic of Uzbekistan 'On Electronic digital signature' #3PY-793 dated 12.10.2022.

delimitation, encryption, integrity control as well as the Token are sufficient to protect against unauthorized access, authentication and authorization of ED/EPD as well as for handling of conflict situations thereunder. [Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, clause 2.7 of the Public Offer was set out in new wording \(the amendment shall come into force from 01.06.2022\).](#)

2.7 The Client shall pay the Bank a fee for the services provided in accordance with the Bank's Tariffs in force and under the terms and conditions provided for in this Agreement and the Bank Account Agreement.

2.8 The list of services, types of transactions, services and functions included in the System as well as possibility for the Client to access them shall be determined by the Bank independently.

[Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, clause 2.9 of the Public Offer was set out in new wording \(the amendment shall come into force from 01.06.2022\).](#)

2.9 The terms for the provision of services in the System are defined in this Agreement, in Appendices 1, 2, 3, 4 and 5 hereto as well as in the approved Bank Tariffs.

3. CONCLUSION OF THE AGREEMENT

3.1 On the basis of Article 369 (2) of the Civil Code of the Republic of Uzbekistan the text of this Agreement constitutes a Public Offer (an offer to conclude the Agreement), the Bank and the Client acknowledge that the conclusion of this Agreement is an acceptance of the Public Offer by the Client (an acceptance of the offer to conclude an Agreement).

3.2 Acceptance of the Public Offer shall be made by Client's personal visit to the Bank to sign the relevant Application in the established form (Appendix 4 to this Agreement).

3.3 The Client's acceptance of the Public Offer constitutes the Client's acknowledgement of the terms of this Agreement, the Appendices to this Agreement and the Bank Tariffs. The Client acknowledges that by accepting this Agreement, the Client agrees to the terms of this Agreement and the Appendices to this Agreement as well as recognizes them as binding upon the Client.

3.4 By accepting this Agreement, the Client acknowledges and the Bank agrees that pressing the relevant confirmation or sending keys as well as other similar keys in the System is analogous to the Client's handwritten signature.

3.5 The Client may read the text of this Agreement, Appendices to this Agreement and the Bank Tariffs in any of the following ways:

- by posting the text of this Agreement, Appendices to this Agreement and the Bank Tariffs on the official website of the Bank www.kdb.uz;
- by placing the text of this Agreement, Appendices to this Agreement and the Bank Tariffs in the branches of the Bank, including the Head Office of the Bank at the address: Tashkent city, 3, Bukhara Street;
- in other ways determined by the Bank.

4. TERMS OF SERVICE

4.1 The Client is connected to the System on the basis of a written Application which specifies the User's full name as well as his/her level of access to the System (Creator, 1st Authorizer, 2nd Authorizer, 3rd Authorizer). Along with the Application, the Client shall submit to the Bank documents confirming the authorization of the Users as well as their identity documents and other information at the discretion of the Bank.

4.2 Subject to the availability of the relevant services in the System, the services set out in Appendix 1 hereto may be provided to the Client within the framework of this Agreement.

4.3 The basis for the provision of one and/or all services of the System to the Client is the corresponding Application for User Registration.

4.4 The basis for suspension/termination of one and/or all services of the System shall be the Client's refusal from one and/or all services of the System, submitted to the Bank in writing.

4.5 Services in the System are provided remotely via the Internet by performing operations and actions on official website of the Internet Banking (ibank.kdb.uz) with the use of personal computer and other devices of the Client with similar functions. In order to access the Client's account(s) via the Internet Banking, each User shall receive access credentials (Login and Password) from the Bank.

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, clause 4.6 of the Public Offer was set out in new wording (the amendment shall come into force from 01.06.2022).

4.6 Upon submitting the application for User registration in the Internet Banking System with the possibility to send requests, applications or carry out transactions on the account(s) and/or conversion transactions, the Client must purchase a Token from the Bank.

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/24/15 dated 05.03.2024, clause 4.7 of the Public Offer was set out in a new wording (the amendment shall come into force from 05.03.2024)

4.7 The Client shall pay the cost of the Token to the Bank in accordance with the Bank Tariffs. Under Article 783 of the Civil Code of the Republic of Uzbekistan the Client agrees to the debiting of funds from the Client's account without its authorization (without the Client's consent) as payment for the cost of the Token;

4.8 The User assigned to the following access levels (Creator, 1st Authorizer, 2nd Authorizer and 3rd Authorizer) shall receive a Token from the Bank under the Token acceptance and handover Act (Appendix 5 to this Agreement).

4.9 The Client shall be entitled to service in the System after having submitted the Application for User registration, receiving the access credentials (Login, Password) from the Bank, purchasing the Token (if necessary) and familiarizing with the Remote Banking Servicing Rules (Appendix 3 to this Agreement).

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 4.10 of the Public Offer was set out in a new wording (the amendment shall come into force from 21.06.2021)

4.10 The Parties acknowledge that the System's access credentials of the 1st and 2nd Authorizer are recognized as equivalent to the handwritten signatures of the authorized persons indicated in the Client's specimen of signature and stamp card.

4.11 From the moment the Token is handed over to the User, any EPD confirmed by the respective Token and received via the System shall be deemed to have been duly sent by the Client and shall be subject to execution by the Bank in accordance with the terms of this Agreement.

4.12 The Parties acknowledge that the Client's ED/EPD sent to the Bank for execution through the System using a Token is equivalent to Client's instruction received on paper, executed in accordance with the Legislation of the Republic of Uzbekistan, signed by hand by a person authorized to manage the Client's account(s) in accordance with the Bank Account Agreement.

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clauses 4.13 and 4.14 of the Public Offer were set out in a new wording (the amendments shall come into force from 21.06.2021)

4.13 The Client's EPD shall be confirmed by the User's/Users' Token(s). At the same time, the Client's EPD in foreign currency exceeding the set threshold value of 10,000 (ten thousand) US Dollars or equivalent in other foreign currency shall be executed by the Bank only after successfully executed Call-Back Authorization.

4.14 The threshold value of the amount of a single EPD in a foreign currency used for Call-Back Authorization shall be determined by the Bank independently or in accordance with a separate written request submitted by the Client.

4.15 The types and forms of ED/EPDs available to the Client are posted in the System and may change in line with the System and services development.

4.16 The Client's ED/EPD shall be executed by the Bank on business days in accordance with the Types and Schedule of System services set out in Appendix 1 to this Agreement.

4.17 Information on the results of processing and execution or refusal to process and execute Client's ED/EPD shall be reflected in the status line of respective ED/EPD.

4.18 The Bank shall provide the Client with account statements in paper form at the Bank's branch, where the Client's accounts are served once a month (by default) or in accordance with the frequency of statements chosen by the Client.

4.19 An ED/EPD created but not confirmed by the Client may be deleted or rejected by the Client before the ED/EPD is confirmed by the Client.

4.20 An EPD becomes irrevocable for the Client at the moment the Client confirms the EPD. The EPD shall become finalized for the Client at the moment the funds are debited from the Client's account.

4.21 An ED/EPD transmitted via the System shall be processed and executed during the Bank's business hours and in accordance with the Bank's regulations, except for a number of automatic functions available in the System 24 hours a day.

4.22 The Bank shall suspend/terminate the Client's access to the System in the following cases:

- closure of the Client's account(s) connected to remote banking service;
- 5 (five) consecutive unsuccessful attempts to enter access credentials (Login, Password, Token code);
- failure to pay the Bank for the services rendered or if the Client the Bank a debt;
- technical failures occurring while using the Internet Banking system;
- occurrence of dispute arising out of the use of this Agreement;
- other cases stipulated by the Legislation.

4.23 During the period of technical problems elimination, the Client shall carry out banking transactions by submitting paper-based payment documents to the Bank.

4.24 The procedure for submitting/receiving complaints and claims of the Client, the conditions for their consideration and resolution shall be determined in accordance with the Legislation.

4.25 Phone number for Client service: +99878 120 80 00.

5. RIGHTS AND OBLIGATIONS OF THE PARTIES

The Bank shall be entitled:

5.1 Temporarily suspend (for the term not exceeding 1 (one) month) or refuse to provide access to the System in case of detection of suspicious transactions carried out via the System in accordance with the rules of Internal Control on countering the legalization of proceeds received from criminal activity, financing of terrorism and financing the proliferation of weapons of mass destruction in commercial banks, until the Client provides a written explanation of the legality of the transactions performed. In the event the Client fails to provide a written explanation of the legality of the transactions performed, the Bank shall be entitled to unilaterally terminate this Agreement with the Client;

5.2 If the event of doubts about suspicious transactions via the System, the Bank shall be entitled to inspect the Client/the User at place (postal address) or the Client's address indicated in the Bank's documents, including inspecting the transactions process directly by a person authorized in accordance with this Agreement;

5.3 To determine and change independently the forms, the terms, the set of transactions, services and functions included in the System, the possibility for the Client to access a certain form/function of the System as well as to set/change the general limits on transactions in the System;

5.4 In order to protect the Client's funds, the Bank is entitled to request from the Client an additional EPD confirmation (Call-Back Authorization) if the amount of one EPD exceeds the threshold value set by the Bank in accordance with clause 4.12 of this Agreement;

5.5 If in the process of the Call-Back Authorization the Bank has failed to reach the Client's Contact Person at the phone numbers listed in the form of Appendix 2 hereto or if the Bank suspects an attempt to commit fraud with the Client's funds, the Bank shall be entitled to suspend/defer execution of the EPD until additional confirmation from the Client is received as specified by the Bank's internal procedure and for a period not exceeding the current business day;

5.6 To request the Client to provide information (Call-Back Contact Details) for execution of additional confirmation of the EPD over the phone as provided for in Appendix 2 hereto, necessary for the Bank to perform Call-Back Authorization of the Client's EPD in foreign currency;

5.7 To request the Client to submit documents confirming the legality and economic feasibility of the transactions being carried out in the cases provided for by the current Legislation;

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, paragraph 3 of clause 5.8 of the Public Offer was set out in a new wording (the amendment shall come into force from 21.06.2021)

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, paragraph 3 of clause 5.8 of the Public Offer was supplemented by sub-item 5 (the amendment shall come into force from 01.06.2022)

5.8 To refuse to execute an EPD in the event of:

- incomplete / inaccurate indication by the Client of the details of the transaction to be performed;
- non-conformity of the transaction being executed to the established time limit;
- non-compliance of the transaction being executed with the Legislation including the Legislation on countering the legalization of proceeds received from criminal activity, financing of terrorism and financing the proliferation of weapons of mass destruction in commercial banks;
- insufficiency of funds on the Client's account(s) for execution of the transaction and/or for payment of the Bank's commission for the transaction being performed;
- insufficiency of funds on the Client's transit account for the execution of the payroll during the business day to replenish corporate plastic cards or cards of individuals (salary project) without notifying the Client. At the same time, the Bank shall be entitled to unilaterally delete an unexecuted payroll;
- in other cases, stipulated by the Legislation;

5.9 In accordance with the Bank Tariffs and on the basis of the Client's Application, the Bank shall be entitled to debit the commission amounts for providing banking services without authorization (without the Client's consent) at the time of the transaction execution via the System. The Bank shall also be entitled to correct erroneously credited amounts without authorization (without the Client's consent) in cases when the fact of erroneous crediting of funds to the Client's account(s) is detected or in other cases stipulated by the Legislation;

5.10 To change the terms of this Agreement and the Bank Tariffs for Internet Banking service with prior notification of the Client 10 (ten) calendar days before the effective date of amendments and additions by posting the information on the Bank's official website, by posting a notification in the System and on information boards in the Bank's premises;

5.11 To block the Client's Login and Password if it is suspected that they have been compromised as well as in cases specified in Section 5 of the Remote Banking Servicing Rules (Appendix 3 to this Agreement);

5.12 To suspend the exchange of ED/EPD with the Client in the event of technical failures or other circumstances, including changes in the Legislation which make it impossible or undesirable to exchange ED/EPD from the security point of view;

5.13 Not to accept for execution an ED/EPD in which mistakes have been made or the execution of which contradicts the current Legislation. In such cases the Bank shall be obliged to inform the Client within one day from the date of receipt of the ED/EPD;

5.14 Exercise other rights stipulated by the Legislation, this Agreement, the Appendices to this Agreement as well as other agreements concluded between the Bank and the Client;

5.15 To unilaterally terminate this Agreement if the Client breaches the terms of this Agreement, as well as in cases provided for by the Legislation.

The Client shall be entitled:

5.16 To use the System in the manner and under the terms provided for in this Agreement;

5.17 To carry out transactions using the System and use other services of the Bank in accordance with this Agreement and Appendices hereto;

5.18 To request the Bank to block access credentials of the User(s) (Login, Password) if unauthorized access or attempted unauthorized access to the System is detected;

5.19 When necessary, the Client shall be entitled to receive paper confirmation (certified copies) of execution payment instructions carried out through the System and account(s) statements for the required period;

[Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 5.20 of the Public Offer was set out in a new wording \(the amendments shall come into force from 21.06.2021\)](#)

5.20 To set limits for a single transaction on the basis of a separate written request;

[Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, Section 5 of the Public Offer was supplemented by clauses 5.20.1 and 5.20.2 \(the amendments shall come into force from 21.06.2021\)](#)

5.20.1 To change the threshold value of the amount of a single EPD in foreign currency determined in the Bank in accordance with clause 4.13 hereof and applied by the Bank for Call-Back Authorization (on the basis of a separate written request);

5.20.2 To suspend the use of the System for an extended period not exceeding 3 (three) consecutive months within 12 consecutive months (on the basis of a separate written request).

During the entire period, this Agreement shall not be terminated and the monthly fee shall not be charged; however, the Client shall be entitled to use the System only at the "View" level.

Herewith, if the period starts after the 15th day of the current month, the monthly fee for the current month shall be charged in full. If the period starts before the 15th day of the month (inclusive), the monthly fee for the current month shall be charged at the end of the last month of the period specified in the Client's written request.

5.21 To change the User's access credentials to the System;

5.22 To exercise other rights in accordance with this Agreement, Appendices to this Agreement, as well as other agreements concluded between the Bank and the Client.

[Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, Section 5 of the Public Offer was supplemented by clause 5.22.1 \(the amendments shall come into force from 21.06.2021\)](#)

5.22.1 If the Bank fails to comply with the deadlines set by the Legislation for debiting the Client's account or crediting the funds owed to the Client, the Client may demand that the Bank pay a penalty amounting to 0.1% of the overdue payment for each day of delay, but not more than 10% of the overdue payment amount.

The Bank undertakes:

- 5.23 To register the User in the System in accordance with the Application;
- 5.24 To provide remote banking services to the Client in the System within the scope of available services and functions in accordance with the Client's Application and in accordance with the terms provided for in this Agreement;
- 5.25 To maintain banking secrecy in respect to the Client's account transactions and to provide information on them only in the cases stipulated by the Legislation;
- 5.26 To suspend operations on the Client's account(s) upon written notification of the Client about the loss of access credentials (Login, Password, Token) or about unauthorized access to them by unauthorized persons;
- 5.27 To immediately block the User's/Users' account(s) upon the corresponding Client's written request;
- 5.28 To accept for execution the Client's ED/EPD executed in accordance with the terms of this Agreement and transmitted via the System;
- 5.29 To inform the Client in the event of refusal/failure to execute transactions and/or process an ED/EPD received from the Client via the System;
- 5.30 If a Token fails within 1 (one) year from the date of conclusion of this Agreement, the Bank undertakes to replace the Token with a new device once at free of charge upon the Client's written request to Bank;
- 5.31 To provide technical support to the Client over the phone and advice the Client on the correct use of the System;
- 5.32 To take all necessary and sufficient measures to ensure the normal and uninterrupted functioning of the System as well as to ensure proper maintenance of the System in accordance with the obligations assumed by the Bank under this Agreement;
- 5.33 To fulfill other obligations stipulated by the Legislation, this Agreement, including the Remote Banking Servicing Rules (Appendix 3 to this Agreement) as well as other agreements concluded between the Bank and the Client.

The Client undertakes:

- 5.34 To ensure the Client has software and hardware that enable the Client to access the Internet securely;
- 5.35 To pay a fee for the Token, a monthly fee for the use of the System in accordance with the Bank Tariffs;
- 5.36 To comply with the ED/EPD preparation requirements stipulated by the current Legislation and instructions of the Bank;
- 5.37 To send to the Bank clearly formulated ED/EPD that does not contain information that could be misinterpreted;
- 5.38 To check the ED/EPD execution status in the System immediately after authorizing the ED/EPD by the Client. The Client shall notify the Bank of any errors, duplications, discrepancies or omissions within the same business day of sending the ED/EPD;
- 5.39 To verify all information and data transmitted or communicated from the Bank through the System within 3 (three) business days after the information and data being received. The Client shall notify the Bank of any errors, discrepancies or omissions within 3 (three) business days after the information or data being transmitted. If no complaints are received from the Client within 3 (three) days, the information and data transmitted to/from the Client shall be deemed to be correct, accurate and complete;
- 5.40 To comply with and be guided by the Remote Banking Servicing Rules as set out in Appendix 3 to this Agreement;

- 5.41 To notify the Bank of all changes, including the dismissal and/or change of Users authorized to work in the System in order to block their access to the System by submitting a written or ED request to the Bank regarding the changes no later than the next business day following the introduction of such changes;
- 5.42 To notify the Bank of all changes, including dismissal and/or change of the Client's Contact Persons specified in Appendix 2 to this Agreement, who are authorized to confirm the Client's EPD in foreign currency received by the Bank through the System (Call-Back Authorization) no later than the next business day following the introduction of such changes;
- 5.43 In case of replacement or appointment of new Users admitted to work with the System, the Client undertakes to submit a corresponding Application for User registration in the System as well as the documents confirming powers/User access rights of the specified persons and their identity;
- 5.44 When transmitting ED/EPDs, the Client undertakes to use information processing, storage and protection systems only on the Client's personal computer and other devices that are in good working order and have been checked for the absence of computer viruses;
- 5.45 Not to transfer the User's access credentials (Login, Password) and the User's Token to third parties and not to grant access to the System to third parties, except for the Client's employees, who have access to the System in accordance with their official duties fixed by respective internal order;
- 5.46 Ensure the confidentiality of the User's access credentials (Login, Password) and the security of the Token (not to be passed on to third parties);
- 5.47 To immediately notify the Bank if unauthorized access or attempts of unauthorized access to the System is detected as well as if the Client's access credentials (Login, Password, Token) are lost or stolen;
[Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 5.48 of the Public Offer was set out in a new wording \(the amendments shall come into force from 21.06.2021\)](#)
- 5.48 To notify the Bank in writing immediately of any cases of Token loss. In cases of verbal notification (by phone), the Client shall confirm this in writing within 1 (one) business day from the date of loss. In this case, the use of the System by a corresponding User shall be discontinued and the User's access to the System shall be blocked from the moment of such notification until the Client receives a new Token from the Bank;
- 5.49 Not to use the services provided by the Bank for illegal purposes, including not to carry out operations/transactions aimed at legalization of proceeds received from criminal activity, financing of terrorism and financing the proliferation of weapons of mass destruction;
- 5.50 If necessary, at the request of the Bank, the Client undertakes to provide copies of contracts (other documents) within 3 (three) business days, confirming the legality and economic feasibility of the transaction carried out using the System in accordance with the requirements of the Legislation;
- 5.51 To comply with the current regulations of the Central Bank of the Republic of Uzbekistan;
- 5.52 To follow the User's Manual of the System (the text of the User Manual is available in the System);
- 5.53 In the event of faults in the System, the Client contacts the Bank's helpdesk to eliminate them.

6. LIABILITIES OF THE PARTIES

- 6.1 For non-performance or improper performance of obligations under this Agreement, the Parties shall be liable in accordance with the current Legislation.
- 6.2 The Client shall be liable:
- 6.2.1 for complying with the security requirements set out in the Remote Banking Servicing Rules (Appendix 3 to this Agreement) as well as for losses and (or) other consequences resulting from failure to comply with these security measures;

- 6.2.2 for ensuring the security and confidentiality of the System access credentials (Login, Password, Token) and Call-Back Contact Details required for additional Call-Back Authorization of the Client's EPD in foreign currency;
- 6.2.3 for losses that may arise as a result of unauthorized use of the System access credentials (Login, Password and/or Token), unauthorized use of Call-Back Contact Details required to perform additional Call-Back Authorization of the Client's EPD in foreign currency, as well as for non-performance / improper performance of established security and confidentiality measures set out in the Remote Banking Servicing Rules (Appendix 3 to this Agreement);
- 6.2.4 for unauthorized access by third parties to the use of the System services as a result of the Client own intent or negligence as well as for all consequences caused by such unauthorized access;
- 6.2.5 for any consequences that may arise as a result of any action or initiative taken by the Client (with or without the Client's knowledge) or third parties using the Client's access credentials (Login, Password, Token) for managing the Client's accounts via the System or using Call-Back Contact Details required to perform additional confirmation of the Clients EPD in foreign currency;

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, Section 6 of the Public Offer was supplemented by clause 6.2.6 (clause 6.3 in the previous version) (the amendments shall come into force from 21.06.2021)

- 6.2.6 The Client is responsible for complying with the rules for the use of payment instruments, the procedure for drawing up and authorization of ED/EPDs in accordance with the Legislation.

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 6.3 of the Public Offer was set out in a new wording (the amendments shall come into force from 21.06.2021)

- 6.3 The Bank shall be liable for the correct reflection of transactions on the Client's account and the timely transmission of information via the Internet Banking System.

- 6.4 The Bank shall not be liable:

- 6.4.1 for non-performance or improper performance of its obligations under this Agreement for reasons related to disruption of the Internet;
- 6.4.2 for the quality of services provided by mobile phone operators, fixed line telephone network operators, Internet service providers, etc.;
- 6.4.3 for the actions of the owners of personal computers and mobile devices, for the actions of the owners of websites and mobile applications used by the Client, for the actions caused by third-party software used by the Client as well as for any losses and/or other consequences resulting from the Client's failure to comply with the security requirements set forth in the Remote Banking Servicing Rules (Appendix 3 to this Agreement);
- 6.4.4 for the theft, damage or loss of the Client's confidential information, including access credentials (Login, Password, Token) as a result of malicious software running on the equipment that the Client uses to access the System and for the consequences thereof;
- 6.4.5 for any losses incurred by the Client due to unauthorized access of third parties to the Client's account management via the System using the Client's access credentials (Login, Password and/or Token) or other Client's information required to access and carry out transactions via the System and in other cases provided for in this Agreement;
- 6.4.6 for the failure to execute a payment instruction or other instructions transmitted by the Client via the System, which occurred through no fault of the Bank, or for irregular, inaccurate, incomplete information and/or data transmitted or requested through the System if such failure occurred due System failure, malfunction or shutdown which occurred through no fault of the Bank;
- 6.4.7 for failure to execute the Client's instructions sent to the Bank via the System in case the Client's account(s) are blocked or seized, as well as in case operations on the Client's account(s) are

suspended as provided for in this Agreement, in the Bank Account Agreement and/or in accordance with the Legislation;

- 6.4.8 for failure to execute Client's instructions sent to the Bank via the System, the execution of which contradicts the current Legislation or in the event of errors made in the process of their creation;
 - 6.4.9 for any losses and/or other consequences that may arise as a result of the Bank's failure to execute the Client's instructions for the reasons set out in this section of the Agreement;
 - 6.4.10 for failure to execute the Client's EPD in foreign currency caused by several consecutive unsuccessful attempts by the Bank's authorised employees to call the Client's Contact Person by phone numbers indicated in the form of Appendix 2 to this Agreement in order to perform additional Call-Back Authorization of the Client's EPD in the manner prescribed by the relevant internal procedure of the Bank;
 - 6.4.11 for any losses and/or other consequences that may arise as a result of the Bank's failure to execute the Client's instructions for the reasons set out in this section of the Agreement.
- 6.5 The Bank does not guarantee that the System will be free of errors, malfunctions, operational failures or delays in the execution of the Client's orders and instructions beyond the Bank's control. Nor does the Bank guarantee that the System will operate uninterruptedly, that the System is the latest achievement of modern technology or that it meets the specific goals or results expected by the Client
- 6.6 The Bank's liability to the Client does not include indirect losses incurred by the Client as a result of System failures due power shortages or other third-party disputes that make the System impossible to operate, even if the Bank has been notified of the possibility of such losses, unless the Client proves that such losses have been caused by deliberate or negligence from the Bank's side.
- 6.7 The Parties shall be released from liability for non-performance or improper performance of obligations under this Agreement if it is due to force majeure circumstances. The terms of exemption from liability and the procedure for Parties' relations in the event of force majeure defined in Section 9 of this.

7. AMENDMENTS AND ADDITIONS

[Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 7.1 of the Public Offer was set out in a new wording \(the amendments shall come into force from 21.06.2021\)](#)

- 7.1 The Client acknowledges and accepts the right of the Bank to unilaterally amend and supplement this Agreement, the Appendices to this Agreement and the Bank Tariffs on the terms set out in this section of the Agreement with prior notice to the Client (10 days before such amendments take effect).
- 7.2 The Bank shall notify the Client in advance before making amendments and additions to the relevant documents in Uzbek, Russian and English by posting notification on the Bank's Official Website, in the premises of the Bank's premises (the "Information" board) and in the System (the "News" section). Notification made in accordance with this article shall be deemed to have been received on the date of its posting.
- 7.3 By notifying the Client of amendments and additions to this Agreement, the Bank shall have the right to suspend the use of the System by the Client until the Client has confirmed that he/she has read the amendments and additions to the terms of the Agreement proposed by the Bank upon notification.
- 7.4 If the Client disagrees with the amendments and additions to this Agreement or Appendices to this Agreement, the Client shall notify the Bank thereof in writing prior to the stated amendments and additions take effect. The Client's disagreement with the amendments and additions to this Agreement and/or Appendices to this Agreement shall constitute the Client's withdrawal from this Agreement and shall result in termination of this Agreement with the Client within 5 (five) days from the date the Bank receives a

written notice from the Client (including in the ED form) of disagreement with amendments and additions to this Agreement and/or Appendices to this Agreement.

7.5 The absence of the Client's notification as specified in clause 7.4 hereof shall constitute the Client's consent of the amendments and additions to this Agreement and/or the Appendices to this Agreement and shall be deemed by the Bank and the Client as the Client's acceptance of the Bank's offer to continue this Agreement under the new terms.

7.6 If the Bank makes amendments and additions to the Bank Tariffs, such amendments and additions shall apply to this Agreement as from their effective date.

8. SECURITY AND CONFIDENTIALITY

8.1 The Client undertakes to ensure sufficient security measures in accordance with the Remote Banking Servicing Rules (Appendix 3 to this Agreement) in order to protect the System from unauthorized access by third parties and shall therefore be liable for all consequences of failure to fulfill this obligation.

8.2 The Client undertakes to take appropriate security measures and to instruct the Users that they may not, directly or indirectly, knowingly or through negligence disclose or show to any unauthorized person or other User, legal entity or corporation the access credentials (Login, Password, Token), as well as not allow the Token to fall into the hands of an unauthorized person and another User, legal entity or corporation.

8.3 The Client guarantees and is responsible for ensuring that only the Users duly indicated in the Application are familiar with the information relating to the System and its use as well as only the Users shall have access to the System.

8.4 The Client agrees to change the Password periodically and timely provide the Bank with updated Call-Back Contact Details necessary to perform additional Call-Back Authorization of the Client's EPD in foreign currency (Appendix 2 to this Agreement).

8.5 The Client understands and agrees that the Bank may record phone conversations between the Bank and the Client upon execution of additional Call-Back Authorization. The Client agrees that such recordings of phone conversations can be used by the Bank as evidence in the event of a dispute between the Bank and the Client.

8.6 The Client shall immediately notify the Bank by phone and confirm in writing to the Bank as soon as possible but no later than within 8 (eight) hours, if the Client has any reason to believe that the System and/or any access credentials (Login, Password, Token) may become available to unauthorized persons or have been misused.

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 8.7 of the Public Offer was set out in a new wording (the amendments shall come into force from 21.06.2021)

8.7 Until the Bank is able to take appropriate measures, but in any case, within 1 (one) hour after receiving the Client's notification, the Client shall be responsible for any unauthorized use of the System and/or any access credentials (Login, Password, Token). The Client shall take all necessary and sufficient measures to protect the Bank from any incurred or possible losses, costs, damages or actions directed against the Bank as a result of such unauthorized use of the System and access credentials.

8.8 The Client confirms that the System and related instructions, documentation, technical literature and other materials / information are trade secrets of the Bank and are strictly confidential, inviolable and important, and this confidentiality significantly affects the efficiency and success of the Bank's business. The Client hereby agrees to keep confidential the System, documentation, information, knowledge and experience gained in relation to the use of the System and not to disclose, make copies, duplicate, sell or

transfer the System or related instructions, documentation, technical literature and other materials / information to third parties.

9. FORCE MAJEURE

9.1 In the event of force majeure circumstances that prevent the Client and/or the Bank from performing their functions under this Agreement, which include natural disasters, accidents, fires, riots, strikes, military actions, illegal actions of third parties, communication networks breakdowns (including the Internet), power supply accidents, entry into force of regulatory legal acts, any other binding decisions of authorized bodies and / or organizations, directly or indirectly prohibiting the activities specified in this Agreement, as well as other circumstances beyond the control of the Bank and the Client, the Parties shall be released from liability for failure to fulfill the obligations assumed.

9.2 The Party affected by force majeure shall immediately but not later than 3 (three) banking days after the force majeure occurs, inform the other Party in writing about the circumstances and their consequences and shall take all possible measures in order to limit negative consequences caused by the specified force majeure circumstances.

9.3 Failure by either Party to timely notify the other Party of the occurrence of force majeure entails the loss of the right to refer to such circumstances in order to exempt from liability for non-performance or improper performance of obligations under this Agreement.

9.4 The occurrence of force majeure may result in an extension of the period of performance of obligations under this Agreement for the duration of the force majeure otherwise agreed by the Parties.

9.5 Exemption of a Party from liability for failure to perform or improper performance of any obligation under this Agreement affected by a force majeure circumstance shall not relieve that Party from liability for failure to perform or improper performance of its other obligations under this Agreement not affected by force majeure.

9.6 In the event of force majeure circumstances lasting more than six months, either Party shall be entitled to refuse to perform its obligations under this Agreement.

10. TERM OF THE AGREEMENT

10.1 This Agreement shall enter into force upon the Client fulfillment of the provisions of section 3 of this Agreement and shall be valid for one calendar year. If the Parties have not applied for its termination within 5 days before the end of one calendar year, the Agreement shall be deemed prolonged for each subsequent year.

10.2 The Agreement may be terminated by either Party at any time, provided that the initiating Party notifies the other Party in writing at least 1 calendar month in advance with all obligations under this Agreement binding.

10.3 If the Agreement is terminated before the 15th (inclusive) day of the month, the monthly fee for that month shall not be charged. If the Agreement is terminated after the 15th day of the month, the monthly fee for that month shall be charged in full.

10.4 If the Client intends to close all accounts with the Bank, the Client's official request to close all accounts will be grounds for terminating this Agreement.

10.5 The Agreement may be unilaterally terminated by the Bank in the event of reasonable suspicion of the use of the System services for the purpose of legalization of proceed received from criminal activity, financing of terrorism and financing the proliferation of weapons of mass destruction.

11. DISPUTE RESOLUTION PROCEDURE

11.1 In the event of disputes under this Agreement, the Bank and the Client shall take all measures to resolve them through negotiations between the Parties. If no agreement is reached between the Parties, the dispute shall be resolved in accordance with and on the order established by the Legislation.

11.2 On matters not regulated by this Agreement, Appendices to this Agreement and Bank Tariffs, the Parties shall be governed by the Bank Account Agreement and/or the current Legislation.

12. OTHER PROVISIONS

12.1 The Parties shall notify each other without delay of any change of address, telephone or fax number, but in any event not later than three (3) days after such change.

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 12.2 of the Public Offer was set out in a new wording (the amendments shall come into force from 21.06.2021)

12.2 The terms of this Agreement are in Uzbek, Russian and English with the greatest possible effort on the part of the Bank to ensure authenticity between the versions in different languages.

13. BANK ADDRESS AND BANK DETAILS

KDB Bank Uzbekistan JSC, Head Office

Address: 3, Bukharo Street, 100047, Tashkent, the Republic of Uzbekistan

Phone: (+998 78) 120-80-00

E-mail info@kdb.uz

Tax ID: 202167236

Bank Code: 00842

SWIFT Code: KODBUZ22

KDB Bank Uzbekistan JSC, Oybek Branch

Address: 32, Oybek Street, 100015, Tashkent, the Republic of Uzbekistan

Phone: (+998 78) 140-06-30

E-mail info@kdb.uz

Tax ID: 207045749

Bank Code: 01065

SWIFT Code: KODBUZ22

License of the Central Bank of the Republic of Uzbekistan # 5 dated 21.10.2017.

Appendix 1 to the Public Offer – “Internet Banking iDBA” remote banking servicing agreement for Legal Entities and Individual Entrepreneurs

Information on amendments: in accordance with the Management Board Protocol #IMG/LGD/HO/22/42 dated 25.05.2022, items #17 and #18 were added to the Appendix 1 (the amendment shall come into force from 01.06.2022).

List of services and service schedule in the Internet Banking System

#	Name of service	Servicing time* (Tashkent time)
1.	Viewing account balances and account movements	24/7
2.	View and print payment history	24/7
3.	Sending a request to the Bank	24/7
4.	Request for account opening	24/7
5.	Plastic card account replenishment (salary and equated payments)	9.00 a.m. – 5.30 p.m.
6.	Corporate plastic card account replenishment	9.00 a.m. – 5.30 p.m.
7.	External transfers in national currency (including transfers with value date option)	9.00 a.m. – 4.45 p.m.
8.	Transfers within the Bank in national currency (including transfers with value date option)	9.00 a.m. – 6.00 p.m.
9.	External transfers in foreign currency (SWIFT)	9.00 a.m. – 4.30 p.m.
10.	Transfers within the Bank in foreign currency	9.00 a.m. – 4.30 p.m.
11.	Conversion operations (currency purchase / sale)	9.00 a.m. – 4.30 p.m.
12.	Transfers in national currency via ANOR system ¹	24/7
13.	Transfers in national currency via ANOR system (including transfers with value date option) ²	24/7
14.	Transfers in national currency via MUNIS system	24/7
15.	View the list of Export/Import contracts	24/7
16.	View the information on the loan agreement	24/7
17.	Submitting pre-approval request for a sub-loan ³	9.00 a.m. – 6.00 p.m.
18.	Sending request for sub-loan drawdown ³	9.00 a.m. – 4.00 p.m.

Notes!

1. The Client's EPD received by the Bank during the specified servicing time* are executed by the Bank on the same business day.
2. The Client's EPD (except items 12, 13 and 14) are accepted by the Bank for execution on official business days according to business hours of the Bank/Bank's branches.
3. The Bank shall be entitled to change the business hours of the Bank/ Bank's branches, as well as the servicing time in the Internet Banking System.
4. The execution of EPD in foreign currencies (SWIFT) is carried out in accordance with the business hours of the Bank's correspondent banks.
5. The time limit for execution of transfer in national currency may be changed (prolonged) depending on the relevant instruction of the Central Bank of the Republic of Uzbekistan.

¹ The Client's EPD received by the Bank after the stipulated servicing time are executed by the Bank on the next business day. An EPD sent by the Client on non-working days shall be executed by the Bank on the first working day following the non-working day.

² The Client's EPD received by the Bank with a value date different from the date on which the EPD was received are executed by the Bank on the value date before 4.30 pm.

³ Available for financial institutions only. Applications are accepted for execution within 2 business days.

Terms of execution of payment documents via ANOR Instant Payment System (ANOR System).

For the purpose of this Agreement, the following terms shall have the following meanings:

Instant payment - a payment made on the basis of the Client's instruction transmitted via Internet Banking System in real time;

Instant payment system (hereinafter referred to as "ANOR System") - a service that allows paying for goods, works, services, obligations to the budget in Uzbek sums in real time, 24 hours a day, 7 days a week without days off and holidays.

1. The Bank shall accept, process and transmit instant payments based on the Client's payment instructions received via the Internet Bank system.
2. The amount of bank commission (cost of services) for the execution of instant payments by the Bank is established in accordance with the Bank's Tariffs.
3. The time of execution of payment orders by the Bank via ANOR System shall be indicated in the Bank's business day duration available to the Client in the Internet Banking System.
4. The Bank executes the Client's payment instructions via ANOR system if the following conditions are met in total:
 - the payment instruction is created as an electronic document (EPD) in Uzbek sums and to be debited from the Client's Uzbek sum account;
 - there are no restrictions on the Client's account in the form of seizure, suspension of operations, reservation of funds for other payment instructions, reservation of funds for urgent needs, for salary payment (within the established minimum), etc.;
 - the Client has sufficient funds in the account to make the payment;
 - the beneficiary bank of an instant payment is a member of ANOR system and is active in that system;
 - the payment instruction (payment type) is marked as "Payment instruction via ANOR system";
 - the transaction is not subject to additional control according to the rules and procedures established by the Bank;
 - there are no other restrictions imposed by law and/or by the Bank.
5. A payment instruction (payment type) marked as "Payment instruction via ANOR system" is irrevocable and not subject to cancellation by the Client.
6. Instant payments are executed in full amount up to the balance on the Client's account minus bank fee (service fee) for execution of instant payments in accordance with Bank Tariffs.
7. If an instant payment is cancelled (rejected) or the payment status changes, the Bank automatically notifies the Client accordingly by sending a message to the Client in the Internet Banking system.

Appendix 2 to the Public Offer – “Internet Banking iDBA” remote banking servicing agreement for Legal Entities and Individual Entrepreneurs

Call-Back Contact Details:

Name of Legal Entity / Individual Entrepreneur:	
TAX ID:	

Contact Persons for Call-Back Authorization

1. Name

Phone number 1) 2)

2. Name

Phone number 1) 2)

3. Name

Phone number 1) 2)

* *Please cross out the blank fields.*

The Client hereby confirms that any of the above-mentioned persons is authorized to confirm payment instructions in a foreign currency sent to the Bank for execution via the Internet Banking System.

Agree to indemnify the Bank against any payment or loss that the Client may incur as a result of the execution or non-execution of the above-mentioned payment instructions.

The Client undertakes to take full responsibility not to disclose the above information to third parties other than the aforementioned persons, to provide true details when confirming electronic payment documents received by the Bank via the Internet Banking System.

The Client also undertakes to timely update the Call-Back Contact Details.

The above stated is confirmed,

Director:

Full name / Position

Signature

SEAL (if required)

Appendix 3 to the Public Offer – “Internet Banking iDBA” remote banking servicing agreement for Legal Entities and Individual Entrepreneurs

**Remote Banking Servicing Rules
for Legal Entities and Individual Entrepreneurs**

1. Operating the System and access to the System.

The Client shall comply with the following requirements when using the System:

1.1 To ensure confidentiality of access credentials (Login, Password, Token) entered into the computer or device used to operate the System, the Client shall use devices with functioning security systems, such as:

- restricted access to the workplace (computer or another device);
- active licensed (not counterfeit) anti-virus software with up-to-date databases;
- operating system update;

1.2 Do not operate the System on the Internet by using a source of connection from places that are not trustworthy or by using public communication channels (free Wi-Fi, etc.);

1.3 Ensure safety and confidentiality of access credentials (Login, Password, Token) and other information required to access and perform transactions and actions using the System, not to disclose such information to other persons (including friends, acquaintances, relatives, employees of the Bank, etc.);

1.4 Under any circumstances, never disclose Internet Banking System access credentials (Login, Password, Token) to anyone. Bank employees and Technical Support employees do not need to know the Password or Token authentication code).

1.5 Change the Password on a regular basis, at least once every 90 days, or immediately upon the occurrence of events that could directly or indirectly affect its confidentiality;

1.6 During an open payment session do not leave the computer or other device unattended (the computer and other device by means of which the Internet Banking System is being operated;

1.7 While working in the System, always press "EXIT" button at the end of a payment session as well as before closing the browser window;

1.8 Immediately notify the Bank of the facts of unauthorized transactions on the accounts accessible through the System, or of the facts of illegal use of access credentials (Login, Password, Token) by third parties as well as other information necessary to access the System and execute transactions or actions using the System;

1.9 Do not enter information into the fields of the System interface which is not requested in the form of the System's window in use or which is not supposed to be entered into the fields of the System's window in use;

1.10 Replace the Client's Token in case of dismissal and/or change of responsible employees (Users) having access to the System and/or having an authority to sign a power of attorney to receive Tokens at the Bank;

1.11 When using the Bank's website www.kdb.uz, make sure that the connection with the Bank's server is in secure mode (HTTPS protocol);

1.12 Do not accept the browser's offer to save Password for an automatic login at a later date;

1.13 Do not save your Login, Password on a computer, mobile device, any other digital media (computer hard drive, removable digital media), paper media or Internet service that other persons may have an access to;

1.14 To maintain the confidentiality of the access credentials (Login, Password, Token) and the information on transactions carried out it is recommended that the Client:

- does not use the "Autofill" browser functions on pages where the access credentials are inputted;
- ensures to use a password-protected operating system user account;
- disables the Autorun function of removable data storage devices in the operating system of the Client's workstation used to operate the Internet Banking System;
- connects the workstation used to operate the Internet Banking System to the Internet only while working in the System;
- does not use the Client's workstation to connect to social networks, to forums, conferences, chat rooms, telephone services and other sites containing potential malware, as well as to read mail and open mail documents from untrustworthy addressees;
- does not use for the Internet Banking System the Login and Password that are already used to authorize the Client on other websites;
- uses strong password containing at least 8 characters with uppercase letters, lowercase letters and minimum one digit);
- carefully examines the information displayed on the computer screen (or other device) used to work in the Internet Banking System, chooses actions from the options offered by the System in accordance with the Client's intentions and carefully checks the correctness of the information inputted;
- pays attention to any changes and software errors while connecting to the Internet Banking System or while working in the System. In case of any doubts as to the correctness of the System's functioning, immediately stops operating the System and contacts the Bank in order to ascertain the absence / presence of unauthorized transactions;
- in case of the browser warnings about redirection to another website while connecting to the Internet Banking System, the Client is advised to postpone transactions and contact the Bank's technical support service in order to determine the reasons for the redirection;
- to inform the authorized employees of the Bank about any attempts to get the access credentials to the Internet Banking System (Login, Password, Token);
- to check the account history/account statements regularly to keep track of errors or unauthorized account transactions;

Failure to comply with the above requirements and recommendations on the part of the Client will be the basis for the Bank to impose liability for the disputed transactions carried out using the Internet Banking System on the Client.

2. Connection to the System

2.1 The Bank provides Internet Banking remote banking services only if the Client has a bank account opened with the Bank.

2.2 The Bank shall connect the Client to the Internet Banking System on the basis of the Agreement. The Agreement can be concluded irrespective of term of servicing the Client at the Bank and the amount of account turnover. Restrictions on connection of the Client to the System may be the grounds provided for by the requirements of the rules of Internal Control on countering legalization of proceed received from criminal activity, financing of terrorism and financing the proliferation of weapons of mass destruction in commercial banks.

[Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 2.3 of Appendix 3 to the Public Offer was set out in a new wording \(the amendments shall come into force from 21.06.2021\)](#)

2.3 To connect to the Internet Banking System the Client shall download a template of the Application for User Registration (Appendix 4 to this Agreement) from the Bank's official website or shall receive a

template of the Application in any branch of the Bank, complete it, certify the Application with the Client's signature and stamp and submit the Application to responsible officer of the respective branch of the Bank.

2.4 The responsible officer of the Bank shall verify the authenticity and validity of the Client's signature and stamp on the Application, sign it, affix the Bank's stamp and hand it over to the authorized officer of the Bank for the Client's registration in the System.

2.5 The authorized officer of the Bank registers the User in accordance with the data specified in the Application. The Client independently chooses the username (Login) and Access Password. The username (Login) chosen by the Client may be rejected by the Bank if it is already in use by another Client.

2.6 The Client's manager or the Client's authorized representative acting under a power of attorney shall receive the second copy / copy of the Application as well as the Token from the Bank in person on the basis of the Token acceptance and handover Act (Appendix 5 to this Agreement).

3. Change of User

3.1 In order to make changes and additions to the number of System Users (registration of new Users and/or change of User), the Client shall submit to the Bank a new Application for registration of another User, which shall clearly state the purpose (connection/correction), as well as the level of access to the System for the new or the changing User.

3.2 Pursuant to clause 4.1 of this Agreement, the Application for user registration shall be submitted to the Bank together with the documents proving the User authority, as well as his/her identity documents and other information requested at the discretion of the Bank

4. User data correction

4.1 If it is necessary to update the User data or the User access credentials (Login, Password) the Client shall submit to the Bank a new, duly completed Application with a clear indication of the purpose (correction) and all the User data subject to change.

4.2 The correction of the User data includes:

- changing the Client's name or form of ownership;
- User personal data update;
- changing the list of Users and/or User access right;
- change of the mobile phone number, e-mail, and other User data.

5. Blocking and unblocking access to the System

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, paragraph 2 of clause 5.1 of the Public Offer was set out in a new wording (the amendments shall come into force from 21.06.2021)

5.1 The Client is entitled to block the Client's access to the System (fully or partially):

- in case of threat of unauthorized access or suspicion of compromised access credentials (Login, Password, Token) the Client shall immediately inform the Bank in order to block the compromised Client's access credentials;
- in case of verbal notification by phone (with duly Client's identification) the Client shall confirm blocking of an access to the System in writing no later than the next business day. Blocking is carried out within 1 (one) hour after the Client's request;
- in case of change of the User or User's data correction, the Client shall submit a new Application to the Bank in accordance with clause 4.1 of the Remote Banking Servicing Rules. Based on the received Application, the Bank shall block the User's access to the System and make corresponding

adjustments in the System. The blocking shall be done no later than the end of the next business day after the Bank receives the Client's request.

Information on amendments: in accordance with the Management Board Protocol # 45 dated 07.06.2021, clause 5.1 (4th paragraph) of Appendix 3 to the Public Offer was set out in a new wording (the amendments shall come into force from 21.06.2021)

When access to the System is blocked on the basis of a corresponding request (verbal or written) received from the Client in accordance with the Remote Banking Servicing Rules or the access is blocked at the discretion of the Bank in order to ensure security of the System, the Bank shall immediately send a confirmation of blocking to the User's email address indicated in the Application.

To unblock the User's/Users' access to the System, the Client shall submit to the Bank a corresponding written request certified by the signature of the Client's Head (or his representative acting on the basis of a power of attorney) and bearing the Client's seal imprint.

5.2 The Bank is entitled to block the Client's access to the System in case the Client owes the Bank for banking services provided. In this case:

- the Bank shall send to the Client a notification about the debt occurred via the Internet Banking System indicating the due date of debt repayment;
- if the Client fails to pay the debt to the Bank within the specified period, the Bank shall block the Client's access to the Internet Banking System;
- after the debt has been paid in full, the Bank shall unblock the Client's access to the System not later than the end of the business day when the debt was paid.

5.3 The Bank shall be entitled to block the Client's access to the System if the Client exceeds the number of attempts allowed to enter the access credentials (Login, Password):

- If the number of attempts to enter the access credentials exceeds the number of attempts specified in the System settings (more than 5 unsuccessful attempts) the System will automatically block the Client's access to the System.
- To unblock the User's/Users' access to the System, the Client shall submit to the Bank a corresponding written request certified by the signature of the Client's Head (or his representative acting on the basis of a power of attorney) and bearing the Client's seal imprint.

6. Restoring the Client's Password

6.1 If the Client's Password needs to be recovered, the User shall go through the password recovery procedure using the "Forgot your password?" option on the Internet Banking System's homepage, following the instructions available to the Client on the Bank's official website www.kdb.uz.

Appendix 4 to the Public Offer – “Internet Banking iDBA” remote banking servicing agreement for Legal Entities and Individual Entrepreneurs

APPLICATION FOR USER REGISTRATION

☐ **Connection**

☐ **Correction**

In order to register a User in the Internet Banking System of KDB Bank Uzbekistan JSC, the following information must be submitted to the Bank (in writing, signed by the Client's Head and sealed):

Name of Legal entity / Individual Entrepreneur	
TAX ID:	
User Full Name	
User Phone Number (landline and mobile)	
User E-mail	
Login (preferably, name of the Legal entity/IE)	
Password (can be changed later)	

Level of Access			Restrict access to:
<input type="checkbox"/> View Only		Token is not required	<input type="checkbox"/> Inquiry
			<input type="checkbox"/> New Account opening
<input type="checkbox"/> Creator		<input type="checkbox"/> New Token * <input type="checkbox"/> Existing Token serial number: _____	<input type="checkbox"/> Salary
<input type="checkbox"/> 1st Authorizer			<input type="checkbox"/> Corporate Card
<input type="checkbox"/> 2nd Authorizer			<input type="checkbox"/> Local Currency Transfers
<input type="checkbox"/> 3rd Authorizer			<input type="checkbox"/> Foreign Currency Transfers
			<input type="checkbox"/> Conversion Section
		<input type="checkbox"/> New ERP Key * <input type="checkbox"/> Existing ERP Key serial number: _____	<input type="checkbox"/> Integration with ERP (1C/Didox)

* Please choose one the options below to pay for the cost of a Token / ERP Key:

<input type="checkbox"/>	Please debit our account No. _____ in Uzbek soums.
<input type="checkbox"/>	Payment by bank transfer on the basis of an invoice.

By signing this Application, the Client acknowledges and agrees to be bound by the terms and conditions of the Public Offer - Internet Banking iDBA remote banking servicing agreement for legal entities and individual entrepreneurs, as well as the applicable Bank Tariffs, as published on the Bank's website (www.kdb.uz) on the date of signing.

Date: _____

Director / Head

Full name / Position

Signature

SEAL (if required)

**Appendix 5 to the Public Offer – “Internet Banking iDBA” remote banking
servicing agreement for Legal Entities and Individual Entrepreneurs**

ACCEPTANCE AND HANDOVER ACT

Tashkent city _____

This Act is made between KDB Bank Uzbekistan JSC (hereinafter the “Bank”) and

(hereinafter the “Client”) certifying that the Bank officer _____
has handed over:

- ☐ a Token (serial number _____) /
- ☐ an ERP Key (serial number _____)

to the authorized person of the Client _____
who is duly entitled to sign financial documents.

The provided Token / ERP Key must be stored by the Client’s responsible employee (User) in a place protected from unauthorized use and be used only by the Client’s responsible employee (User) for authorization (signing) of electronic documents/electronic payment documents transmitted to the Bank.

Acceptance and handover is confirmed.

The Client:

The Bank:

Name & Signature

Name & Signature

Manager/Director

Name & Signature

Bank Officer

SEAL
(if required)

SEAL
(if required)